Sicherheit für KMUs in 5 Teilen

Teil 2: Grundlagen und die Bedeutung von Logs

Einführung in ein SIEM-System

Security Information and Event Management (SIEM) ist ein kritischer Bestandteil der IT-Sicherheitsstrategie in modernen Unternehmen. Diese Systeme sammeln, analysieren und speichern Log-Daten aus verschiedenen Quellen innerhalb einer IT-Infrastruktur, um Sicherheitsbedrohungen in Echtzeit zu identifizieren und darauf zu reagieren. SIEM-Systeme kombinieren Sicherheitsinformationsmanagement (SIM) und Sicherheitsereignismanagement (SEM) zu einem ganzheitlichen Sicherheitsüberwachungs- und Management-Ansatz.

Bedeutung von Log-Dateien

Jedes IT-System, ob es sich um einen einzelnen Computer, ein Smartphone oder ein Netzwerkgerät handelt, erstellt kontinuierlich digitale Aufzeichnungen seiner Aktivitäten – diese Aufzeichnungen nennt man Log-Daten oder Log-Dateien. Diese automatisch generierten Berichte enthalten detaillierte Informationen über die Vorgänge innerhalb des Systems, wie zum Beispiel:

- Wer hat sich wann angemeldet?
- Welche Befehle wurden ausgeführt?
- Welche Fehler sind aufgetreten?
- Wie reagieren die Systemkomponenten auf verschiedene Anfragen?

Warum sind Log-Daten so wichtig?

Diese Log-Daten sind von unschätzbarem Wert für die Cybersicherheit, da sie es IT-Profis ermöglichen, zu verstehen, was normalerweise in ihren Systemen passiert und wann Anomalien auftreten. Durch das Studium dieser Logs können Sicherheitsexperten ungewöhnliche oder verdächtige Verhaltensweisen

erkennen, die auf einen Cyberangriff, Systemfehler oder andere Sicherheitsrisiken hinweisen könnten. Zum Beispiel:

- Ein ungewöhnliches Login zu einer untypischen Uhrzeit könnte ein Hinweis auf einen unbefugten Zugriffsversuch sein.
- Häufige Fehlermeldungen von einer Anwendung könnten auf eine mögliche Schwachstelle hinweisen, die behoben werden muss.

Log-Daten bieten also eine fundamentale Grundlage, um die Sicherheit eines Systems proaktiv zu überwachen und zu verbessern. Sie helfen, Probleme schnell zu identifizieren und zu beheben, bevor sie zu ernsthaften Bedrohungen führen können.

Implementierung der Log-Datensammlung

Die effektive Sammlung und Analyse von Log-Daten ist ein fundamentaler Baustein für jedes robuste Sicherheitssystem. In modernen Sicherheitsinformations- und Ereignismanagement-Systemen (SIEM) wird diese Aufgabe oft von spezialisierten Software-Agenten übernommen. Diese Agenten werden auf verschiedenen Geräten innerhalb des Netzwerks installiert und sind dafür verantwortlich, relevante Log-Daten automatisch zu erfassen und zur zentralen SIEM-Plattform zu senden.

Vorteile der Verwendung von SIEM-Agenten:

- **Automatisierte Datenerfassung**
  Diese Agenten erleichtern die kontinuierliche und automatische Erfassung von Log-Daten von Endpunkten, Servern und anderen Netzwerkgeräten, ohne dass eine manuelle Intervention erforderlich ist.

- **Erweiterte Sicherheitsanalyse**
  Neben der Sammlung von Logs führen diese Agenten auch erste Sicherheitsbewertungen durch, die als Sicherheitskonfigurationsbewertungen (Security Configuration Assessments, SCA) bekannt sind. Dabei analysieren sie die Sicherheitseinstellungen der Geräte im Vergleich zu etablierten Sicherheitsstandards und Best Practices.

Funktionsweise der Sicherheitsbewertungen durch Agenten

Durch die Implementierung dieser Agenten können Unternehmen nicht nur ihre Datensammlung optimieren, sondern auch eine proaktive Sicherheitsüberwachung durchführen. Die Agenten bewerten die Konfigurationen der Geräte und identifizieren potenzielle Schwachstellen, indem sie aktuelle Einstellungen mit Industriestandards vergleichen. Dies ermöglicht es Sicherheitsteams, schnell auf mögliche Sicherheitsrisiken zu reagieren und die notwendigen Anpassungen vorzunehmen, um die Netzwerksicherheit kontinuierlich zu verbessern.

Integration in das SIEM-System

Die nahtlose Integration dieser Agenten in das übergeordnete SIEM-System ermöglicht eine zentrale Sicht auf die Sicherheitslage des gesamten Netzwerks. Durch die zentralisierte Sammlung und Analyse der Daten können Sicherheitsverantwortliche effektiver auf Bedrohungen reagieren und umfassende Sicherheitsmaßnahmen orchestrieren.

Praxisbeispiele

Beispiel 1: Erkennung von Insider-Bedrohungen

Situation: Ein großes Finanzunternehmen bemerkte ungewöhnlich hohe Datenzugriffe durch einen Mitarbeiter außerhalb der regulären Arbeitszeiten. Die Sicherheitsüberwachungsplattform erfasste diese Aktivitäten durch die kontinuierliche Analyse der Log-Daten.

Lösung: Die Plattform wertete die erfassten Daten aus und stellte fest, dass der Mitarbeiter auf sensible Informationen zugriff, die nicht zu seinem Arbeitsbereich gehörten. Durch die sofortige Alarmierung des Sicherheitsteams konnte eine interne Untersuchung eingeleitet werden.

Ergebnis: Es stellte sich heraus, dass der Mitarbeiter versuchte, Kundendaten zu extrahieren. Dank der frühzeitigen Erkennung durch die Sicherheitsüberwachungsplattform konnte das Unternehmen den Datenverlust verhindern und entsprechende rechtliche Schritte einleiten.

Beispiel 2: Abwehr von Ransomware-Angriffen

Situation: Ein mittelständisches Produktionsunternehmen wurde Ziel eines Ransomware-Angriffs. Die Sicherheitssoftware auf den Endgeräten konnte den Angriff zunächst nicht blockieren.

Lösung: Die Sicherheitsüberwachungsplattform identifizierte ungewöhnliche Verschlüsselungsaktivitäten auf mehreren Netzwerkgeräten und löste sofort Alarme aus. Die Plattform analysierte die Log-Daten, um die Quelle des Angriffs zu identifizieren und automatisierte Gegenmaßnahmen einzuleiten.

Ergebnis: Obwohl einige Anfangsdaten verschlüsselt wurden, verhinderte die schnelle Reaktion der Plattform eine umfassende Ausbreitung der Ransomware. Das Unternehmen konnte die betroffenen Systeme schnell isolieren und wiederherstellen, was den Betriebsausfall minimierte und die finanziellen Einbußen reduzierte.

Beispiel 3: Compliance-Überwachung

Situation: Ein Gesundheitsdienstleister benötigte eine Lösung zur Einhaltung strenger Datenschutzrichtlinien, um patientenbezogene Daten zu schützen und Compliance-Anforderungen zu erfüllen.

Lösung: Die Sicherheitsüberwachungsplattform wurde eingesetzt, um alle Zugriffe auf patientenbezogene Daten zu überwachen und zu protokollieren. Die Plattform bewertete laufend die Sicherheitskonfigurationen der Systeme und meldete Abweichungen von den Compliance-Vorgaben.

Ergebnis: Die Plattform stellte nicht nur sicher, dass alle Zugriffe auf sensible Daten dokumentiert wurden, sondern half auch dabei, die Einhaltung von HIPAA und anderen Datenschutzgesetzen kontinuierlich zu überprüfen und zu bestätigen. Dies reduzierte das Risiko von Compliance-Strafen erheblich.