Schwachstellenmanagement 2.0

Ganzheitliche Strategien zur Angriffsflächenminimierung

Von reaktiv zu proaktiv

—

23.10.2024

Zunehmende Bedrohungen

1 Schwachstellenzunahme

Die Anzahl neuer Schwachstellen (CVEs) ist im Jahr 2023 auf über 25.000 gestiegen, ein Anstieg von 15% gegenüber dem Vorjahr. Das betrifft alle Bereiche der IT-Infrastruktur, von Betriebssystemen über Webanwendungen bis hin zu IoT-Geräten.

2 Schnellere Ausnutzung

Die Zeit zwischen der Veröffentlichung einer Schwachstelle und ihrer Ausnutzung durch Angreifer hat sich drastisch verkürzt. Oftmals werden Sicherheitslücken innerhalb weniger Tage nach Bekanntwerden für Angriffe genutzt. Dies erfordert schnelles Handeln bei der Reaktion auf Sicherheitsvorfälle.

3 Ransomware-Angriffe

Schätzungsweise 80% der Ransomware-Angriffe nutzen ungeschlossene Schwachstellen aus. Kriminelle nutzen diese Schwachstellen, um sich Zugang zu Netzwerken zu verschaffen und Daten zu verschlüsseln, um Lösegeld zu erpressen. Dieser Trend zeigt die Notwendigkeit, Schwachstellen aktiv zu beheben und die IT-Sicherheit kontinuierlich zu verbessern.

Vulnerability Management 2.0

1

Automatisierte Scans

Regelmäßige Überprüfung der gesamten Infrastruktur.

2

Penetrationstests

Manuelle Tests simulieren gezielte Angriffe auf kritische Systeme.

3

Konfigurationskontrollen

Überprüfung von System- und Applikationskonfigurationen.

4

Attack Path Analysis + ASM

Analyse möglicher Angriffswege in der Infrastruktur.

Digitale Identitäten und Supply Chain

Identitätsüberwachung

Kontinuierliche Überwachung von Benutzerkonten, Zugriffsrechten und Anmeldeaktivitäten. Regelmäßige Überprüfung der Identitätsdaten und -managementsysteme zur Minimierung von Zugriffsrisiken durch unbefugte Personen oder kompromittierte Konten.

Supply Chain Risiken

Analyse von Drittanbieter-Risiken in der digitalen Lieferkette. Identifizierung potenzieller Schwachstellen bei Software, Hardware oder Diensten von externen Lieferanten, die zu Sicherheitslücken in der eigenen Infrastruktur führen können. Regelmäßige Überwachung von Drittanbietern und deren Sicherheitsmaßnahmen zur Minderung von Supply Chain Risiken.

Priorisierung und Datenkorrelation

Risiko-basierte Bewertung

Schwachstellen werden anhand des Werts der betroffenen Systeme, der Umgebung und des möglichen Angriffserfolgs priorisiert. Kritische Systeme mit hohem Wert und großer Angriffsfläche stehen dabei im Vordergrund. Systeme in besonders sensiblen Umgebungen wie Finanz- oder kritischen Infrastrukturen sollten ebenfalls besonders beachtet werden.

Datenkorrelation

Die Verknüpfung von Schwachstellen mit Exploit-Daten und Bedrohungsindikatoren ermöglicht es, das Risiko eines erfolgreichen Angriffs einzuschätzen. Bekanntheit der Schwachstelle und Verfügbarkeit von Exploit-Code sollten bei der Priorisierung berücksichtigt werden. Threat Intelligence-Feeds ermöglichen es, Bedrohungsindikatoren zu identifizieren und mit den erkannten Schwachstellen zu korrelieren, um die Bedrohungslage besser einzuschätzen.

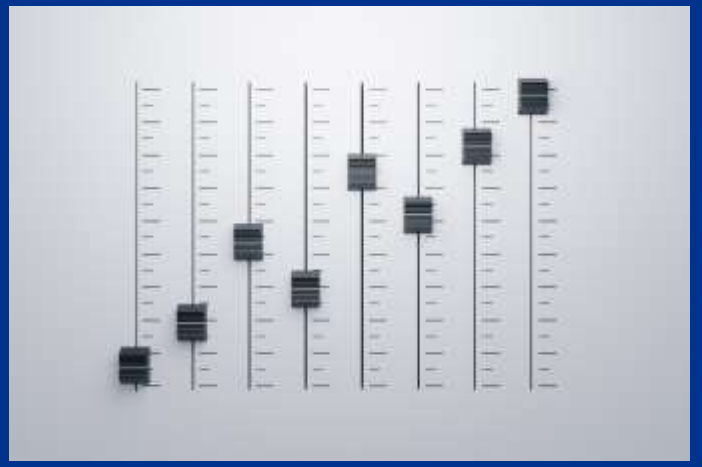
Kontextualisierte Aggregation

Die Integration von Asset-Management-Systemen und CMDB ermöglicht die Korrelation von Informationen über Assets im Netzwerk mit den erkannten Schwachstellen. Dies ermöglicht eine umfassendere Bewertung der Risiken im Netzwerk. Beispielsweise sollte eine als kritisch eingestufte Schwachstelle in einem wichtigen System, das in einer sensiblen Umgebung arbeitet, als hohes Risiko eingestuft werden.

Maßnahmenzuweisung

Automatisierte Zuweisung

Priorisierte Zuweisung von Maßnahmen basierend auf Kritikalität und Verfügbarkeit.



Compensating Controls

Implementierung alternativer Maßnahmen bei nicht direkt behebbaren Schwachstellen.

Nachverfolgbarkeit

Durchgehendes Tracking von Zuweisung, Fortschritt und Umsetzung der Maßnahmen.

Tracking und Reporting

End-to-End-Transparenz

Detailliertes Tracking des gesamten Lebenszyklus einer Schwachstelle.

Automatisiertes Reporting

Anpassbare Berichte für verschiedene Stakeholder und Zeiträume.

Automatisierung

KI und ML zur Verbesserung der Reaktionsgeschwindigkeit.

Ausblick und Verbesserung

1

KI-basierte Analysen

Die Integration von KI-Modellen ermöglicht eine präzisere Bedrohungsanalyse. Dies erlaubt die Automatisierung der Schwachstellenpriorisierung und die Identifizierung von Angriffsmustern.

2

Kollaborative Zusammenarbeit

Verbesserte Kommunikationskanäle und gemeinsame Plattformen optimieren den Datenaustausch zwischen den Sicherheitsteams.

3

Kontinuierliche Verbesserung

Regelmäßige Reviews und Analysen von Sicherheitsvorfällen ermöglichen die Optimierung des Vulnerability Management Prozesses.

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft
München

Julian-Alexis Wolf
Partner, FS Cyber Security
T +49 174 3009866
jwolff@kpmg.com

KPMG AG
Wirtschaftsprüfungsgesellschaft
Frankfurt am Main

Patrick Frech
Manager, FS Cyber Security
T +49 151 42434214
patrickfrech@kpmg.com

kpmg.de/socialmedia

kpmg.de