SECUINFRA
Cyber Defense. Made in Germany.

FACHARTIKEL

So finden Unternehmen die passende Lösung

Die fünf wichtigsten Aspekte einer erfolgreichen SIEM-Implementierung

Security Information and Event Management (SIEM) liefert bei der Detektion von IT-Sicherheitsvorfällen einen entscheidenden Mehrwert für die Informationssicherheit im Unternehmen. Damit kann die Zeit bis zur Identifikation einer Bedrohung deutlich verkürzt und damit das IT Security Niveau erhöht werden. Die Voraussetzung: Die Wahl und Implementierung der Lösung erfolgen gut geplant.

Cyberkriminelle schlafen nicht: Im vergangenen Jahr gab es weltweit so viele Angriffe auf Unternehmen, NGOs und Regierungen wie nie zuvor. Nicht nur die reine Masse stellt eine Herausforderung dar, sondern auch die zunehmende Professionalität der Angriffe. Ob Ransomware-, Phishing-, Drive-By-Downloads oder Social Engineering: Hacker lassen nichts unversucht, um Netzwerke zu kompromittieren, an Unternehmensdaten zu gelangen und Lösegelder zu erpressen.

Bei der Fülle an täglichen Bedrohungen müssen die Cyber-Sicherheitsteams von Unternehmen in der Lage sein, schnell und effizient auf die Bedrohungslagen zu reagieren. Genau hier setzt Security Information and Event Management (SIEM) an: Es kombiniert Bestandteile des Security Information Managements (SIM) und des Security Event Managements (SEM). Eine SIEM-Lösung sammelt unternehmensweit Logdaten aus zugrunde liegenden Quellen wie Servern, Endpoints, Firewalls, Intrusion Detection und Prevention Systemen (IDS und IPS) sowie Anwendungen. In einer zentralen Management-Station werden die Daten zusammengeführt, aufbereitet sowie unter- und miteinander in Beziehung gesetzt und auf Dashboards visualisiert. Anhand von vorher definierten Use Cases können nun Auffälligkeiten und Regelverstöße automatisiert erkannt werden. IT-Sicherheitsvorfälle können so frühzeitig durch Cyber Defense Analysten identifiziert werden – und zwar in Bereichen, welche konventionelle IT-Sicherheits-Lösungen nicht berücksichtigen. Das bietet IT-Sicherheitsteams einen entscheidenden Vorteil – denn die Zeit, die bis zur Identifizierung einer akuten Bedrohung benötigt wird (Meantime to Detect), lässt sich durch ein SIEM deutlich reduzieren. Damit macht es die Arbeit von IT-Sicherheitsspezialisten effektiver und erhöht das IT Security Niveau entscheidend.

Die Voraussetzung: Vor der Implementierung werden die relevanten Aspekte berücksichtigt. Denn SIEM ist weit mehr als ein Produkt. Die Einführung muss gut geplant sein, um enttäuschte Erwartungen und späte Kostenexplosionen zu vermeiden. Hierbei ist es zunächst elementar, die spezifischen Unternehmensanforderungen zu definieren. Es ist sinnvoll, ein SIEM-Konzept zu erstellen, das die Basis für die Einführung und den späteren Betrieb bildet. Fünf Aspekte sind bei der Implementierung zentral.

Integrierbarkeit

SIEM-Lösungen bringen in der Regel Schnittstellen für gängige Systeme mit, die aber nicht zwangsläufig zu den im Unternehmen verwendeten Systemen passen. Fehlen Schnittstellen, verlängert sich die Implementierungsdauer maßgeblich, da Konnektoren manuell zu entwickeln sind. Dies führt zu zusätzlichen Investitionskosten. Damit ein SIEM-System einen relevanten Mehrwert im Kampf gegen Cyberbedrohungen bietet, muss die Lösung möglichst gut auf die bestehende IT-Infrastruktur zugeschnitten sein. Vor Einführung ist deshalb zu definieren, welche Logdaten eine SIEM-Lösung verarbeiten muss.

Kosten

Die Bezahlmodelle für SIEM-Lösungen unterscheiden sich teils deutlich: Es wird nach Datenvolumen, der eingehenden Anzahl von Events oder der angeschlossenen Systeme abgerechnet. Viele Systemhersteller bieten auch attraktive Rabatte für umfangreiche Implementierungen, für kleine und mittlere Unternehmen (KMU) kann sich hier allerdings eine Kostenfalle auftun. Verarbeitet ein KMU täglich zehn Gigabyte Datenvolumen in seinem SIEM-System, muss es dafür voll bezahlen. Konzerne hingegen profitieren von der Skalierbarkeit – wenn hier beispielsweise 250 Gigabyte Datenvolumen angesetzt werden, wird der Endpreis wegen der Rabatte proportional geringer. KMU sollten deswegen auch in Bezug auf Umsatz- und Gewinnzahlen die Kostenstruktur der SIEM-Lösung genau ansehen.

Funktionsumfang

Auch was den Funktionsumfang betrifft, sind viele SIEM-Systeme für den Einsatz in Großkonzernen ausgelegt - etwa mit einer granularen Rechteverwaltung oder einer Mandantenteilung für die Mutter und die IT-Systeme der Unterfirmen. Dies ist für KMU häufig überdimensioniert und unnötig komplex. Außerdem zeigt sich, dass viele Unternehmen in den ersten Jahren nach der Implementierung lediglich die Basis-Funktionen nutzen. Wird eine im Umfang reduzierte Lösung auf die Anforderungen des Unternehmens optimiert, ist dies ein wirtschaftlicher und sicherer Ansatz. Allerdings entscheiden sich Unternehmen häufig für eine SIEM-Lösung, die viel zu umfangreich ist. Die Verantwortlichen entscheiden in Ermangelung von Erfahrung

häufig nach der Bekanntheit eines Produktes und vertrauen darauf, dass es ihnen die gesamte Arbeit abnimmt. Das jedoch kann kein Produkt – auch nicht jenes mit dem umfangreichsten Leistungsspektrum. Vor der Entscheidung muss also unbedingt definiert werden, welche Funktionen wirklich gebraucht werden. Die Erarbeitung eines initialen SIEM-Konzepts ist sinnvoll.

Use Cases und Detektionsregeln

Use Cases als logisches Element zur Erkennung von Angriffen bzw. deren Detektionsregeln als technische Umsetzung der Logik sind das Herzstück eines SIEM-Systems. Bei fast allen Anbietern sind mitgelieferte Use Cases als praktische „Out-of-the-Box"-Lösungen eines der zentralen Verkaufsargumente. Diese vorgefertigten Regeln bringen jedoch meist nur geringen Mehrwert. Zum einen sind sie generisch, passen somit kaum zur IT-Landschaft bzw. der Bedrohungslage und müssen aufwändig angepasst werden. Meist fehlen sowohl die Angaben, welche Logs bzw. Events vom IT-System benötigt werden, als auch Handlungsanweisungen für die Cyber Defense Analysten im Falle eines Alarms. Die Vielzahl von Regeln führt zudem oft zu einer regelrechten Alarmflut, wenn sie umfänglich aktiviert werden. Die Regeln müssen vorab sinnvoll ausgewählt werden. Sowohl für diesen Auswahlprozess als auch für die spätere Bearbeitung der Alarme aus den Use Cases ist zudem wichtig, dass diese einen direkten Bezug zu bekannten IT Security-Frameworks wie MITRE ATT&CK haben. Damit und mit entsprechendem Expertenwissen kann das wesentliche Ziel der Use Case-Auswahl erreicht werden: mit einer möglichst geringen Anzahl an hochwertigen Use Cases die maximale Abdeckung bekannter Angriffsvektoren zu erhalten.

SIEM Consultants wie die Experten von SECUINFRA empfehlen daher den Einsatz von Use Cases, deren Dokumentation und Handlungsempfehlungen umfassend sind und deren Detektionsregeln auf die IT-Landschaft gezielt angepasst sind. Bei der Auswahl sollte auf eine breite Streuung der Detektionsmechanismen geachtet werden, um Angriffsverhalten früh zu erkennen. Hierbei gilt der Grundsatz: Besser wenige hochwertige Use Cases als viele fehler- und arbeitsanfällige Regeln zu implementieren. Dies ist der Schlüssel zu einem wirkungsvollen und wirtschaftlichen SIEM-Betrieb.

Geschultes Personal

Damit ein SIEM wirkungsvoll eingesetzt werden kann, müssen die Nutzer – in der Regel SOC Analysten – Angriffsszenarien und -alarme verstehen und wissen, wie genau zu reagieren ist. SIEM-Lösungen übernehmen zwar die repetitive Arbeit, die Analysten müssen jedoch die daraus entstehenden Alarme in den Kontext setzen. Oft benötigen Unternehmen hier die Unterstützung von Experten: Erfahrene Cyber Defense Analysten können Angriffsmuster und komplexe Zusammenhänge zuverlässig erkennen.

Ein SIEM-System ist nur dann wirkungsvoll, wenn es optimal an die bestehende IT-Infrastruktur angepasst ist. Mit der Entscheidung für ein vorangehendes beziehungsweise projektbegleitendes SIEM Consulting sparen Unternehmen nicht nur Zeit und Kosten, sondern vermeiden auch Probleme und Stolpersteine, die sich auf dem Weg zu einem erfolgreichen SIEM-Betrieb häufig ergeben. Werden diese Aspekte berücksichtigt, stellt SIEM ein überaus mächtiges Werkzeug im Kampf gegen Cyberbedrohungen dar.

Fazit

Ein Security Information and Event Management beschleunigt die Erkennung von Angriffen deutlich und entlastet die Cyberabwehr von repetitiven Routine-Aufgaben. Maßgeschneiderte Detektionsmechanismen in SIEM-Lösungen können die Cyber-Resilienz eines Unternehmens maßgeblich steigern – aber nur dann, wenn das Produkt auf den individuellen Bedarf angepasst werden kann. Wer sich auf Out-of-the-Box Lösungen verlässt, zahlt am Ende oft doppelt und hat damit insgesamt höhere Kosten. Um wirtschaftliche Fehlentscheidungen zu vermeiden und gleichzeitig die Funktionalität des SIEM-Systems zu optimieren, ist es sinnvoll, sich bereits in der Frühphase der Entscheidungsfindung Unterstützung von Experten zu holen.

Autoren: Norbert Nitsche, Senior Cyber Defense Consultant SECUINFRA

David Bischoff, Senior Cyber Defense Consultant SECUINFRA

Weitere Informationen: https://www.secuinfra.com/de/solutions/siem/

Pressekontakt: SECUINFRA GmbH

Svenja Koch

Stefan-Heym-Platz 1

10367 Berlin

Mobile: +49 160 921 633 44

marketing@secuinfra.com