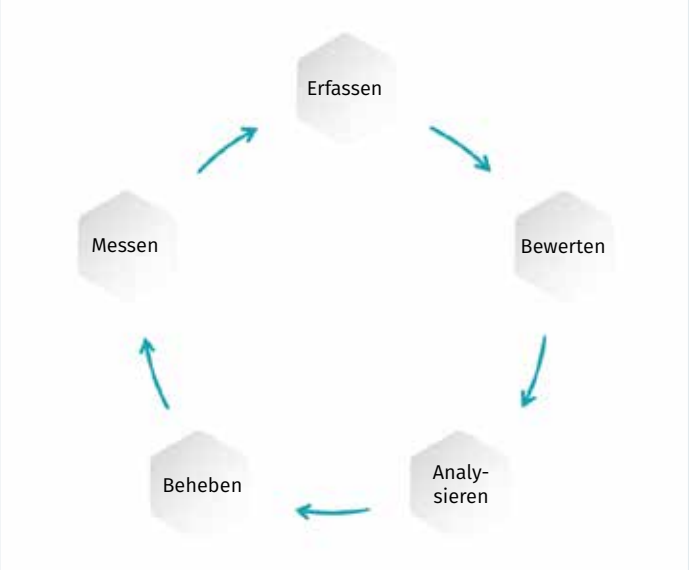
tenable

Schwachstellen-Management:
Bewerten

Schwachstellen-Management ist eine wesentliche Komponente des Sicherheitsprogramms in jedem Unternehmen. Es bildet die Grundlage für Cyber Exposure, einer neuen Disziplin zur Verwaltung und Messung des Cybersecurity-Risikos im digitalen Zeitalter. Ein ausgereiftes Programm für das Schwachstellen-Management (Vulnerability Management, VM) umfasst alle fünf Schritte des unten aufgeführten Cyber Exposure Lifecycle.



Cyber Exposure Lifecycle

Im Mittelpunkt dieser Lösungsübersicht steht der zweite Schritt beim Schwachstellen-Management: Bewerten.

Ziel des Bewertungsschrittes ist es, die Cyber Exposure aller Assets zu verstehen, einschließlich ihrer Schwachstellen, Fehlkonfigurationen und anderen Sicherheitsindikatoren.

Wichtige Vorteile

- **Bewertung der gesamten Angriffsoberfläche**, sodass Sie das Risiko kennen und Ihr Unternehmen angemessen schützen können.
- **Prüfung von Patches und Konfigurationsänderungen**, um zu gewährleisten, dass Schwachstellen und Fehlkonfigurationen wie erwartet behoben wurden.
- **Bereitstellung von Informationen für das Vorfallsmanagement** über Schwachstellen und Fehlkonfigurationen, damit die entsprechenden Untersuchungen priorisiert werden können.

Herausforderungen

Die Bewertung sämtlicher Assets ist aus zwei Hauptgründen eine Herausforderung:

- Für verschiedene Asset-Typen – herkömmliche IT-Assets, unbeständige, mobile und dynamische Assets sowie Assets aus dem Bereich der operativen Technologien (OT) – sind häufig unterschiedliche Bewertungstechnologien erforderlich. Aktive Bewertungsscans eignen sich am besten für herkömmliche IT-Assets. Für Cloud, Web-Apps, Container und operative Technologien sind jedoch zusätzliche Bewertungsmethoden erforderlich. Beispielweise sollte zur Bewertung von OT-Assets wie SPS-Systemen und RTUs passives Monitoring eingesetzt werden. Dadurch verringert sich das Risiko, dass ihr Betrieb durch aktives Scannen unterbrochen wird.
- Die Richtigkeit der Daten muss gewährleistet sein. Nichts schadet der Glaubwürdigkeit von Sicherheitsverantwortlichen in den Augen von Asset-Besitzern oder Administratoren mehr als ungenaue Bewertungsdaten. Eine einzige falsche Zahl kann dazu führen, dass Ihre gesamte Arbeit in Frage gestellt wird. Es ist eine sorgfältige Vorbereitung erforderlich, damit die Bewertung mit der optimalen Breite, Tiefe und Häufigkeit stattfinden kann. Sie benötigen die richtigen Technologien, um die gesamte Bandbreite von Assets bewerten zu können, ohne bestimmte Assets bzw. Schwachstellen doppelt zu berücksichtigen. Sie benötigen aktuelle Zugangsdaten für tiefgehende, authentifizierte Bewertungen, in deren Verlauf Sie die richtigen Tests durchführen müssen. Und Sie müssen Informationen zeitnah bereitstellen.

Lösung

Der Aufbau einer ausgereiften Bewertungsfunktion, mit der die gesamte Angriffsoberfläche Ihres Unternehmens ermittelt werden kann, durchläuft vier Stufen. Tenable kann Sie auf jeder dieser Stufen unterstützen.

STUFE 1: BEWERTUNG HERKÖMMLICHER ON-PREMISES-ASSETS

Wählen Sie die erfassten Hosts aus, die bewertet werden sollen, und führen Sie mit der Nessus Basic Network Scan-Vorlage einen internen Schwachstellen-Scan durch, der für alle Host geeignet ist. Bei den Bewertungen auf Stufe 1 wird davon ausgegangen, dass Nessus nicht über die für authentifizierte Scans benötigten Zugangsdaten verfügt. Aus diesem Grund überspringt Nessus automatisch die lokalen Sicherheitschecks, die zwar im Basic Network Scan enthalten sind, aber nur mit entsprechenden Zugangsdaten ausgeführt werden können.

STUFE 2. ERHÖHUNG DER BREITE, TIEFE UND HÄUFIGKEIT VON BEWERTUNGEN

Die Breite der Bewertung muss auf alle modernen Assets ausgedehnt werden, um die gesamte Angriffsoberfläche zu beurteilen. Tenable bietet Bewertungsfunktionen, die für Laptops, Mobilgeräte, virtuelle Infrastrukturen, Cloud, Web-Apps, Container und operative Technologien optimiert sind. Unter Umständen müssen Sie umdenken, neue Beziehungen mit der Applikationsentwicklung aufbauen, innovative Methoden zur Umsetzung von Sicherheitsmaßnahmen finden und gleichzeitig schnelle DevOps-Prozesse ermöglichen. Eine Methode besteht darin, die Bewertung während der Entwicklungsphase in Software-Build-Workflows zu integrieren, anstatt zu warten, bis die Software-Assets in der Produktion bereitgestellt werden.

Durch den Einsatz von authentifizierten Scan-Vorgängen und Agenten steigern Sie die Tiefe der Bewertung. Authentifizierte Scans, auch Credentialed-Scans genannt, melden sich remote bei Geräten an, um diese von innen heraus zu untersuchen. Da authentifizierte Scans Geräte intern abfragen, können sie eine Fülle sicherheitsrelevanter Daten über installierte Software und Schwachstellen zusammentragen. Agentenbasiertes Scanning, das von auf den Zielgeräten installierter Software durchgeführt wird, betrachtet Geräte ebenfalls von innen heraus und kann ähnlich detaillierte Informationen wie wie authentifizierte Scans bereitstellen. Mit Agenten lassen sich zwei gängige Probleme im Zusammenhang mit unbeständigen Assets lösen: Zum einen beseitigen sie den blinden Fleck, der entsteht, wenn Assets, die während des Scan-Vorgangs vom Netzwerk getrennt sind, nicht bewertet werden. Zum anderen werden bestimmte Assets (und die zugehörigen Schwachstellen) nur einmal gemeldet, auch wenn sich bei jeder erneuten Verbindung mit dem Netzwerk die IP-Adresse ändert.

Sie sollten Malware-Erkennung in Ihre Bewertungen einbeziehen. Authentifizierte Scans können dann Dateisysteme nach bekannter Malware durchsuchen. Außerdem können sie das Vorhandensein, den Update-Status und die Ausführung von vielen Antivirus-Produkten erkennen.

Bewertungen sollten nicht nur ad hoc, sondern in regelmäßigen Intervallen stattfinden. Empfehlenswert ist ein wöchentliches Intervall, mindestens aber sollte sich die Scan-Häufigkeit an Ihrem Patching-Zyklus orientieren.

STUFE 3: BEWERTUNG VON KONFIGURATIONEN UND OPTIMIERUNG DER BEWERTUNG NACH ASSET-KLASSE

Durch Konfigurationsbewertung wird die Angriffsoberfläche eines Assets reduziert, indem nicht benötigte Dienste wie FTP und RDP deaktiviert werden, starke Authentifizierung erzwungen wird und die Sicherheit des Assets allgemein gehärtet wird. Sie können Ihre Server, Desktops, Laptops, Webdienste, Datenbanken, Cloud-Infrastrukturen, Netzwerkgeräte usw. anhand von Standards des Center for Internet Security, der Defense Information Systems Agency und vieler anderer Anbieter bewerten. Hinweis: Wenn Sie die Assets zum ersten Mal anhand dieser Standards bewerten, finden Sie wahrscheinlich deutlich mehr Konfigurationsprobleme

als erwartet. Aus diesem Grund müssen Sie die Anforderungen unter Umständen zunächst etwas herunterfahren und dann allmählich steigern.

Sie definieren die Bewertungsparameter basierend auf der SLA für die jeweilige Asset-Klasse. SLAs für verschiedene Asset-Klassen sorgen für die optimierte Einstellung der Tiefe, Breite und Häufigkeit von Bewertungen, sodass Sie Ihre Angriffsoberfläche basierend auf den erwarteten Verlust-Größenordnungen in den einzelnen Geschäftsbereichen absichern können. Assets mit der Klassifizierung „Hoch“ werden einer gründlicheren Bewertung unterzogen als andere Asset-Klassen.

STUFE 4: KONTINUIERLICHE BEWERTUNG VON ASSETS UND INTEGRATION MIT PRIVILEGED ACCESS MANAGEMENT

Auf dieser Stufe ergänzen Sie den Prozess durch die Bewertung neuer Assets in nahezu Echtzeit sowie durch eine periodische Überprüfung der Bewertungs-SLAs. Gegebenenfalls kann auch eine Integration mit Privileged Access Management-Systemen vorgenommen werden.

Bei der Echtzeitbewertung werden neu erfasste Assets umgehend beurteilt. Passives Monitoring identifiziert kontinuierlich zahlreiche neue Schwachstellen und kann zudem automatisch einen aktiven Scan auslösen, um ein neu erfasstes Asset eingehender zu untersuchen. Wenn im Build-Image des neuen Assets ein Agent vorhanden ist, führt dieser automatisch eine Asset-Bewertung durch und meldet die Ergebnisse.

Durch regelmäßige Prüfungen der SLAs wird gewährleistet, dass Bewertungsrichtlinien für die einzelnen Asset-Klassen (in Bezug auf Tiefe, Breite und Häufigkeit) immer auf dem neuesten Stand sind. Wenn beispielsweise Ihr Team für Anwendungsentwicklung für eine Umsatz generierende Website zuständig ist und seit kurzem Container-Technologie oder Azure einsetzt, müssen Sie gemeinsam mit dem Team die entsprechende Bewertungsrichtlinie aktualisieren.

Privileged Access Management (PAM)-Integration ist sehr hilfreich, wenn Sie regelmäßig die Zugangsdaten für authentifiziertes Scannen ändern. Durch die Integration werden dem Scanner automatisch aktuelle Zugangsdaten bereitgestellt, damit Scan-Vorgänge nicht fehlschlagen.

Weitere Informationen: Besuchen Sie **de.tenable.com**
Kontakt: Senden Sie eine E-Mail an **sales@de.tenable.com** oder besuchen Sie **de.tenable.com/contact**

ÜBER TENABLE

Tenable®, Inc. ist das Cyber Exposure-Unternehmen. Über 27.000 Organisationen aus aller Welt verlassen sich auf Tenable, wenn es um die Erkennung und Minimierung von Cyberrisiken geht. Als Erfinder von Nessus® hat Tenable sein Know-how im Bereich des Schwachstellenmanagements erweitert, um die weltweit erste Plattform bereitzustellen, mit der jedes digitale Asset auf jeder beliebigen Computing-Plattform erkannt und abgesichert werden kann. Zu den Kunden von Tenable zählen mehr als die Hälfte der Fortune 500, mehr als 25 Prozent der Global 2000 sowie große Regierungsbehörden. Erfahren Sie mehr über uns auf **de.tenable.com**.