

Security Information & Event Management (SIEM):

Wie aus Logfiles und Events geschäftsrelevante Informationen werden



von Pino Cuccaro,
Senior Security Consultant
bei der in Uster beheimateten
Sicherheitsspezialistin
bw digitronik ag

Obwohl zu einem guten Security Management auch die regelmässige Überprüfung dieser Logfiles zählt, ist es mit herkömmlichen Mitteln nahezu unmöglich, aus dieser Datenflut eine ganzheitliche Sicht über Bedrohungen oder Regelverstösse zu gewinnen. Denn bei jeder dieser Lösungen handelt es sich um Informationsinseln. Erschwerend zur riesigen Datenflut verlangen verschiedene Regularien Transparenz über die Güte der getroffenen Sicherheitsvorkehrungen. Mehr denn je brauchen Unternehmen automatisierte und Audit-konforme Auswertungen, um die Einhaltung der sicherheitsrelevanten Regularien zu beweisen.

Einen Lösungsweg bietet Security Information & Event Management (SIEM). SIEM befähigt Unternehmen, Log- und Event-Daten zentral zu sammeln, zu korrelieren und zu analysieren. So können Unternehmen die Einhaltung von Regularien überprüfen, den jeweiligen Security Status einsehen, und den Überblick über aktuelle Bedrohungen behalten.

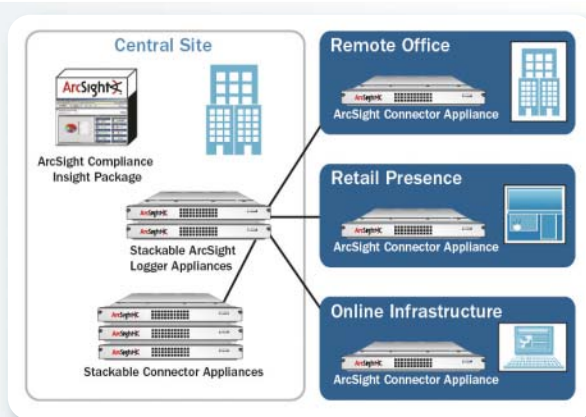
Eine SIEM Implementation ist dann erfolgreich, wenn man die richtigen Daten ins System einfliessen lässt. Dabei ergeben sich zwei Herausforderungen:

- Die Integration von Events aus Systemen, welche vom SIEM Hersteller nicht unterstützt werden.
- Die Verzögerung zwischen einem neuen Release eines schon überwachten Systems und der Unterstützung des neuen Release durch den SIEM Hersteller.

Vorsicht ist geboten, wenn ein SIEM Anbieter «out-of-the-box» nur eine kleine Anzahl von Event-Quellen unterstützt, oder nur einen einfachen Parser anbietet, der als komplette Ausstattung zur Entwicklung von eigenen Agenten angepriesen wird.

Täglich erscheinen Meldungen über Unternehmen, welche durch Cyberkriminelle geschädigt wurden. Um sich zu schützen, setzt man heute eine Vielzahl von Sicherheitssystemen ein, welche es zu überwachen gilt und jeden Tag eine Unmenge an Log- und Event-Meldungen generieren.

Die ArcSight Log Management Suite deckt sowohl die Bedürfnisse von KMU's wie auch jene von Enterprise Kunden ab, und skaliert auch in grossen heterogenen und weit verteilten Umgebungen.



Die Fähigkeit zur Datenkorrelation ist bei SIEM Lösungen ein überaus kritischer Punkt. Denn daraus ergeben sich die Messgenauigkeit, die automatischen Priorisierungen, die Identifikation von richtigen Bedrohungen und der Abgleich mit den Compliance Anforderungen. Bei der Auswahl einer SIEM Lösung sollte auf folgende Anforderungen Wert gelegt werden:

- Cross-Device Korrelation: zwingend notwendig
- Berücksichtigung der Vermögenswerte: Ist es im Korrelationsverfahren möglich, geschäftsrelevante Einflüsse und technische Wertkategorien abzubilden und diese zu korrelieren und zu priorisieren?
- Fähigkeit zur Entdeckung von Anomalien
- Auswertung- und Statistik-Funktionen
- Korrelation von neuen Regeln in Echtzeit: Kann die SIEM Lösung neue Regeln in Echtzeit mit schon gesammelten Events korrelieren?
- Verwertbare, voreingestellte Korrelationsregeln: Die Effektivität einer SIEM Lösung ergibt sich, wenn schon mit den voreinge-

stellten Korrelationsregeln ein grosserer Teil der Anforderungen abgedeckt wird.

- Benutzerfreundlichkeit bei der Erstellung und Anpassung der Regeln

Vor dem Einsatz einer SIEM-Lösung befasst sich die Security Abteilung eher selten mit Geschäftsprozessen. Erst mit der Einführung von SIEM wird ein Hauptaugenmerk darauf gelegt, weil man neuen Möglichkeiten erhält. So können Security-Informationen mit Geschäftsprozessen verknüpft werden. Viele Praxisbeispiele belegen, dass Unternehmen dank SIEM-Technologie ihre Reaktionszeiten auf Sicherheitsvorfälle von Stunden auf wenige Minuten reduzieren konnten. □

weitere Informationen

bw digitronik
E-SECURITY IS OUR MISSION

bw digitronik ag
Strickstrasse 15
8610 Uster
Tel. 044 905 48 50
verkauf@bwdigitronik.ch
www.bwdigitronik.ch