Schwachstellenmanagement und Schwachstellenscans

Der Schwachstellenm Prozess: Scannen, Priorisierung und Behebung

Kontinuierliche Identifizierung und Bewertung von Risiken in Ihrer Umgebung

Was sind Schwachstellenma und Schwachstellensca

Schwachstellenmanagement (/de/solutions/vulnerability-management/) ist der Prozess, mit dessen Hilfe Sicherheitslücken in Systemen und in der auf diesen Systemen laufenden Software erkannt, bewertet, behandelt und gemeldet werden. Dies, zusammen mit der Implementierung anderer Sicherheitstaktiken, ist für Unternehmen entscheidend, um mögliche Bedrohungen zu priorisieren und ihre „Angriffsfläche" zu minimieren.

Sicherheitslücken (/de/cybersecurity-grundlagen/vulnerabilities-exploits-threats/) wiederum bezeichnen technische Schwächen, die es Angreifern ermöglichen, ein Produkt und die darauf befindlichen Informationen zu kompromittieren. Dieser Prozess muss kontinuierlich durchgeführt werden, um mit im Laufe der Zeit neu zu Netzwerken hinzugefügten Systemen, Änderungen an Systemen sowie der Entdeckung neuer Schwachstellen Schritt zu halten.

GRUNDLAGEN

Schwachstellen-Risikomanagement

Abschnitt auswählen

Software für das Schwachstellenmanagement kann dazu beitragen, diesen Prozess zu automatisieren. Dabei werden ein Schwachstellenscanner (/de/products/nexpose/download/) und manchmal auch Endpoint-Agents genutzt, um eine Vielzahl von Systemen in einem Netzwerk zu inventarisieren und Schwachstellen darin zu erkennen. Sobald Schwachstellen erkannt werden, muss das Risiko, das sie darstellen, in verschiedenen Kontexten bewertet werden, um zu entscheiden, wie am besten mit ihnen umzugehen ist. So kann beispielsweise eine Schwachstellenvalidierung ein wirksamer Weg sein, die wirkliche Schwere einer Schwachstelle in ihrem Kontext zu ermitteln.

Was ist der Unterschied zwischen Schwachstellenmanager und Schwachstellenbewertu

Im Allgemeinen ist eine Schwachstellenbewertung (/solutions/vulnerability-assessment/) ein Teil des kompletten

Schwachstellenmanagementsystems. Normalerweise führen Unternehmen mehrere Schwachstellenbewertungen durch, um mehr Informationen für ihren Maßnahmenplan für das Schwachstellenmanagement zu erhalten.

Der Schwachstellenmanager Prozess kann in die folgenden vier Schritte unterteilt werden:

- 1) Schwachstellen erkennen
- 2) Schwachstellen bewerten
- 3) Schwachstellen behandeln
- 4) Schwachstellen melden

Schritt 1: Schwachstellen erkennen

Das Herzstück einer typischen Lösung für das Schwachstellenmanagement (/de/products/insightvm/)ist ein Schwachstellenscanner. Der Scan besteht aus vier Phasen:

1. Scannen von über das Netzwerk zugänglichen Systemen, indem sie angepingt werden oder ihnen TCP/UDP-Pakete geschickt werden
2. Identifizieren von offenen Ports und Diensten, die auf den gescannten Systemen laufen
3. Wenn möglich, Remote-Anmeldung an den

Systemen, um detaillierte Systeminformationen zu sammeln
4. Systeminformationen mit bekannten Schwachstellen abgleichen

Schwachstellenscanner können eine Vielzahl von Systemen in einem Netzwerk erkennen, wie Laptops und Desktops, virtuelle und physische Server, Datenbanken, Firewalls, Switches, Drucker usw. Identifizierte Systeme werden auf verschiedene Attribute untersucht: Betriebssystem, offene Ports, installierte Software, Benutzerkonten, Dateisystemstruktur, Systemkonfigurationen und vieles mehr. Diese Informationen werden dann verwendet, um bekannte Schwachstellen mit den gescannten Systemen zu verknüpfen. Um diesen Zusammenhang herstellen zu können, nutzen Schwachstellenscanner eine Schwachstellendatenbank, die eine Liste mit veröffentlichten Schwachstellen enthält.

Die ordnungsgemäße Konfiguration von Schwachstellenscans ist ein wichtiger Bestandteil einer Schwachstellenmanagement-Lösung. Schwachstellenscanner können manchmal Unterbrechungen bei den von ihnen gescannten Netzwerken und Systemen herbeiführen. Wenn während der Spitzenzeiten eines Unternehmens nicht genug Netzwerkbandbreite zur Verfügung steht,

sollten Schwachstellenscans außerhalb der normalen Geschäftszeiten durchgeführt werden.

Sollten einige Systeme in einem Netzwerk instabil werden oder während des Scanvorgangs auf unvorhergesehene Weise reagieren, müssen sie möglicherweise von den Schwachstellenscans ausgeschlossen werden oder die Scans müssen nachjustiert werden, damit sie weniger Störungen verursachen. Adaptives Scannen (/de/products/insightvm/features/lightweight-endpoint-agent/) ist ein neuer Ansatz zur weiteren Automatisierung und Vereinfachung von Schwachstellenscans bei Veränderungen im Netzwerk. Wenn beispielsweise ein neues System erstmals mit einem Netzwerk verbunden wird, wird ein Schwachstellenscanner nur dieses eine System so schnell wie möglich scannen, anstatt auf den wöchentlichen oder monatlichen Scan des gesamten Netzwerks zu warten.

Schwachstellenscanner sind jedoch nicht mehr der einzige Weg, um Schwachstellendaten eines Systems zu sammeln. Endpoint-Agents ermöglichen Schwachstellenmanagement-Lösungen, um kontinuierlich Schwachstellendaten von Systemen zu sammeln, ohne dass Netzwerk-Scans durchgeführt werden müssen. Dies hilft

Unternehmen dabei, aktuelle Daten über Systemschwachstellen vorzuhalten, ist jedoch abhängig davon, ob beispielsweise die Laptops der Mitarbeiter mit dem Netzwerk des Unternehmens oder dem Heimnetzwerk der Mitarbeiter verbunden sind.

Unabhängig davon, wie eine Schwachstellenmanagement-Lösung diese Daten sammelt, können diese verwendet werden, um Berichte, Metriken und Dashboards für viele unterschiedliche Arten von Zielgruppen zu erstellen.

Schritt 2: Schwachstellen bewerten

Nachdem Schwachstellen erkannt wurden, müssen sie bewertet werden, damit die Risiken, die von ihnen ausgehen, angemessen und entsprechend der Risikomanagementstrategie des Unternehmens behandelt werden können. Schwachstellenmanagement-Lösungen bieten verschiedene Risikobewertungen und Scores für Schwachstellen, wie z. B. CVSS-Scores (Common Vulnerability Scoring System). Diese Ergebnisse geben Unternehmen Auskunft darüber, auf welche Schwachstellen sie sich zuerst konzentrieren sollten. Jedoch hängt das echte Risiko einer jeden Schwachstelle von einigen anderen Faktoren ab, die über diese standardisierten Risikobewertungen und Scores hinausgehen.

Hier sind einige Beispiele für zusätzliche Faktoren, die bei der Bewertung von Schwachstellen berücksichtigt werden sollten:

- Ist diese Schwachstelle echt oder ein falsch positives Ergebnis?
- Könnte jemand diese Schwachstelle direkt aus dem Internet ausnutzen?
- Wie schwer ist es, diese Schwachstelle auszunutzen?
- Gibt es für diese Schwachstelle einen bekannten, veröffentlichten Exploit-Code?
- Welche Auswirkungen hätte es für das Geschäft, wenn diese Schwachstelle ausgenützt würde?
- Sind noch andere Sicherheitsmaßnahmen vorhanden, die die Wahrscheinlichkeit, dass diese Schwachstelle ausgenutzt wird und/oder deren Auswirkungen reduzieren?
- Wie alt ist die Schwachstelle/wie lange ist sie bereits im Netzwerk?

Wie jedes Sicherheitstool sind Schwachstellenscanner nicht perfekt. Ihre falsch positive Quote bei der Erkennung von Schwachstellen ist zwar niedrig, aber dennoch größer als null. Die Durchführung von Schwachstellen-Validierungen mittels Penetrationstest-Tools (/de/products/metasploit/) und -Verfahren trägt dazu bei, falsch positive Ergebnisse auszumerzen, damit Unternehmen ihre Aufmerksamkeit auf den Umgang mit echten Schwachstellen richten können. Die Ergebnisse von Schwachstellen-Validierungen

oder umfangreichen Penetrationstests sind häufig eine aufschlussreiche Erfahrung für Unternehmen, die überzeugt waren, dass sie ausreichende Sicherheitsvorkehrungen getroffen hatten oder dass die Schwachstelle gar nicht *so* riskant wäre.

Schritt 3: Schwachstellen beheben

Sobald eine Schwachstelle bestätigt und als Risiko eingestuft wurde, besteht der nächste Schritt darin, gemeinsam mit den beteiligten Akteuren im Unternehmen oder Netzwerk Priorisierungen vorzunehmen, wie die Schwachstelle behandelt werden soll. Es gibt verschiedene Möglichkeiten, Schwachstellen zu behandeln, einschließlich:

- **Beseitigung:** Vollständige Behebung oder Patchen einer Schwachstelle, so dass sie nicht ausgenutzt werden kann. Dies ist die ideale Vorgehensweise, die Unternehmen anstreben.
- **Schadensbegrenzung:** Verringerung der Wahrscheinlichkeit und/oder Auswirkungen, die durch Ausnutzung einer Schwachstelle entstehen können. Dies ist manchmal notwendig, wenn ein entsprechender Fix oder Patch für die identifizierte Schwachstelle noch nicht zur Verfügung steht. Diese Option sollte normalerweise nur verwendet werden, um Zeit für das Unternehmen bis zur endgültigen Beseitigung der Schwachstelle zu gewinnen.

- **Akzeptanz:** Keine Maßnahmen ergreifen, um die Wahrscheinlichkeit/Auswirkung, dass eine Schwachstelle ausgenutzt wird, zu beheben oder anderweitig zu reduzieren. Dies ist typischerweise gerechtfertigt, wenn eine Schwachstelle als ein geringes Risiko eingestuft wird, und die Kosten für die Behebung der Schwachstelle wesentlich höher sind als die Kosten, die einem Unternehmen entstehen, sollte die Schwachstelle ausgenutzt werden.

Schwachstellenmanagement-Lösungen liefern empfohlene Methoden für die Beseitigung von Schwachstellen. Gelegentlich ist eine empfohlene Methode nicht die optimale Lösung zur Beseitigung einer Schwachstelle. In diesen Fällen müssen ein Sicherheitsteam, die Systemverantwortlichen und Systemadministratoren des Unternehmens die richtige Vorgehensweise festlegen. Manchmal kann die Beseitigung ganz einfach durch Anwendung eines sofort verfügbaren Software-Patches erfolgen, ein anderes Mal ist der komplexe Austausch einer Reihe von physischen Servern im Netzwerk eines Unternehmens erforderlich.

Nach Abschluss der Beseitigungsmaßnahmen bietet es sich an, einen weiteren Schwachstellenscan durchzuführen, um sicher zu gehen, dass die Schwachstelle vollständig beseitigt wurde.

Allerdings müssen nicht alle Schwachstellen behoben werden. Wenn beispielsweise der Schwachstellenscanner eines Unternehmens Schwachstellen im Adobe Flash Player auf den Firmencomputern erkannt hat, das Unternehmen jedoch die Verwendung des Adobe Flash Players in Web-Browsern und anderen Client-Anwendungen vollständig deaktiviert hat, könnten diese Schwachstellen durch eine kompensierende Kontrollmaßnahme als ausreichend entschärft angesehen werden.

Schritt 4: Schwachstellen melden

Die Durchführung regelmäßiger und kontinuierlicher Schwachstellenbewertungen (/solutions/vulnerability-assessment/) erlaubt es Unternehmen, im Laufe der Zeit die Geschwindigkeit und die Effizienz ihres Schwachstellenmanagement-Programms zu verstehen. Schwachstellenmanagement-Lösungen besitzen normalerweise mehrere Optionen für den Export und die Visualisierung der in Schwachstellenscans gesammelten Daten mittels einer Vielzahl von anpassbaren Berichten und Dashboards. Dies erleichtert IT-Teams nicht nur das Verständnis dessen, welche Beseitungsverfahren ihnen helfen, den größten Teil der Schwachstellen mit möglichst geringem Aufwand zu beheben oder unterstützt Sicherheitsteams dabei,

Schwachstellentrends in verschiedenen Teilen ihres Netzwerks zu überwachen, sondern es hilft Unternehmen auch bei der Einhaltung von Compliance- und regulatorischen Anforderungen (/fundamentals/compliance-regulatory-frameworks/).

Durch Schwachstellenmanagement Angreifern immer einen Schritt voraus sein

Bedrohungen und Angreifer ändern sich ständig, genauso wie Unternehmen ständig neue mobile Geräte, Cloud-Dienste, Netzwerke und Anwendungen in ihre Umgebung einfügen. Bei jeder Änderung besteht das Risiko, dass in Ihrem Netzwerk ein neues Loch geöffnet wird, das es Angreifern ermöglicht, sich Zutritt zu verschaffen und mit Ihren Schätzen zu verschwinden.

Jedes Mal, wenn Sie eine neue Partnerschaft eingehen, einen neuen Mitarbeiter, Mandanten oder Kunden gewinnen, eröffnen Sie nicht nur neue Chancen für Ihr Unternehmen, sondern Sie setzen es auch neuen Bedrohungen aus. Ihr Unternehmen gegen diese Bedrohungen zu schützen, erfordert eine Schwachstellenmanagement-Lösung, die mit diesen Änderungen Schritt halten und sich an alle diese Änderungen anpassen kann. Wenn dies nicht der Fall ist, sind Ihnen die Angreifer immer einen Schritt voraus.

Schwachstellen, Exploits und Bedrohungen (/de/cybersecurity-grundlagen/vulnerabilities-exploits-threats/)

Bezeichnungssysteme für Schwachstellen (/de/cybersecurity-grundlagen/vulnerabilities-exploits-threats/)

Schwachstellenmanagement

Suche

ZURÜCK ZUM ANFANG

(/)

KUNDEN SUPPORT

+1-866-390-8113 (tel:1-866-390-8113)

VERTRIEB

+49 89 97 007 007 (tel:+498997007007)

Brauchen Sie dringend Hilfe bei einem Vorfall?

+1-844-RAPID-IR (tel:18447274347)

PRODUKTE

InsightIDR (/de/products/insightidr/)

InsightVM (/de/products/insightvm/)

InsightCloudSec (/de/products/insightcloudsec/)

InsightAppSec (/de/products/InsightAppSec/)

InsightConnect (/de/products/insightconnect/)

Metasploit (/de/products/metasploit/)

DIENSTLEISTUNGEN

Alle Managed Services (/de/services/managed-services/)

Managed Service für Schwachstellen-Management (/de/services/managed-services/vulnerability-management/)

Managed Detection and Response (/de/services/managed-services/managed-detection-and-response-services/)

Managed Service für Anwendungssicherheit (/de/services/managed-services/managed-appsec/)

Penetrationstest Services (/de/services/security-consulting/penetration-testing-services/)

SUPPORT & RESSOURCEN

Kontaktdaten (/de/kontakt/)

Cybersecurity Grundlagen (/de/cybersecurity-grundlagen/)

Kunden (/de/about/customers/)

Suchen (/de/search/)

(https://www.rapid7.com/de/)

Contact Us