

# Frühzeitig über Sicherheitsverstöße informiert werden – aber wie?

Die steigenden Mengen an sicherheitsrelevanten Log- und Ereignisdaten können kaum mehr effektiv und zeitnah mit herkömmlichen Mitteln analysiert werden. Zumal die zur Aufklärung von Sicherheitsverstößen relevanten Informationen auf IT-Systemen verteilt und autark vorliegen. Diesen gordischen Knoten gilt es mittels „SIEM“ aufzulösen.

**D**as Anforderungsprofil: bei Sicherheitsvorfällen diese Informationen systemübergreifend über zeit- und ressourcenbezogene Prozesse in Relation zu bringen. Solche Prozesse müssen schnell ablaufen, weil dem Unternehmen bei Sicherheitsverstößen meist wenig Zeit bleibt einzugreifen. Ein praxisbewährtes Mittel, um in diesen Fällen angemessen zu reagieren, sind so genannte „Security-Information- und Event-Management-Systeme“ (SIEM). Mit SIEM wird ein Alarmierungs- und Warnsystem eingerichtet, mit dem bei akuten Sicherheitsverstößen alle potenziell Betroffenen schnell und angemessen informiert werden. Rechtzeitige Gegenmaßnahmen werden möglich, Schäden größeren Ausmaßes oft vermieden.

Die für SIEM relevanten Log- und Ereignisdaten werden von aktiven Netzwerkkomponenten, Sicherheitskomponenten, Betriebssystemen, Anwendungen, Diensten und physikalischen Zutrittssystemen erzeugt. Alle diese Systeme und Komponenten generieren im Betrieb fortwährend große Mengen an Meldungen und Informationen. Das Ausgangsproblem in den Unternehmen: Diese zumeist verteilte Masse an Daten kann auf Grund ihrer ungeheuren Menge nicht mehr manuell analysiert und bearbeitet werden. Die Folge: Systemübergreifende Vorgänge werden nicht erkannt und können nur reaktiv mit hohem zeitlichen Verzögerung nachgestellt werden.

Was also tun, um diese Reservoirs gezielt und vor allem kostenvertretbar für mehr IT-Sicherheit, Betrugssicherheit und Compliance-Konformität anzuzapfen und auszuwerten? SIEM eröffnet die geeigneten Werkzeuge, um eine zentrale und revisions-sichere Ablage sowie eine Langzeitarchivierung und Auswertung von Log-Daten umzusetzen. Siem-Systeme realisieren dies, indem sie eine dedizierte Log-Managementkomponente zur Verfügung stellen. Sie zeichnet für die zentrale und Langzeit-

speicherung von Log-Daten verantwortlich. Ein großer Vorteil dieses zentralen Ansatzes ist, dass Sicherheitsverantwortliche und Administratoren zentral Volltext-indizierte Log-Daten erhalten, zusätzlich für Auswertungen auf eine intuitiv bedienbare grafische Schnittstelle sowie eine Filtersprache zurückgreifen können. Mit SIEM stehen, beispielsweise für forensische Analysen oder zur Erfüllung von Nachweispflichten, neben den normalisierten Daten die Ursprungsdaten gesichert zur Verfügung.

## „SIEM löst den gordischen Sicherheitsknoten“

Was SIEM-Systeme zusätzlich können ist eine Echtzeitanalyse von sicherheitsrelevanten Ereignisdaten, die Korrelation von verschiedenen Ereignisquellen sowie die frühzeitige Alarmierung und Reaktion bei Vorfällen. Um dies zu erreichen, durchlaufen SIEM-Lösungen die elementaren Phasen der Log- und Ereignisdaten-Sammlung, der Normalisierung dieser Daten und der anschließenden Korrelation und Alarmierung. Um an die relevanten Log- und Ereignisdaten der Quellsysteme zu gelangen, sollte SIEM sowohl Push- als auch Pull-Mechanismen vorhalten. Für beides müssen die Kollektoren als passive Elemente und die Agenten als aktive Elemente nahtlos zusammenwirken.

Die meisten Hersteller von SIEM-Systemen offerieren eine große Vorauswahl für

gängige Log- und Ereignisquellen. Die Daten werden anschließend gefiltert, aggregiert und kategorisiert sowie durch Normalisierung in ein einheitliches Format gebracht. Das Gros der Informationen wird bereits in dieser frühen Phase gefiltert und aggregiert, damit keine unnötigen Redundanzen entstehen und später die rechenintensiven Prozesse sich voll auf die Auswertung der werthaltigen Daten konzentrieren können. In der Phase der Kategorisierung sollten Inhalte der Logs verfeinert beziehungsweise durch typenspezifische Informationen ergänzt werden können. Das vereinfacht für die spätere Priorisierung das Erstellen der Korrelationslogik und der dazu passenden Korrelationsregeln.

Die normalisierten Informationen werden anschließend an ein zentrales System weitergeleitet, welches das Ausgangsereignis mit anderen Ereignissen korreliert. Dabei werden gemäß des hinterlegten Logik- und Regelwerks die unterschiedlichen Ereignisse meist durch Anwendung boolescher Operatoren verknüpft. Weitere mögliche Korrelationsmechanismen basieren auf Mustererkennung oder statistischen Analysen (Anomalieerkennung). In dieser Phase erweist sich, wie intelligent das SIEM-System tatsächlich ist. Für ein effektives Security-Monitoring sollten die Entscheider außerdem ihr Augenmerk auf die Feinjustierung der Korrelationsregeln lenken. So sollten besonders kritische Ereignisse nicht durch eine Masse an wertlosen Informationen (falsch-positive) verdeckt werden. Unter dieser Voraussetzung können die verantwortlichen Personen über einen Incident-Management-Prozess schnell alarmiert werden. (RL)



**Christian Ehlen**

Consultant IT-Security bei Twinsec  
E-Mail: Christian.Ehlen@Twinsec.de



funkschau bei Facebook:  
Diskutieren Sie mit