KURZVORSTELLUNG

SIEM: Fünf Voraussetzungen zur Lösung größerer Geschäftsprobleme

Nach mehr als zehnjährigem erfolgreichem Einsatz in Produktionsumgebungen gelten die Sicherheitsinformations- und Ereignis-Management (SIEM)-Lösungen nun als ausgereift. Funktionen wie die Ereigniserfassung und Korrelation sowie Warnmeldungen und der Nachweis der Compliance mit rechtlichen Vorschriften gehören zu den Basisanforderungen, die von den meisten SIEM-Lösungen erfüllt werden. Die Sicherheitsbedrohungen ändern sich jedoch. Unternehmen stehen vor neuen Bedrohungen wie gezielten und dauerhaften Angriffen, neuen Trends wie Mobilgeräten, Cloud und Virtualisierung sowie dem zunehmenden Fokus der Geschäftsprioritäten auf Kundenakquise, betriebliche Effizienz und Kosteneinsparungen. Als Folge dessen müssen SIEM-Systeme modernere Funktionen bieten, um größere Geschäftsprobleme lösen zu können.

McAfee hat SIEM-Benutzer nach ihren primären Herausforderungen mit SIEM-Lösungen befragt. Dabei wurden die folgenden fünf wichtigsten Herausforderungen genannt:

- Umfangreiche Sicherheitsdaten
- Überblick über die Sicherheitslage
- Echtzeitkontextinformationen
- Einfache Verwaltung
- Integrierte Sicherheit

Damit SIEM-Lösungen zur Einführung effektiverer Sicherheits- und Risiko-Management-Strategien beitragen, insbesondere zur besseren Bedrohungsabwehr, zur Nutzung neuer Trends sowie zur Abstimmung mit Unternehmensprioritäten, müssen fünf Herausforderungen gelöst werden. Im Folgenden stellen wir Ihnen diese mit entsprechenden Kundenbeispielen und Anwendungsfällen vor.

1. Umfangreiche Sicherheitsdaten

Umfangreiche Sicherheitsdaten können sehr wertvoll sein – sofern Sie diese nutzen können. Ältere SIEM-Lösungen wurden jedoch weder für die Integration einer solchen Vielzahl an Endgeräten, Netzwerken und Datenquellen konzipiert, noch waren sie für die Verarbeitung derart hoher Ereignisraten oder Umsetzung so langer Aufbewahrungszeiten vorgesehen. Als Folge dessen erfüllen relationale Datenbanken und ähnliche Defizite älterer SIEM-Lösungen, die hauptsächlich für netzwerkorientierte Ereignisse entwickelt wurden, nicht die Sicherheitsanforderungen aktueller dynamischer IT-Infrastrukturen. Sie sind nicht schnell, erweiterbar und skalierbar genug, um den erforderlichen Grad an Effizienz und Nutzen zu bieten.

Beispiel: Bundesbehörden

Eine große Regierungsbehörde wollte die umfangreichen Sicherheitsdaten in den mehrere Petabyte großen relationalen Datenbanken ihrer SIEM-Lösung mit fortschrittlichen Analysen untersuchen. Doch selbst einfache Berichte dauerten Stunden und manchmal sogar mehr als einen Tag, wodurch die eingesetzte SIEM-Lösung für forensische Analysen ungeeignet war.

Nach dem Umstieg auf die SIEM-Lösung McAfee® Enterprise Security Manager konnte die Behörde nicht nur mehr, sondern auch unterschiedlichere Geräte integrieren und ihre Analysen um daten- sowie benutzerorientierten Kontext erweitern. Darüber hinaus konnten die Ereignisraten und die Menge der gespeicherten Daten erhöht werden. Berichte können nun innerhalb von Minuten erstellt und damit der gesamte Einsatz forensischer Analysen verbessert werden.

2. Überblick über die Sicherheitslage

Früher waren SIEM-Lösungen einfach nur Tools, mit denen Ereignisse aus Firewalls sowie Eindringungserkennungssystemen korreliert und dann eventuell einige Schwachstellenbewertungsdaten angewendet wurden. Auch heute gibt es noch einige SIEM-Lösungen, die hauptsächlich mit Netzwerkverkehrsdaten arbeiten. Obwohl alle diese Quellen wichtig sind, müssen sie um Anwendungen, Datenkontexte und Identitätsinformationen ergänzt werden. Ohne diese zusätzlichen Informationen sind mehr Zeit und Ressourcen nötig, um Ereignisse erfassen, auf Grundlage

Anwendungsfall: Umfangreiche Sicherheitsdaten

- Erweiterung der Datenerfassung um mehr Datenströme aus mehr Quellen
- Durchführung von Analysen und forensischen Analysen für sehr große Datensätze
- Optimierung für die Geschwindigkeits- und Mengenanforderungen umfangreicher Sicherheitsdaten
- Höhere Mitarbeiter- und Prozesseffizienz

Anwendungsfall: Überblick über die Sicherheitslage

- Besserer Einblick in die Sicherheitslage durch mehr Lösungen für die Identitätsverwaltung
- Informationen über Anwender, Zeitpunkt, Zugriffsart und -ort sowie genutzte Inhalte
- Informationen über Nutzungsdauer sowie weitere Anwender und zusätzlich genutzte Inhalte
- Einsatz von BYOD-Ressourcen wie Laptops und Smartphones

ausreichender Situationsdaten priorisieren und damit zeitnah nutzbar machen zu können.

Beispiel: Gesundheitsdienstleister

Ein regionaler Gesundheitsdienstleister wollte das BYOD-Konzept (Bring Your Own Device) nutzen, um mithilfe privater Tablets die Mitarbeitermobilität zu verbessern. Aufgrund früherer Sicherheitsvorfälle machte er sich jedoch Sorgen über den Missbrauch durch Insider. Die vorherige SIEM-Lösung des Gesundheitsdienstleisters konnte auf keinem Gerät – egal ob Laptop, Desktop-PC, Tablet oder virtueller Desktop-Rechner – erkennen, welche Anwender sensible Daten nutzten.

Dank McAfee Enterprise Security Manager konnte der Gesundheitsdienstleister eine Verbindung mit der Identitäts- und Mobilitätsverwaltung, mit Active Directory sowie mit LDAP-Produkten herstellen, um einen Überblick über Benutzer und Geräte zu erhalten. Aufgrund der Integration in strukturierte und unstrukturierte Datenspeicher wie systemeigene Datenbanken sowie die Integration in den Datenkompromittierungsschutz und die Datenbankaktivitätsüberwachung erhielt der Dienstleister einen umfassenderen Überblick über die aktuelle Sicherheitslage und konnte dadurch die Behebung von Insider-Bedrohungen verbessern.

3. Echtzeit-Kontextinformationen

Anfangs dienten SIEM-Lösungen in erster Linie der Protokollverwaltung, d. h. der Erfassung, Speicherung und Abfrage von Informationen mit einigen zusätzlichen Features. Protokolle sind zwar nach wie vor eine grundlegende SIEM-Komponente, doch heute benötigen SIEMs auch Echtzeit-Kontextinformationen.

McAfee Global Threat Intelligence (McAfee GTI) und McAfee Vulnerability Manager stellen solche Kontext-informationen bereit. Während McAfee GTI als Cloud-basierter Echtzeitreputationsdienst fungiert, erfasst McAfee Vulnerability Manager, welche Unternehmensressourcen durch die Schwachstellen gefährdet sind.

Beispiel: Einzelhändler

Ein Einzelhandelsunternehmen der Fortune 100-Liste ohne SIEM-Lösung für die Produktion und ohne McAfee-Lösungen führte ein Proof-of-Concept durch und erkannte bereits in der ersten Woche, dass mehr als 30 Prozent des Datenverkehrs, der in das Unternehmensnetzwerk gelangen wollte, aus böswilligen Quellen stammte und/oder schädliche Daten enthielt.

Durch die Nutzung von McAfee Enterprise Security Manager zur Korrelation der Ereignisinformationen mit McAfee GTI konnte das Unternehmen schnell erkennen, welche Ressourcen der einzelnen Speicherorte und Rechenzentren angegriffen wurden und bekam somit eine bessere Vorstellung von den Angriffsarten, die auf das Unternehmen abzielten. Die McAfee-SIEM-Lösung ermittelte den höchsten Schweregrad und wies den Reaktionen auf dieser Grundlage Prioritäten zu. Durch die Kombination von SIEM und Echtzeitkontext-informationen wurde eine schnellere Erkennung, Priorisierung und Behebung von Bedrohungen möglich.

4. Einfache Verwaltung

Ältere SIEM-Lösungen sind sehr starr aufgebaut und verfügen nicht über alle wichtige Funktionen. Sie können beispielsweise nicht problemlos in ehemals

Anwendungsfall: Echtzeit-Kontextinformationen

- Informationen über Bedrohungen inner- und außerhalb der Umgebung
- Verbesserung der SIEM-Daten mit Echtzeit-Kontextinformationen
- Schnellere Erkennung und Reaktion auf Sicherheitsvorfälle
- Erkennung und Priorisierung von Bedrohungen dank zusätzlicher Sicherheitsinformationen

Anwendungsfall: Einfache Verwaltung

- SIEM-Lösung mit dynamischen Whitelists und Hardware-unterstützter Sicherheitstechnologie zum Schutz von Geräten mit fester Funktion
- Vereinfachung forensischer Analysen durch anpassbare Drilldowns
- Integration der SIEM-Lösung in die Firewall und Eindringungs-schutzsysteme für schnellere Reaktionen auf Sicherheitsvorfälle
- Längere Nutzungsdauer älterer Ressourcen dank verbesserter Sicherheit

nicht unterstützte Geräte integriert werden, um deren Informationen nutzen zu können. SIEM-Lösungen der nächsten Generation können hingegen einfach angepasst werden und sind flexibel genug, um sich in jede Umgebung zu integrieren. Genau aus diesem Grund sind sie für viele Unternehmen von strategischer Bedeutung.

Beispiel: Versorgungsunternehmen

Ein großes Versorgungsunternehmen musste Sicherheitskontrollen implementieren, um zu verhindern, dass Stuxnet-ähnliche Angriffe die Infrastruktur lahm legen und Millionen Kunden von Stromausfällen betroffen sind. Dank McAfee Enterprise Security Manager konnte sich das Versorgungsunternehmen unter Einsatz eigener Geräte, Anwendungen und Protokolle Überblick über die aktuelle Sicherheitslage der Unternehmens-IT sowie der SCADA- und Industriesteuersysteme (ICS) verschaffen.

Dabei stellte die McAfee-SIEM-Lösung Tools zur individuellen Integration in die SCADA- und ICS-Geräte bereit. Das wiederum ermöglichte Korrelationen, Anomalie-Erkennung sowie Trendanalysen über alle drei Bereiche hinweg. Zusätzlich zur angepassten Ereigniserfassung profitierte das Unternehmen von der Möglichkeit zur schnellen und unkomplizierten Erstellung individueller Dashboards, Berichte, Korrelationsregeln sowie Warnmeldungen. Damit wurde SIEM zu einem wertvollen Tool für die Gewährleistung der Sicherheit, den Nachweis der Compliance mit rechtlichen Vorschriften und die Ressourcenverfügbarkeit. Anders ausgedrückt: Die Lösung sorgte für einen ausfallsicheren Betrieb, damit die Kunden nicht im Dunkeln saßen.

5. Integrierte Sicherheit

SIEM ist zwar eine wichtige, aber dennoch nur eine von vielen Komponenten jeder strategischen Sicherheitsinitiative. Die Integration von Schutz- und Compliance-Lösungen bietet mehr Sicherheit als reine Einzellösungen und sorgt zudem für eine weniger komplexe Architektur. Oftmals ist gerade Komplexität der Grund, warum Schutzmaßnahmen nicht strategischer und damit auf die Geschäftsprioritäten ausgerichtet, sondern rein taktisch ausgelegt sind.

Beispiel: Finanzdienstleister

Ein internationaler Bankkunde setzte eine Fülle verschiedener Produkte von unterschiedlichen Anbietern ein. Während er mit einigen dieser Produkte arbeitete, wurden viele aufgrund eingeschränkter Ressourcen nicht regelmäßig genutzt oder gepflegt. Die Bank fand heraus, dass durch die Nutzung von SIEM in Kombination mit integrierten Endgeräten, Netzwerken und Datenkontrollen Risiken effizienter behoben, Kosten reduziert und gleichzeitig Schutzmaßnahmen geschäftsrelevanter gestaltet werden können.

Durch die Beschränkung auf weniger Anbieter konnte die Bank Skaleneffekte nutzen. Darüber hinaus ließen sich die Schulungskosten sowie die Anzahl der Agenten, Konsolen, Server usw. reduzieren. Als Folge dessen wurden auch Vertragskosten und eine Reihe damit verbundener Ausgaben eingespart. Zusätzlich zu den Kosteneinsparungen stellte die Bank sicher, dass alle vorhandenen und zukünftigen Lösungen vollständig in McAfee Enterprise Security Manager integriert wurden, um eine bessere Kontrolle und einen Überblick über die Sicherheitslage zu gewährleisten.

Anwendungsfall: Integrierte Sicherheit

- Optimierung des Sicherheits- und Betriebsablaufs
- Weniger Komplexität dank Automatisierung und unkomplizierter Anpassung
- Mehr Transparenz und besserer Überblick über die Sicherheitslage durch aufeinander abgestimmte Sicherheitslösungen
- Verbesserte Sicherheit durch Informationen und Integration

Wichtige Überlegungen

- Wie wichtig ist es, dass Sie die Herausforderungen bei Erfassung, Speicherung, Zugriff, Verarbeitung und Analyse von umfangreichen Sicherheitsdaten problemlos meistern?
- Erhalten Ihre Sicherheitsverantwortlichen die erforderlichen Informationen rechtzeitig, um fundierte Entscheidungen treffen und zeitnah Maßnahmen ergreifen zu können?
- Verfügt Ihr Sicherheitsteam über die erforderlichen Echtzeit-Kontextinformationen, um Risiken und Angriffe zu erkennen, bevor diese Schaden anrichten können?
- Wie würde eine SIEM-Lösung mit intuitivem Zugriff auf Detailinformationen und schnell anpassbaren Ansichten Ihre Sicherheit und Ressourcen beeinflussen?
- Wie würde die Integration in Ihre gesamte Infrastruktur Ihre Sicherheit und Transparenz sowie die Prozesse und Reaktionsfähigkeit verbessern?

Was in den letzten zehn Jahren mit älteren SIEM-Lösungen funktioniert hat, reicht in Anbetracht heutiger Anforderungen einfach nicht mehr aus. Aufgrund der neuen Anforderungen in Bezug auf Big Data, Sicherheitsinformationen, Überblick über die aktuelle Sicherheitslage, Leistungsfähigkeit, Bedienbarkeit und Integration hat sich das Einsatzgebiet für SIEM-Lösungen vergrößert. SIEM-Lösungen sollten für weniger und nicht für mehr Komplexität sorgen. Erwarten Sie also auch mehr von Ihrer SIEM-Lösung.

Heute müssen SIEMs als Teil eines größeren, verbundenen Sicherheits-Frameworks arbeiten, in dem die Sicherheits- und Geschäftsprioritäten aufeinander ausgerichtet sind. Die SIEM-Lösung spielt eine wichtige Rolle, wenn die Sicherheit strategischer gestaltet und ein echter Vorteil für das Unternehmen erreicht werden soll.

Weitere Informationen zu den SIEM-Lösungen von McAfee finden Sie unter **www.mcafee.com/de/products/siem/index.aspx**.

Integrierte Sicherheit

McAfee bietet ein einheitliches, integriertes Framework für hunderte Produkte, Services und Partner, damit diese voneinander lernen, kontextspezifische Daten in Echtzeit austauschen sowie als Team agieren, um somit die Sicherheit von Informationen sowie Netzwerken gewährleisten zu können. Dank des innovativen Konzepts, der optimierten Prozesse sowie der effektiven Einsparungen, durch die sich diese Plattform auszeichnet, kann jedes Unternehmen nicht nur seine Sicherheitslage verbessern, sondern gleichzeitig die Betriebskosten senken.

McAfee
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de