FIREEYE™

LÖSUNGSÜBERSICHT

Einsatzbereiche für Bedrohungsdaten

Analysten für das Schwachstellenmanagement

HERAUSFORDERUNGEN FÜR ANALYSTEN FÜR DAS SCHWACHSTELLENMANAGEMENT

Die Analysten und Administratoren, die für das Aufspüren und Priorisieren von Schwachstellen verantwortlich sind, stehen vor einigen Herausforderungen:

- Softwareanbieter und Sicherheitsberater, aber auch Hacker und Cyberkriminelle, geben ständig Informationen zu neuen Schwachstellen bekannt.
- Viele der Einträge in Schwachstellen-Datenbanken haben hohe Risikobewertungen. 41% der Schwachstellen in der National Vulnerability Database, einem Daten-Repository der US-amerikanischen Regierung, haben beispielsweise einen CVSS-Wert (Common Vulnerability Scoring System) von 7–8, 8–9 oder 9–10. Dadurch ist es sehr schwierig, festzulegen, welche Schwachstellen die höchste Priorität haben.
- Es gibt kaum Informationen, die Unternehmen helfen, festzustellen, welche der Hunderte von Schwachstellen, die jeden Monat bekanntgegeben werden, für eine bestimmte Branche, Region oder das jeweilige Unternehmen relevant sind.
- Es lässt sich nur sehr schwer herausfinden, ob neue Exploits entwickelt wurden, mit denen Hacker neue Schwachstellen ausnutzen, und welche Exploits vermutlich in einem zukünftigen Angriff genutzt werden.

Prinzipiell sollte ein Unternehmen jeden neuen Sicherheits-Patch sofort implementieren. In der Realität verfügen die Unternehmen aber meist nicht über genügend Ressourcen und müssen daher entscheiden, welche Patches zuerst installiert werden sollen.

NIST Special Publication 800-40, Version 3

Analysten für das Schwachstellenmanagement

In den meisten IT-Abteilungen gibt es Analysten, die für das Aufspüren und Priorisieren von Schwachstellen und die Entwicklung von Abwehrmaßnahmen verantwortlich sind. Sie gehören zu Security Operations- oder Security Engineering-Gruppen oder dem Team für das Compliance- und Risikomanagement und zu ihren Aufgaben zählen:

- Sie identifizieren die vom Unternehmen verwendeten Server, Geräte, Endpunkte und Anwendungen und identifizieren potenzielle Schwachstellen.
- Sie ermitteln, welche Schwachstellen eine akute Gefahr für das Unternehmen darstellen und welche nicht so gefährlich sind. Dazu nutzen sie Anhaltspunkte wie den Schweregrad der Schwachstelle, die im Unternehmen genutzten Systeme und Anwendungen, die vorhandenen Abwehrmaßnahmen und Sicherheitslösungen sowie Meldungen, ob die Schwachstelle bereits in anderen Unternehmen ausgenutzt wird.
- Sie unterstützen die Verantwortlichen bei der Auswahl der optimalen Abwehrmaßnahmen.
- Sie kommunizieren mit Auditoren, Risikomanagern und anderen IT-Teams über die Risiken von Schwachstellen, die nicht sofort behoben werden können.

So profitieren Analysten für das Schwachstellenmanagement von Cyberbedrohungsdaten

Analysten für das Schwachstellenmanagement ermitteln mithilfe von Cyberbedrohungsdaten, welche Schwachstellen kritisch sind. Sie helfen, optimale Abwehrstrategien zu finden, und informieren Manager und andere IT-Teams über die Risiken.

Tabelle 1: Einsatzbereiche – Analyst für das Schwachstellenmanagement

Einsatzbereich	Ziel	Erforderliche Bedrohungsdaten
Schwachstellenanalyse	• Klassifizieren der Schwachstellen nach Typ, Quelle und potenziellen Zielen • Ermitteln, welche Schwachstellen bei komplexen Angriffen ausgenutzt werden	• Bedrohungsdatenbank zu Schwachstellen, Hackern, Angriffstechniken und potenziellen Zielen • Bedrohungsanalyseberichte für die Branche oder das Unternehmen
Priorisierung der Schwachstellen	Ermitteln, welche Schwachstellen … • Systeme und Software im Unternehmen betreffen • nicht von vorhandenen Sicherheitsmaßnahmen und -lösungen abgewehrt werden • aktiv von Hackern ausgenutzt werden	• Bedrohungsdatenbank • Untersuchungen zu Angriffsmethoden, die derzeit verwendet werden, und zu Exploit-Kits, die auf Hacker-Websites angeboten werden
Identifizierung von Abwehrmaßnahmen	• Ermitteln von Patches für Schwachstellen • Ermitteln geeigneter Alternativen zu Patches	• Bedrohungsdatenbank mit Empfehlungen für Abwehrmaßnahmen
Kommunikation mit Risikomanagern und Systemadministratoren	• Identifizieren der gefährdeten Systeme, die überwacht werden müssen, bis Abwehrmaßnahmen implementiert sind	• Bedrohungsdatenbank • Bedrohungsanalyseberichte für die Branche oder das Unternehmen

Warum sind Bedrohungsdaten so wichtig?

Verdeutlichung der Relevanz und des Schweregrads einer Schwachstelle

Anhand von Cyberbedrohungsdaten lassen sich die Schwachstellen bestimmten Angreifern, ihren Zielen und ihren Taktiken, Techniken und Prozessen (TTP) zuordnen. Mit diesen Informationen können die Analysten feststellen, welche Schwachstellen für die Systeme und Software im Unternehmen relevant sind und welche wahrscheinlich von Hackern ausgenutzt werden, die in ihrer Branche und Region aktiv sind.

Informationen zu Exploits und Exploit-Kits

Die Wissenschaftler in Unternehmen für Cyberbedrohungsdaten überprüfen Exploits und Exploit-Kits, die im Dark Web von Hackern und Cyberkriminellen angekündigt, besprochen und zum Verkauf angeboten werden. Wenn für eine Schwachstelle ein effektives Exploit-Kit verfügbar ist, steigt die Wahrscheinlichkeit, dass sie in der nahen Zukunft ausgenutzt wird. Diese Informationen helfen den Analysten für das Schwachstellenmanagement bei der Entscheidung, welche Schwachstellen sofort gepatcht oder behoben werden müssen und welche nicht ganz so dringend sind.

Abwehrmaßnahmen

Bedrohungsdatenbanken enthalten auch Angaben zu Patches für bestimmte Schwachstellen. Außerdem werden Abwehrmethoden aufgeführt, die Schutz bieten, falls keine Patches verfügbar sind oder die Bereitstellung zu lange dauern würde. Zu den Abwehrmaßnahmen gehören beispielsweise Regeln für Netzwerk- und Anwendungs-Firewalls und IPS (Intrusion Prevention Systems), Konfigurationsänderungen für anfällige Systeme, die Verbesserung und Durchsetzung von Zugriffs- und Passwortrichtlinien sowie eine verstärkte Überwachung anfälliger Systeme und Anwendungen.

Bessere Einschätzung der Geschäftsrisiken

In den Cyberbedrohungsdaten wird auch beschrieben, wie Schwachstellen im Rahmen eines komplexen Angriffs ausgenutzt werden können. Wenn diese Informationen in Bezug zum jeweiligen Unternehmen gesetzt werden (zum Beispiel von einem lokalen Analysten), lässt sich das Geschäftsrisiko besser einschätzen. Auf Basis dieser Beschreibungen können Analysten und Administratoren den IT-Managern und der Unternehmensleitung besser die wirtschaftlichen Auswirkungen aufzeigen und erklären, welche Systeme überwacht werden sollten, bis Patches installiert und Maßnahmen zur Schadensbehebung abgeschlossen wurden.

Das Ergebnis

Mithilfe von Cyberbedrohungsdaten können Analysten für das Schwachstellenmanagement …

- besser nachvollziehen, wie und von wem Schwachstellen wahrscheinlich ausgenutzt werden,
- die Geschäftsrisiken minimieren, da Schwachstellen basierend auf reellen Bedrohungen für die Branche und das Unternehmen, fehlenden Sicherheitsmaßnahmen und der Verfügbarkeit von Exploits priorisiert werden können,
- optimale Abwehrmethoden auswählen und implementieren sowie
- Auditoren, Risikomanager und andere IT-Teams über die entsprechenden Risiken informieren.

Mehr Informationen zu FireEye erhalten Sie unter: **www.FireEye.de**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035, USA
+1 408 321 6300/+1 877-FIREEYE (347 3393)
info-dach@FireEye.com

Über FireEye, Inc.

FireEye spezialisiert sich auf datengestützte Sicherheit. FireEye erweitert die Sicherheitskapazitäten seiner Kunden nahtlos und skalierbar und bietet über eine einheitliche Plattform die weltweit anerkannten Beratungsdienste von Mandiant®, innovative Sicherheitstechnologien und Bedrohungsdaten an, die denen staatlicher Sicherheitsbehörden in nichts nachstehen. Mit diesem Ansatz übernimmt FireEye die Verantwortung für die Vorbereitung von Kundenunternehmen auf die Erkennung und Abwehr von Cyberangriffen.