RAPID7

KUNDENRATGEBER

SCHWACHSTELLEN-MANAGEMENT-LÖSUNGEN

Wie Sie Ihre Anforderungen definieren und den richtigen Anbieter auswählen

INHALTSVERZEICHNIS

Einführung

Mithilfe des Schwachstellen-Managements können Sicherheitsschwachstellen in Geschäftsprozessen, Webanwendungen und Betriebssystemen (sowie in der darauf ausgeführten Software) erkannt, bewertet, behoben und gemeldet werden. Dieser Prozess muss kontinuierlich durchlaufen werden, um mit neuen Systemen in Netzwerken, Änderungen an Systemen und Anwendungen Schritt zu halten, um neue Schwachstellen frühzeitig zu erkennen.

Üblicherweise werden bei Angriffen und Sicherheitsverletzungen im ersten Schritt Schwachstellen in Browsern, Betriebssystemen und Softwareanwendungen von Drittanbietern ausgenutzt. Das Ermitteln und Beheben dieser Schwachstellen, bevor Angreifer diese ausnutzen können, stellt eine proaktive Schutzmaßnahme dar, die für alle Sicherheitsprogramme von wesentlicher Bedeutung ist.

Lösungsarchitektur

Die Lösungsarchitektur bildet die Grundlage für Ihr Schwachstellen-Management-Programm und kann sich auf Ihre Fähigkeit zur Optimierung der Scan-Leistung und schnellen Skalierung Ihrer Bereitstellung auswirken.

Moderne Anwendungen für das Schwachstellen-Management müssen eine komplexe, dynamische IT-Umgebung überwachen und innerhalb von wenigen Stunden oder sogar Minuten reagieren, sobald Probleme erkannt werden. Sie sollen das herkömmliche Netzwerk-Schwachstellen-Management ergänzen und so die Handhabung komplexerer Infrastrukturen ermöglichen. Auf diese Weise können Sie:

- vollständige Transparenz in Ihrem IT-Umfeld erzielen
- die Leistungsfähigkeit beim Testen von sich schnell weiterentwickelnden, komplexen Webanwendungen erhöhen
- die Achtsamkeit gegenüber Phishing und anderen Social-Engineering-Angriffen stärken und ungewöhnliches Nutzerverhalten erkennen
- mittels Penetrationstests das Gesamtrisiko bewerten und Gegenmaßnahmen besser priorisieren

Lesen Sie mehr zum Thema Entwickeln von modernen Programmen für das Schwachstellen-Management.

Die zentrale technische Komponente dieses Prozesses ist in der Regel ein Tool für das Schwachstellen-Management, das mit Ihrer lokalen, virtuellen oder Cloud-Umgebung verbundene Systeme und Container erkennt. Es überprüft diese anschließend mithilfe von Scan-Engines und Agents oder überprüft die Images innerhalb der Container Registry auf Schwachstellen. Moderne Programme setzen für den Abruf von Schwachstellendaten von Geräten in Echtzeit zunehmend auf Agents – vor allem bei Endpunkten und Geräten, die sich auf herkömmliche Weise nur schwer scannen lassen.

Sie müssen zudem ein Anwendungs- und Benutzer-Schwachstellen-Management umfassen. Diese Erweiterung des Prüfradius über die üblichen Netzwerk-Scans hinaus ist der zunehmenden Komplexität moderner Netzwerke geschuldet. Heute befinden sich Unternehmensnetzwerke in kontinuierlichem Wandel und werden ständig erweitert, häufig ohne die ausdrückliche Zustimmung des Sicherheitsteams. Daher ist die Zusammenarbeit mit anderen unternehmensinternen Teams entscheidend.

Ein modernes Programm für das Schwachstellen-Management muss über das einfache Scannen und Beheben von Problemen hinausgehen. Es sollte Unterstützung bei der Automatisierung und Orchestrierung von kritischen Aufgaben (z. B. Erkennung von Assets in virtuellen und Cloud-Umgebungen sowie in Umgebungen für die Anwendungsentwicklung) bieten und zudem die Automatisierung nutzen, um die Priorisierung und Behebung von Schwachstellen zu beschleunigen oder, falls notwendig, Systeme vom Netzwerk zu trennen.

Ein idealer Partner im Bereich Schwachstellen-Management hilft Unternehmen, mit seinen Lösungen diese Herausforderungen zu bewältigen, und durch Umsetzen der Grundprinzipien von SecOps – teamübergreifender Sichtbarkeit, Analytik und Automatisierung – eine moderne Sicherheitsinfrastruktur einzurichten.

Für die Durchführung eines effektiven Proof of Concept (PoC) für ein Schwachstellen-Management-Tool sind vier wesentliche Schritte notwendig:

Vorbereiten: Beginnen Sie zunächst damit, den Umfang Ihres Vorhabens zu definieren. Legen Sie fest, was Sie prüfen müssen, sowie in welcher Form und wie häufig dies geschehen soll. Identifizieren Sie zeitaufwändige und ständig wiederkehrende Aufgaben, die möglicherweise durch die Automatisierungsfähigkeiten der Lösung verbessert werden könnten. Dokumentieren Sie zudem Ihre wichtigsten Assets, Verantwortlichkeiten sowie ihren Standort.

Prüfen: Im Rahmen des PoC überprüfen Sie das Netzwerk auf Schwachstellen, unsichere Geräte- und Softwarekonfigurationen (oder Fehlkonfigurationen), die Einhaltung interner und/oder externer Sicherheitsrichtlinien sowie weiterer Sicherheitsmaßnahmen, die im Netzwerk vorhanden sind.

Beheben: Priorisieren Sie die zu behebenden Schwachstellen anhand von Informationen über die Bedrohungslandschaft und der Bedeutung des Systems für das Unternehmen. Stellen Sie sicher, dass das Tool Sie bei der effektiven Implementierung von automatisierten Prozessen unterstützt und gleichzeitig die Kommunikation zwischen den am Prozess der Remediation (Schwachstellenbehebung) beteiligten Personen und Lösungen ermöglicht.

Ergebnisse kontrollieren: Prüfen Sie abschließend, ob das getestete Tool die gewünschte Wirksamkeit für Ihr allgemeines Schwachstellen-Management-Programm erzielt. Sie können dies tun, indem Sie Ausgangswerte bestimmen, Metriken für den Erfolg festlegen (z. B. Risikominderung, eingesparte Zeit) und den Fortschritt zur Zielerreichung verfolgen.

01 Wichtigste Komponenten

Flexible Implementierung

Systeme und Netzwerkinfrastruktur sind in jedem Unternehmen anders. Ihre Schwachstellen-Management-Lösung sollte daher flexible Implementierungsoptionen und volle Kontrolle über die Scanvorgänge bieten. Die Möglichkeit der optimalen Anpassung Ihrer Schwachstellen-Management-Lösung an die speziellen Erfordernisse Ihres Unternehmens ist entscheidend, wenn Sie die Schnelligkeit und Genauigkeit der Analysen erhöhen möchten.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Bietet die Architektur der Lösung ausreichende Flexibilität, um die Scan-Konfiguration für optimale Leistung anzupassen?
- Müssen für die Automatisierung zusätzliche Lösungen erworben werden?

Verteilte Scanvorgänge

Die Verwaltung der Scan-Vorgänge an einem zentralen Ort und die Zusammenführung der Scan-Daten steigert die Effizienz Ihrer Schwachstellen-Management-Lösung und verringert die Belastung des Netzwerks. Eine optimal verteilte Architektur beinhaltet eine zentrale Konsole für die Verwaltung der Abläufe, das Reporting und die Administration sowie mehrere verteilte Scan-Engines zur Abdeckung der gesamten IT-Umgebung.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Ermöglicht die Lösung die zentralisierte Verwaltung von verteilten Scan-Engines?

Interne und externe Scanvorgänge

Mit internen Scanvorgängen wird die Sicherheit Ihres Netzwerks diesseits der Firewall überprüft. Externe Scanvorgänge werden von außen durchgeführt. Durch die Kombination von internen und externen Scanvorgängen können Sie sich ein vollständiges Bild von den Risiken machen, denen Ihr Unternehmen ausgesetzt ist.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Ist die Lösung in der Lage, interne und externe Scanvorgänge auszuführen?

Agent-basierte Analyse

Agents können für die kontinuierliche Überwachung von Assets eingesetzt werden, die anhand von herkömmlichen Scanvorgängen möglicherweise nur schwer erreichbar sind, wie etwa Netzwerke mit geringer Bandbreite oder Remote-Benutzer. Sie ermöglichen detaillierte Scans ohne die Angabe von Anmeldeinformationen und können auch in virtuelle oder cloudbasierte Golden Images eingebettet werden, um automatisch Einblick in neu eingefügte Infrastrukturen zu erhalten. Anbieter mit mehreren Produkten sollten auf der Grundlage eines Ansatzes mit „universellem Agent“ arbeiten, sodass die Daten von nur einem Agent für mehrere Lösungen gesammelt werden können und so die Bereitstellung vereinfacht wird.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Verwendet der Anbieter einen ressourcenschonenden Agent?
- Wie einfach lässt sich der Agent installieren?
- Welchen Nutzen bietet der Agent?

Endpunktüberwachung

Da immer mehr Unternehmen das Augenmerk auf die Absicherung ihrer Server richten, haben sich Angreifer der veränderten Situation angepasst und konzentrieren ihre Aktionen nun auf Benutzer und Endpunkte. Endpunkte und Benutzer gehören zu den Aspekten des Netzwerks, deren Verwaltung sich besonders schwierig gestaltet. Dies ist speziell bei Unternehmen mit Remote-Benutzern bzw. bei Auftragnehmern der Fall, die nur selten eine Verbindung zum Netzwerk herstellen. Eine Schwachstellen-Management-Lösung sollte diese Geräte kontinuierlich überwachen, selbst wenn diese sich außerhalb des Netzwerks befinden, wobei für die Überwachung vorzugsweise Agents zu verwenden sind. Agents müssen sich einfach mithilfe Ihrer Softwaremanagement- und Orchestrierungstools bereitstellen lassen und sehr kompakt sein, damit die Auswirkungen auf die Netzwerkleistung möglichst gering bleiben.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Wie überwacht die Lösung Remote-Benutzer und Endpunkte, die vom Netzwerk getrennt sind?

Skalierbarkeit

Die Schwachstellen-Management-Lösung sollte mit dem Wachstum Ihrer Infrastruktur Schritt halten können. Idealerweise muss die Lösung in der Lage sein, die Kapazität durch Hinzufügen von Scan-Engines zu Ihrer bestehenden Installation zu steigern. Dabei sollten nur geringe bzw. keine zusätzlichen Kosten anfallen. Der Lösungsanbieter muss bei größeren Infrastrukturen über ausgewiesene Kompetenz in ähnlich dimensionierten Installationen verfügen. Zudem erleichtert die Fähigkeit eines Anbieters, die Datenverarbeitung ganz oder teilweise auf eine Cloud-Plattform zu verlagern, die Skalierung für große Infrastrukturen und Datensets.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Ist die Lösung schnell und einfach skalierbar?

Netzwerk-Schwachstellenanalyse

Die Netzwerk-Schwachstellenanalyse ist wichtig für die Identifizierung von Risiken in Ihrer Infrastruktur. Ein effektives Sicherheitsprogramm erfordert jedoch eine umfassende Lösung, die mehr als nur eine reine Auflistung der Schwachstellen bietet.

Erkennung

Sie müssen genau wissen, über welche Assets Sie verfügen, bevor Sie das Risiko dieser Assets bewerten und steuern können. Das Scannen des gesamten Netzwerks zur Erkennung und Inventarisierung aller Assets, einschließlich ihrer Betriebssysteme, Anwendungen und Dienste, stellt eine grundlegende Funktionalität für ein effektives Schwachstellen-Management-Programm dar. Es sollte eine automatische Kategorisierung und Überwachung auf Basis mehrerer Attribute und nicht nur auf der Grundlage der IP-Adressen erfolgen.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Führt die Lösung eine automatische Erkennung und Kategorisierung von Assets durch?

Einheitliche Schwachstellen- und Konfigurationsanalyse

Wenn Assets, Schwachstellen und Fehlkonfigurationen im Zuge nur eines Scanvorgangs identifiziert werden, minimiert sich hierdurch die Belastung für Ihr Netzwerk. Außerdem gewährleistet dies eine kürzere Scan-Dauer und verringert den Verwaltungsaufwand. Die Lösung sollte eine einheitliche Benutzeroberfläche und Reporting für die Schwachstellen- und Konfigurationsanalyse bereitstellen, damit Sie sich einen vollständigen Überblick über Ihr Sicherheitsrisiko und die Compliance-Situation machen können.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Ist die Lösung in der Lage, die Erkennung sowie die Schwachstellen- und Konfigurationsanalyse in nur einem Scanvorgang durchzuführen?

Container-Analyse

Container bieten unglaubliche Flexibilität für die Anwendungsentwicklung. DevOps-Teams können Anwendungen mithilfe von Containern schnell einführen und aktualisieren. Allerdings bringen Container auch besondere Herausforderungen im Bereich Sicherheit mit sich: Sie werden häufig ohne Wissen des Sicherheitsteams verwendet. Dabei können sich Schwachstellen in Container-Images auf zahlreiche Anwendungen auswirken, sofern diese nicht schnell behoben werden. Moderne Lösungen für das Schwachstellen-Management können Container-Hosts identifizieren, in Registrys gespeicherte Container-Images überprüfen und Container noch während des Buildprozesses analysieren, indem diese in das CI/CD-Tool des Teams integriert werden.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Kann die Lösung automatisch Container-Hosts identifizieren und in Registrys gespeicherte Container-Images überprüfen? Lässt sie sich zudem in Ihr CI/CD-Tool integrieren?

Authentifizierte Scanvorgänge

Durch die Verwendung von Zugangsdaten ist eine Anmeldung an den Systemen möglich, wodurch mehr Informationen gesammelt und eine genauere Aussage über Risiken und Konfigurationen getroffen werden kann. Remote-Scans liefern dagegen lediglich eine Sicht von außen auf die Assets. Suchen Sie nach einer Lösung, die authentifizierte Scanvorgänge mit einer breiten Palette von Betriebssystem-, Datenbank- und Netzwerk-Zugangsdaten sowie mit Zugangsdaten auf der Anwendungsebene unterstützt.

FRAGEN SIE DEN LÖSUNGSANBIETER

- In welche Access-Management-Produkte kann die Lösung integriert werden?

Virtuelle und Cloud-Umgebungen

Virtualisierungs- und Cloud-Technologien ermöglichen es Unternehmen, Assets bedarfsorientiert einzufügen. Dies birgt jedoch Herausforderungen, da viele Lösungen beim Scanvorgang nicht zwischen physischen und virtuellen Assets unterscheiden. Ihre Lösung muss in der Lage sein, Risiken für virtuelle und Cloud- Assets dynamisch zu erkennen und zu analysieren, um diese Umgebungen abzusichern.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Kann die Lösung durch direkte Integration eine automatische Erkennung und Analyse der Risiken für virtuelle und Cloud-Assets durchführen?

Netzwerkveränderungen

Die meisten Unternehmen führen Schwachstellenscans monatlich oder vierteljährlich durch. Moderne Netzwerke verändern sich jedoch minütlich: neue Geräte werden dem Netzwerk hinzugefügt und neue Schwachstellen außerhalb der regelmäßig geplanten Scan-Zeitfenster offengelegt. Ein effektives Schwachstellen-Management-Tool ist in der Lage, neue Geräte und Schwachstellen zwischen den einzelnen Scanvorgängen zu erkennen und dabei die Anzahl von False-Positives zu minimieren.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Ist die Lösung imstande, neue Geräte zu erkennen und zu analysieren, die dem Netzwerk zwischen den geplanten Scanvorgängen hinzugefügt werden?

Scanfrequenz

Ihr Netzwerk unterliegt ständigen Veränderungen. Durch Festlegen von regelmäßigen Scans können Sie sicherstellen, dass Sicherheitslücken ermittelt und zeitnah behoben werden. Planen Sie die automatische Ausführung von Scanvorgängen innerhalb bestimmter Zeitfenster ein, um Netzwerkunterbrechungen zu minimieren. Die Ausführung sollte monatlich, wöchentlich oder sogar täglich erfolgen.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Stellt die Lösung eine Kalenderfunktion für die Planung von Scans und zulässigen Zeitfenstern bereit?

Priorisierung

Häufig wissen Sicherheitsteams nicht, welche Schwachstellen sie zuerst beheben sollen. Je nach Unternehmen kann die Kritikalität einer Schwachstelle unterschiedlich bewertet werden. Sie müssen zudem einschätzen, welche Angriffsvarianten derzeit gängig sind.

Risiko-Score

Da die Anzahl der Schwachstellen in einem Unternehmen inzwischen in die Tausende oder gar Millionen gehen kann, benötigen Sie einen modernen Risiko-Scoring-Algorithmus, der Sie bei der Auswahl der Schwachstellen unterstützt, die zuerst behoben werden müssen. Die bloße Anwendung des Industriestandards CVSS ist für eine effektive Priorisierung nicht ausreichend. In den Risiko-Score müssen Bedrohungsmetriken wie die Gefährdung durch Exploits und Malware-Kits sowie Informationen zur Dauer der Ausnutzbarkeit der Schwachstelle einfließen, damit die Priorisierung von Schwachstellen möglichst präzise automatisiert werden kann.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Liefert die Lösung einen granularen Risiko-Score, der Bedrohungsanalysen und temporale Metriken berücksichtigt?

Geschäftskontext

Ein effektiver Ansatz für die Schwachstellenpriorisierung erfordert zusätzliche Informationen über Ihre Assets, u. a. wo sich diese befinden, welche Funktion sie haben, wer der Besitzer ist und welche relative Bedeutung ihnen zukommt. Anhand dieser kontextbezogenen Informationen können Sie geschäftskritische Systeme und Daten für die Remediation priorisieren. Die Lösung muss darüber hinaus in der Lage sein, den Risiko-Score automatisch aufgrund der Kritikalität des jeweiligen Assets anzupassen.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Ist die Lösung imstande, Remediation-Maßnahmen für geschäftskritische Assets zu priorisieren?

Threat Feeds

Neben der Ausnutzbarkeit erkannter Schwachstellen muss auch unbedingt deren Aktualität berücksichtigt werden. Zukunftsorientierte Schwachstellen-Management-Lösungen integrieren Bedrohungsanalysen und das Wissen über aktuelle Angriffsmethoden, um Sie bei der Priorisierung tatsächlich kritischer Schwachstellen zu unterstützen – insbesondere in Reaktion auf Zero-Day-Bedrohungen.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Fallen zusätzliche Kosten für den Zugang zu Erkenntnissen und Analysen über Bedrohungen an?
- Sind die Erkenntnisse und Analysen so zugeschnitten, dass die für Ihre Umgebung relevanten Informationen dargestellt werden?

Validierung der Schwachstellen

Anhand einer Kombination aus Scanvorgängen und Penetrationstests können Sie überprüfen, ob identifizierte Schwachstellen ein tatsächliches Risiko für Ihr Unternehmen darstellen. Auf diese Weise können Sie die Schwachstellenbehebung priorisieren und Ausnahmen für Schwachstellen erstellen, die nicht ausgenutzt werden konnten.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Bietet der Anbieter der Schwachstellen-Management-Anwendung auch ein Penetrationstest-Tool für die Schwachstellenvalidierung an, damit Ihnen eine zentrale Anlaufstelle für den Support und die Abrechnung zur Verfügung steht?

Schwachstellenbehebung

Die Schwachstellenbehebung stellt den kritischsten Schritt des Schwachstellen-Managements dar. Leider fallen hier viele Programme durch. Eine Lösung sollte die notwendige – aber oft schwer zu erreichende – Zusammenarbeit zwischen Sicherheits-, IT- und Entwicklungsteams fördern, damit Schwachstellen möglichst rasch behoben werden.

Patching mit Automatisierung und Einbindung der IT

Der Patching-Prozess erfordert meist viel Kommunikation zwischen den Sicherheits- und IT-Teams. Automatisierung kann dazu beitragen, Sie von ständig wiederkehrenden Arbeitsschritten zu entlasten, indem eine Integration in bestehende IT-Tools und Workflows wie Ticketing-Systeme und Patch-Management-Software vorgenommen wird.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Bietet die Lösung Integrationen für Ihre bestehenden Sicherheits- und IT-Lösungen, um den Patching-Prozess zu straffen?

Automatisierte Quarantäne

Nicht alle Schwachstellen können unmittelbar bei Erkennung behoben werden. Durch die automatisierte Implementierung von Gegenmaßnahmen können Sie die Gefährdung durch diese Schwachstellen über bestehende Netzwerk- und Endpunktsysteme vorübergehend (oder dauerhaft) verringern.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Kann die Lösung auf Ihre bestehenden Tools wie Firewall, Network Access Control (NAC), Endpunkterkennung und Incident Response zugreifen, um Bedrohungen einzudämmen?
- Unterstützt die Lösung die vollständige Isolierung von Assets oder einzelner Dienste (Quarantäne)?

Planung der Schwachstellenbehebung

Wenn Sie Sicherheitslücken festgestellt und priorisiert haben, müssen diese auch behoben werden. Legen Sie für einen effizienten Remediation-Prozess Reports zugrunde, die die am besten umsetzbaren und für die Minderung des Gesamtrisikos wirkungsvollsten Schritte aufzeigen. Diese sollten die erforderlichen Maßnahmen sowie Angaben zu der benötigten Zeit und den zugehörigen Patches, Downloads und Referenzen beinhalten.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Stellt die Lösung priorisierte Remediation-Pläne bereit, die Anweisungen auf der IT-Betriebsebene beinhalten?

Rollenzuweisung

Von wem die Schwachstellenbehebung durchgeführt wird, ist u. a. davon abhängig, wo sich das Asset befindet, welche Funktion dieses hat und wer dafür verantwortlich ist. Je länger der Zeitraum zwischen der Feststellung des Risikos und der Zuweisung von Gegenmaßnahmen ist, desto länger bleibt das entsprechende Asset ungeschützt. Remediation-Pläne sollten automatisch an den zuständigen Mitarbeiter gesendet werden.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Ist die Lösung imstande, nach jedem Scanvorgang automatisch Aufgaben zur Schwachstellenbehebung entsprechend dem Geschäftskontext zuzuweisen?

Ergebnisse der Schwachstellenbehebung

Die Schwachstellenbehebung stellt einen kontinuierlichen Prozess dar, der stets verbessert werden kann. Eine gute Schwachstellen-Management-Lösung sollte Sie dabei unterstützen, Schwächen in Ihrem Remediation-Workflow zu identifizieren, damit Sie potentiellen Problemen vorbeugen und Ihren Fortschritt besser nachvollziehen können.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Ermöglicht Ihnen die Lösung, den Fortschritt der Schwachstellenbehebung zu verfolgen?
- Stellt die Lösung Angaben bezüglich effizienter (oder ineffizienter) Punkte im Remediation-Prozess bereit?

Reporting

Im Zuge von Schwachstellenscans ergibt sich eine überwältigende Menge an Informationen. Daher ist es entscheidend, die wirklich wichtigen Informationen zu ermitteln und diese klar, kompakt und in einem verwertbaren Format darzustellen.

Konsolidiertes Reporting

Durch das Zusammenführen der Daten aller Scan-Engines und Agents für das Reporting können Sie die Priorisierung und Schwachstellenbehebung im gesamten Netzwerk zentral verwalten und das gesamte Sicherheitsrisiko sowie Compliance analysieren. Die Lösung sollte Schwachstellen, Konfigurationen, die Einhaltung von Richtlinien und andere Systeminformationen (z. B. installierte Anwendungen) in einer zentralen, einheitlichen Oberfläche anzeigen.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Stellt die Lösung eine einheitliche Ansicht der Schwachstellen, Konfigurationen und Systeminformationen bereit?

Report-Templates und -Anpassung

Ein effektiver Ansatz für die Schwachstellenpriorisierung erfordert zusätzliche Informationen über Ihre Assets, u. a. wo sich diese befinden, welche Funktion sie haben, wer dafür verantwortlich ist und welche relative Bedeutung ihnen zukommt. Anhand dieser kontextbezogenen Informationen können Sie geschäftskritische Systeme und Daten für die Remediation priorisieren. Die Lösung muss darüber hinaus in der Lage sein, den Risiko-Score automatisch aufgrund der Kritikalität des jeweiligen Assets anzupassen.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Stellt die Lösung Funktionen für kontextreiches Reporting bereit?

Assets- und Schwachstellenfilter

Welche Systeme könnten von einer neuen Zero-Day-Schwachstelle betroffen sein? Mithilfe von Assets- und Schwachstellenfiltern können Sie komplexe Fragestellungen beantworten und sich schnell einen Überblick über die Risiken in Ihrem Unternehmen verschaffen. Sie müssen Schwachstellen in Reports nach Schweregrad, Plattform, Software, Protokoll, Schwachstellenart und betroffenen Diensten filtern können.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Unterstützt die Lösung das Filtern von Assets und Schwachstellen nach Attributen, Kategorie und Schweregrad?

Assetgruppen

Die Assets müssen sich in der Lösung nach technischen Attributen gruppieren lassen, beispielsweise nach dem installierten Betriebssystem oder benutzerdefinierten Attributen wie dem Standort, dem Besitzer oder der Kritikalität. Suchen Sie nach einer Lösung, mit der Sie diese Gruppen auf der Basis von neu erkannten Assets und Assetinformationen dynamisch aktualisieren können. Die Lösung sollte es zudem ermöglichen, Reports auf Basis dieser Gruppen zu erstellen.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Muss manuell überprüft werden, ob Schwachstellen behoben wurden?

Validierung der Remediation

Wenn das IT-Team die Behebung einer Schwachstelle meldet, muss die Lösung automatisch überprüfen können, ob das Problem tatsächlich gelöst wurde. Falls die Remediation-Maßnahmen nicht erfolgreich sind, muss die Lösung den Task in der Ticketing-Lösung des IT-Teams automatisch neu öffnen.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Muss manuell überprüft werden, ob Schwachstellen behoben wurden?

Dashboards

Schwachstellendaten liefern zahlreiche Informationen über die in Ihrem Netzwerk bestehenden Risiken, jedoch kann die Visualisierung und Remediation auf Basis dieser Informationen bisweilen eine Herausforderung darstellen. Mithilfe von Dashboards können die Techniker und Nicht-Techniker des Teams auf einen Blick feststellen, wie sich die Schwachstellen auf die Sicherheitslage auswirken. Effektive Dashboards lassen sich einfach anpassen. Sie bieten einfache Abfragemöglichkeiten und Aktualisierungen in Echtzeit, sobald neue Informationen ermittelt werden.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Stellt die Lösung benutzerfreundliche und leicht anpassbare Dashboards bereit?

Datenbankabfragen

Bisweilen müssen Sie eventuell eine weitergehende Analyse der Schwachstellen- und Assetdaten durchführen, die an die speziellen Anforderungen Ihres Unternehmens bzw. Sicherheitsteams angepasst ist. Die Lösung sollte direkte SQL-Abfragen in Bezug auf das Reporting-Datenmodell unterstützen und die Ergebnisse in einem Format ausgeben, das für die Erstellung von Pivot-Tabellen, Diagrammen und Kurven geeignet ist.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Gestattet die Lösung die Ausführung von SQL-Abfragen auf die gesammelten Daten?

Compliance- und Konfigurationsanalyse

Unsichere Konfigurationen („Fehlkonfigurationen“) und fehlende Gegenmaßnahmen stellen eine der wichtigsten Risikoquellen dar, weshalb einige Schwachstellen-Management-Lösungen auch die Durchführung von Scanvorgängen in Bezug auf Konfigurationen, Gegenmaßnahmen und Richtlinieneinhaltung ermöglichen.

Compliance-Analyse

Viele Sicherheitsstandards und -vorschriften schreiben die Durchführung einer Schwachstellen-Management vor, beispielsweise die PCI-DSS-Standards (Payment Card Industry Data Security Standards). Vorgefertigte Scan- und Reportvorlagen machen die Einhaltung dieser Richtlinien einfacher und effizienter. Um die Einhaltung der PCI-Standards zu gewährleisten, sollte es sich bei dem Lösungsanbieter um einen Approved Scanning Vendor (ASV) handeln.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Stellt die Lösung Vorlagen für die Compliance-Analyse bereit?
- Handelt es sich um ein separat installiertes Produkt oder Modul, für welches Zusatzkosten anfallen?

Konfigurationsanalyse

Die sichere Konfiguration Ihrer Systeme gemäß den Benchmarks und Best Practices der Branche stellt einen wichtigen Baustein einer vollwertigen Lösung für das Schwachstellen-Management dar. Konfigurations- und Compliance-Analysen sollten in Verbindung mit dem Schwachstellen-Management erfolgen, wobei die Ergebnisse in einer einheitlichen Oberfläche zu präsentieren sind. Darüber hinaus müssen die Konfigurationsrichtlinien vollständig über die Benutzeroberfläche anpassbar sein, um Ihren spezifischen Anforderungen gerecht zu werden.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Führt die Lösung Konfigurations- und Compliance-Analysen in nur einem Scanvorgang mit einheitlichem Reporting durch?

Überprüfung der Gegenmaßnahmen

Die meisten Unternehmen investieren viel Zeit und Ressourcen in die Implementierung von Gegenmaßnahmen zum Schutz vor den aktuellen Bedrohungen. Indem Sie überprüfen, ob diese Gegenmaßnahmen optimal implementiert wurden und wie effektiv diese mit Hinblick auf die Best Practices der Branche sind, können Sie etwaige Lücken in Ihrem Sicherheitsprogramm identifizieren. Suchen Sie nach einer Schwachstellen-Management-Lösung, die die Wirksamkeit Ihrer Maßnahmen überwacht.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Überwacht die Lösung die Implementierung und die Wirksamkeit Ihrer Gegenmaßnahmen?

Administration

Rollenbasierter Zugriff

Die verschiedenen Benutzergruppen in Ihrem Unternehmen benötigen eventuell unterschiedliche Berechtigungsstufen für das Scannen von Daten. Daher sollte eine rollenbasierte Zugriffssteuerung (role-based access controls, RBAC) vordefinierte Rollen, das Ändern oder Hinzufügen neuer Rollen, Berechtigungen für das Ändern von Scan-Konfigurationen, die Assetgruppierung, das Reporting und andere administrative Funktionen unterstützen.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Unterstützt die Lösung den Zugriff auf der Basis vordefinierter bzw. benutzerdefinierter Rollen?

Exceptions-Management

Gelegentlich werden Sie auf Schwachstellen stoßen, die entweder nicht behoben werden können oder als für das Unternehmen akzeptables Risiko gelten. Der Genehmigungsprozess einer Ausnahme sollte automatisiert werden, um eine einfache Überprüfung und Verwaltung zu ermöglichen. Sie müssen auch in der Lage sein, Ausnahmen auf Instanz-, Asset- und Scangruppen-Ebene bzw. auf globaler Ebene zu erstellen und Gründe für die Ausnahme hinzuzufügen.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Stellt die Lösung einen Approval-Workflow für Schwachstellenausnahmen bereit?

Updates der Anwendung

Regelmäßige Updates sorgen dafür, dass Sie die neuesten Funktionen und Performanceverbesserungen nutzen können. Sie müssen zwischen automatischen und manuellen Updates wählen können. Zudem sollte ein Prozess für die Aktualisierung der Anwendung in Offline-Umgebungen vorhanden sein.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Unterstützt die Lösung automatische, manuelle und Offline-Updates?

Updates der Schwachstelleninformationen

Um mit der sich ständig verändernden Bedrohungslandschaft Schritt zu halten, benötigen Sie eine Schwachstellen-Management-Lösung, die häufige Updates für neue Schwachstellen zur Verfügung stellt. Im Zusammenhang mit kritischen Updates zu Schwachstellen, beispielsweise Schwachstellen im Rahmen des Microsoft Patchday, sollte der Anbieter Service Level Agreements (SLA) für garantierte Aktualisierungsintervalle anbieten.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Gibt es regelmäßige Updates für neue Schwachstellen, einschließlich eines damit verbundenen SLA für kritische Schwachstellen?

Integration

Virtuelle und Cloud-Umgebungen

Sie können Ihre Schwachstellen-Management-Lösung in virtuelle und Cloud-Plattformen wie VMware, Amazon Web Services (AWS) und Microsoft Azure integrieren, um die dynamische Erkennung und Analyse von Assets in diesen Umgebungen zu ermöglichen. Suchen Sie nach einem Lösungsanbieter, der vom Anbieter der virtuellen bzw. Cloud-Plattform zertifiziert wurde und der vorgefertigte Integrationen für die schnelle und einfache Einrichtung ohne großen Verwaltungsaufwand anbietet.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Unterstützt die Lösung die Integration in Ihre virtuelle bzw. Cloud-Umgebung?

Andere IT-Sicherheitslösungen

Viele Schwachstellen-Management-Lösungen stellen vorgefertigte Integrationen für andere Sicherheitslösungen in Ihrer Umgebung bereit, u. a. für Netzwerktopologie-Tools, IDS/IPS-, IT-GRC- und SIEM-Lösungen. Diese Integrationen bieten eine zentralisierte Berichterstattung und Verwaltung sowie die Möglichkeit, zusätzliche Kontextinformationen zu Assets zu korrelieren, um die Warnungsgenauigkeit zu erhöhen und Fehlalarme zu vermeiden.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Unterstützt die Lösung die Integration in andere Sicherheitslösungen?

Ticketing-Systeme

Wenn Ihr Unternehmen bereits ein Ticketing-System wie Atlassian Jira oder ServiceNow einsetzt, können Sie dank Technologieintegrationen Ihren bestehenden Workflow für die Schwachstellenbehebung nutzen. Dies ermöglicht es Ihrem IT-Team, Probleme schnell zu lösen oder zur besseren Nachverfolgung zu eskalieren.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Unterstützt die Lösung die Integration in Ticketing-Systeme des Unternehmens?

Automatisierungs- und Orchestrierungstools

Tools für die Sicherheitsautomatisierung und -orchestrierung entpuppen sich mehr und mehr als das Bindeglied, das Sicherheitsprogramme zusammenhält. Stellen Sie bei der Evaluierung von neuen Schwachstellen-Management-Tools sicher, dass sich die Lösung in Ihre Automatisierungs- und Orchestrierungslösungen integrieren lässt.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Lässt sich die Lösung im Zusammenhang mit erweiterten Anwendungsfällen in robuste Automatisierungs- und Orchestrierungslösungen integrieren?

RESTful API

Holen Sie das Maximum aus Ihren bestehenden Sicherheitsinvestitionen heraus: Wenn Sie eigene benutzerdefinierte Integrationen oder Workflows erstellen möchten, stellen Sie sicher, dass Ihre Schwachstellen-Management-Lösung ein RestFul API gemäß der Spezifikation OpenAPI v2 beinhaltet, um die Flexibilität und Interoperabilität zu gewährleisten.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Stellt die Lösung ein bidirektionales, öffentliches und sprachunabhängiges API bereit?
- Sind mit der Verwendung des API zusätzlichen Kosten oder Gebühren verbunden?

Anbieter

Marktanalyse

Wählen Sie einen bekannten und in der Branche bewährten Anbieter. Marktforschungsunternehmen wie Gartner und Fachpublikationen wie das SC Magazine veröffentlichen Analysen und Vergleiche von Schwachstellen-Management-Lösungen (auch als VRM-Lösung bezeichnet: Vulnerability Risk Management). Achten Sie auf einen Lösungsanbieter, der in den letzten Jahren durchgehend als branchenführender Anbieter bewertet wurde.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Sind entsprechende Bewertungen oder Empfehlungen von Marktanalysten aus den letzten fünf Jahren verfügbar?

Unternehmensfokus

Wählen Sie für eine Best-of-Breed-Lösung einen Anbieter, der das Schwachstellen-Management als Kernangebot ins Zentrum stellt und nicht nur als reine Erweiterung seines Portfolios betrachtet. Der Anbieter sollte in diesem Bereich kontinuierlich Investitionen tätigen sowie Innovationen vorantreiben und in der Lage sein, seine Produkt-Roadmap und seine Vision für zukünftige Weiterentwicklungen zu artikulieren.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Fanden im Verlauf des letzten Jahres größere Innovationen oder Weiterentwicklungen der Lösung statt?

Kundenzufriedenheit

Kundensupport ist nicht gleich Kundensupport. Suchen Sie nach Anbietern, die ein zweistufiges Supportmodell anbieten. Der Support sollte rund um die Uhr an sieben Tagen in der Woche verfügbar sein, damit sichergestellt ist, dass Ihre Probleme direkt vom ersten Ansprechpartner gelöst werden. Holen Sie Informationen oder Referenzen von anderen Kunden des Lösungsanbieters ein, die in einem ähnlichen geschäftlichen Bereich tätig sind.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Welche Kundenzufriedenheitswerte erzielt die Lösung und wie steht es mit der „First Call Resolution“-Quote?

Schulung und Zertifizierung

Formale Produktschulungen sowie eine Zertifizierung können Ihnen dabei helfen, das Produkt optimal zu nutzen, den Zeitaufwand für die Problembehebung zu verringern und die Produktivität zu steigern. Zertifizierungen helfen Ihrem Unternehmen auch dabei, potenzielle Mitarbeiter zu identifizieren, die sich schneller in die Lösung für das Schwachstellen-Management einarbeiten können.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Bietet der Anbieter Produktschulungen oder Zertifizierungen vor Ort oder online an?

Bereitstellungsservices

Mithilfe professioneller Dienstleistungen können Sie den ROI maximieren, indem Sie Implementierung, Scan-Konfiguration, Prozesse und Berichterstattung den Best Practices entsprechend optimieren lassen. Sie können zudem Unterstützung beim Erstellen von benutzerdefinierten Skripten, Schnittstellen und Integrationen entsprechend den spezifischen Anforderungen Ihres Unternehmens erhalten.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Bietet der Anbieter Dienstleistungen und Best Practices für die Implementierung und Optimierung an?

Tools für das Anwendungs- und Benutzer-Schwachstellen-Management

Die Analyse von Netzwerk-Schwachstellen stellt nur einen Mosaikstein einer modernen Anwendung für das Schwachstellen-Management dar. Der Anbieter, den Sie als Partner wählen, sollte Lösungen bereitstellen, die Sie zudem bei der Analyse von Anwendungs- und Benutzer-Schwachstellen unterstützen. Die Lösungen sollten integriert sein, damit ein einheitliches Schwachstellen-Management-Programm geschaffen werden kann.

FRAGEN SIE DEN LÖSUNGSANBIETER

- Stellt der Anbieter Produkte für das Anwendungs- und Benutzer-Schwachstellen-Management bereit?
- Handelt es sich um integrierte Produkte?

02 Weitere Erwägungen

Preisgestaltung

Die Preise und Lizenzen für Schwachstellen-Management-Lösungen können stark variieren. Einige Anbieter bieten eine unbefristete Lizenz, wobei dann anschließend laufende Gebühren für Wartung und Support anfallen. Andere Anbieter verwenden ein Abo-Modell, bei dem Sie die Gesamtkosten der Lösung in Form einer Jahres- oder Monatsgebühr entrichten. Berücksichtigen Sie bei der Berechnung des ROI die Gesamtbetriebskosten sowie eventuelle versteckte Kosten für Assets oder Module, die Sie möglicherweise im Laufe der Zeit hinzufügen müssen. Häufig wird die Inanspruchnahme von Schulungs- und Implementierungsdienstleistungen empfohlen, um Schwachstellen-Management-Programme bestmöglich auszunutzen. Daher sollten diese Kosten ebenfalls berücksichtigt werden.

Einige Open-Source-Anwendungen bzw. Tools aus dem Low-End-Bereich stellen nur einen Schwachstellenscanner mit beschränkter Funktionalität zu einem sehr geringen Einstiegspreis oder sogar kostenfrei bereit. Sie werden jedoch feststellen, dass die laufenden Kosten für die Pflege eines solchen Schwachstellen-Management-Programms viel höher sind, da die Verwaltung, Berichterstattung und Anpassung viel zeit- und ressourcenaufwändiger ist.

Managed Services

Die ideale Schwachstellen-Management-Lösung unterstützt Ihr Team dabei, effizienter zu arbeiten. Sie sollte keine (wertvolle) Zeit kosten. In einigen Fällen ist Ihr Team – selbst bei Verfügbarkeit der besten Technologien – nicht in der Lage, ein Schwachstellen-Management-Programm auszuführen. Wenn das der Fall ist, achten Sie auf Anbieter mit einem Managed-Services-Angebot. Der Managed Service für das Schwachstellen-Management muss auf einem Schwachstellen-Management-Tool aufsetzen, das den in diesem Ratgeber dargelegten Kriterien und den von Ihrem Unternehmen festgelegten Kriterien entspricht.

Kennzahlen für den Erfolg

Erweist Ihr Schwachstellen-Management-Programm die gewünschte Wirksamkeit? Nachfolgend sind einige Kennzahlen aufgeführt, anhand derer Sie den Fortschritt verfolgen sowie verbesserungswürdige Bereiche ermitteln können:

- Anzahl der gefundenen und behobenen Schwachstellen
- Dauer bis zur Erkennung und Behebung von risikoreichen Schwachstellen
- Anzahl der zuvor unbekannten Assets/ Dienste/Anwendungen, die erkannt wurden
- Zeit- und Kostenaufwand für den Abschluss des Priorisierungs- und Schwachstellenbehebungsprozesses
- Grad der Fehlerreduzierung bei Tasks, die an die IT übergeben wurden
- Zeit- und Kostenaufwand für die Vorbereitung auf Compliance-Audits
- Prozentsatz der erfolgreich bestandenen Compliance-Audits
- Für Verwaltungsaufgaben und Berichterstattung aufgewendete Zeit
- Höhe des Risikos und dessen Veränderung über die Zeit

Ein Schwachstellen-Management-Tool für Ihre moderne IT-Umgebung

Und hier noch einige Anmerkungen in eigener Sache:

InsightVM von Rapid7 nutzt die Insight-Plattform und die Vorleistung unseres preisgekrönten Produkts Nexpose, um Sie besser für die Herausforderungen des modernen Schwachstellen-Managements zu wappnen. Mit InsightVM erhalten Sie vollständige Transparenz über Ihr komplexes IT-Umfeld. Außerdem können Sie Risiken anhand von Angreiferanalysen priorisieren und Gegenmaßnahmen mit flexiblen Sicherheitsverfahren ergreifen, damit in Ihren Cloud-, Remote- und Container-Infrastrukturen sowie in Ihren virtuellen und lokalen Umgebungen nichts verborgen bleibt.

„Rapid7 hat schon heute das Schwachstellen-Management der Zukunft umgesetzt.“

– The Forrester Wave™: Schwachstellen- und Risikomanagement (VRM), Q1 2018

Mithilfe der modernen Analyse-, Automatisierungs- und Orchestrierungstechnologie von InsightVM können Sie Schwachstellen in Echtzeit erkennen und schnell deren Schweregrad in Ihrem speziellen Unternehmenskontext bestimmen, um eine besser verwertbare Priorisierung zu erreichen. Zudem wird die Schwachstellenbehebung bzw. -eindämmung durch die Integration in die bestehenden Workflows und Tools Ihres IT-Teams vereinfacht und automatisiert – dank der umfassenden Integrationen von InsightVM ein problemloser Prozess.

Um InsightVM in Ihrer Infrastruktur zu testen, melden Sie sich für eine kostenlose 30-Tage-Testversion an:

www.rapid7.com/try/insightvm

Über Rapid7

Rapid7 (Nasdaq: RPD) bringt Unternehmen mit der Insight-Cloud voran, die auf Sichtbarkeit, Analytik und Automatisierung setzt. Unsere Lösungen vereinfachen komplexe Sachverhalte und ermöglichen es Sicherheitsteams, effektiver mit den IT- und Entwicklungsteams daran zu arbeiten, Sicherheitslücken zu schließen, schädliche Aktivitäten zu erkennen, Angriffe zu untersuchen und abzuwehren sowie Abläufe zu automatisieren. Kunden rund um die Welt bauen auf die Technologien, die Dienstleistungen und die Forschung von Rapid7, um die Sicherheit zu erhöhen und ihre Unternehmen sicher voranzubringen. Weitere Informationen finden Sie auf unserer Website. Besuchen Sie außerdem unseren Blog oder folgen Sie uns auf Twitter.

Weitere Informationen über Rapid7 und die Beteiligung an unserer Bedrohungsforschung finden Sie unter

www.rapid7.com.