CAPCO

4 EFFECTIVE STRATEGIES TO CONQUER VULNERABILITY THREATS

INTRODUCTION

A rapidly shifting threat landscape and multiplying points of exposure, coupled with the devastating effects a security breach can bring, requires organizations to rethink their vulnerability management strategy.

According to a recent ServiceNow security report, 60% of breaches are related to an unpatched known vulnerability where the patch was not applied[1]. Now is the time for security teams to act and begin a vulnerability management program.

This means moving away from reactive strategies toward a comprehensive, risk-based approach that continuously identifies, evaluates and maps potential threats using data analytics and, in response, proposes remediation and mitigation techniques.

1. https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html

WHAT IS VULNERABILITY MANAGEMENT?

Vulnerability management is defined by NIST as "a capability that identifies vulnerabilities on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network[2]." Vulnerability management offers a streamlined approach for addressing vulnerabilities to susceptible systems. These assessments can target one or more of the following areas:

- **Host:** Assess servers for vulnerabilities and test for base image alignment
- **Network:** Analyze access management policies for networks and network available resources
- **Database:** Assess databases for vulnerabilities and misconfigurations, identifying insecure environments and infrastructure weaknesses
- **Application:** Scan web applications to identify front-end and source code vulnerabilities

2. https://csrc.nist.gov/glossary/term/Vulnerability_Management#:~:text=Definition(s)%3A,extend%20compromise%20to%20the%20network.

4 STEPS TO TRANSITION TO RISK-BASED VULNERABILITY MANAGEMENT

The key to the success of a vulnerability management program is transitioning to a risk-based model that will identify and address the greatest threats to your organization.

Get started building your successful vulnerability management program with these four steps:

1. Identify and classify your organization's assets. This will ensure the ability to accurately measure and communicate risk to your key stakeholders.

2. Select software that fits the needs of your organization's IT footprint. The market for vulnerability management software is expected to be worth $15.5 billion by 2025[3] vendors are crowding the marketplace with tools of varying maturity as they vie for some of that market share. Conduct short-term proofs of concept with at least two vendors to identify the best fit.

3. Determine frequency of scanning. Decide how the vulnerability management software will be implemented, and set up a frequency of scanning that best fits the needs of your organization. Best practice is to perform continuous scanning of the organization's environment.

4. Remediate and fix vulnerabilities. The hard work begins once the vulnerabilities have been identified and assigned a risk-based score. Vulnerabilities must be addressed by the security policy to ensure issues are quickly remediated and fixed. However, not all vulnerabilities discovered will require an all-hands-on-deck mitigation approach. Some may be queued for future efforts, and recorded in mitigation service level agreements. Most mature software offerings integrate with existing change management tools to easily track vulnerability mitigation efforts.

3. https://www.asdnews.com/news/defense/2020/05/25/security-vulnerability-management-market-worth-155-bn-2025

HOW VULNERABILITY MANAGEMENT PROTECTS AGAINST THREATS

With traditional network perimeters collapsing and organizations becoming more and more distributed, it is increasingly difficult to monitor every point of a network and support dynamic, secure access needs. A vulnerability management program provides continuous centralized reports and visualizations to better assess the cyber health of your organization.

Sure, running one-off scans provides valuable information, but this single snapshot in time grows stale quickly. Continuous scanning increases efficiencies and begins capturing assets the moment they are deployed. Initial tool implementation and security policy creation require an investment of time to get the details right. However, once enabled operational efficiencies are realized immediately and laborious, manual scans become a thing of the past.

Vulnerability assessments and proper management help protect against some of the following common threats:

- SQL injection and cross-site scripting (XSS) attacks, where code is input by an attacker that processes an action unintended for the original prompt's purpose
- Faulty authentication systems, allowing an attacker to gain unauthorized access or privileges
- Insecure configurations and standards that do not meet the organization's security policy

RISK-BASED VULNERABILITY MANAGEMENT PAYS OFF

Vulnerability management is a high priority initiative for security teams around the world that look to comply with industry frameworks and secure their environments. Automatically detecting and prioritizing vulnerabilities is an invaluable industry best practice. Take the four steps outlined in this post to get the most out of your vulnerability management systems and maintain a strong security posture.

AUTHORS

Grant Auerbach, Consultant
Grant.Auerbach@capco.com

Scott Carmichael, Senior Consultant
Scott.Carmichael@capco.com

Robert Furr, Managing Principal
Robert.Furr@capco.com

FOR MORE INFORMATION:

John Janssen, Partner
John.Janssen@capco.com

Robert Furr, Managing Principal
Robert.Furr@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com**, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO