

# Security Event Management hat grosses Potenzial

Mit dem Einsatz klassischer IT-Schutzmassnahmen entsteht das Bedürfnis nach Transparenz und Gewissheit, dass die Massnahmen auch greifen. Oft scheitert dies jedoch an der Unmöglichkeit, die grossen Datenmengen verarbeiten und interpretieren zu können. *Urs Rufer*



**Urs Rufer**  
Leiter Consulting & Projects,  
terreActive

Die Meldungen über Sicherheitsvorfälle reisen nicht ab, die Angriffe werden immer brillanter, und zunehmend muss sich der Sicherheitsverantwortliche gegen Kriminelle zur Wehr setzen. Dass hier neben den klassischen Schutzmassnahmen wie Firewall, Verschlüsselung und Web-Entry-Server, um nur einige zu nennen, neue Ansätze zu verfolgen sind, ist heute bestens bekannt. Doch wie sieht diese Alarmanlage der IT-Infrastruktur und der Anwendungen aus? Einzelne Anbieter haben ihre Produkte mit Auswertungs- und Erkennungsmassnahmen versehen und bieten so eine Lösung für diese Herausforderung an. In vielen heterogenen Umgebungen hingegen reichen solche Insellösungen nicht aus, um sich ein umfassendes Bild der Sicherheit machen zu können. Es sind generelle Ansätze und Umsetzungen gefragt, die die Anforderungen an ein Security-Event-Management(SEM)-System abdecken.

## Logfiles als Quelle nützlicher Information

Während in der Vergangenheit Logfiles oft ein Übel für den Systemadministratoren darstellten und in der Regel baldmöglichst gelöscht wurden, wird diese Information heute als wertvolle Grundlage für SEM verwendet. Als Erstes sind die Logs zentral zu sammeln und zu normalisieren, das heisst mit einem einheitlichen Zeitstempel zu versehen und gemäss dem Log-Konzept zu typisieren. Gleichzeitig sind die Daten in der Originalform zur Weiterverarbeitung zu speichern. Nur so können Vorfälle auch zurückverfolgt werden. Denn diese Weiterverarbeitung, die sowohl automatisiert wie auch manuell erfolgen kann, ist der eigentliche Nutzen von SEM.

Bei der automatisierten Verdichtung der Logs werden Events modelliert, die sich aus den Grunddaten ableiten lassen. Dabei können spezielle Muster in Häufigkeit und zeitlichem Auftreten über verschiedene Quellen korreliert und gebildet werden. Solche Events werden dann typischerweise an überlegende Überwachungs- beziehungsweise Helpdesk-Systeme weitergeleitet. Bei der Definition der Events muss auf die individuellen

**«Bei der Definition der Events muss auf die individuellen Anforderungen der IT-Sicherheit eingegangen werden.»**

Anforderungen der IT-Sicherheit eingegangen werden. Es empfiehlt sich, die langjährigen Erfahrungen und Kenntnisse der Systembetreuer einfließen zu lassen. Damit lassen

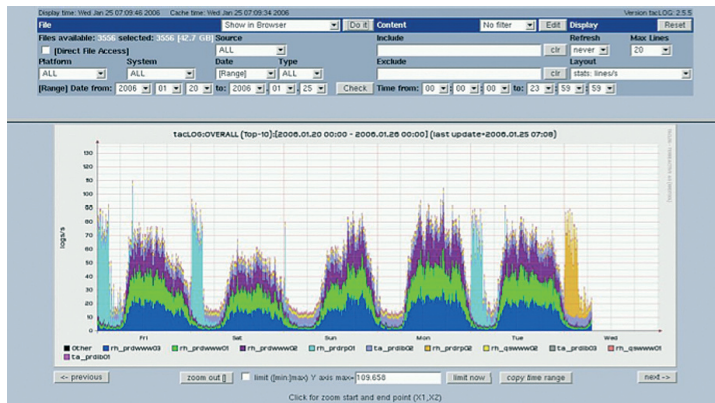
sich Routinarbeiten reduzieren, und die Suche nach Unregelmässigkeiten sowie die Entwicklung von neuen Events können intensiviert werden. Damit sind wir auch schon bei den manuellen Arbeiten angelangt, die sich auf die Analyse der Daten mit entsprechenden Werkzeugen beschränkt. Das Spektrum reicht dabei von forensischer Analyse über Untersuchungen von Fehlverhalten bis zur systematischen Erkennung der Abweichung vom Normalzustand.

## Die Anwendungsmöglichkeiten sind vielfältig

Die Gründe und Motivation zur Einführung eines SEM-Tools respektive zur Durchführung eines entsprechenden Integrationsprojekts sind vielfältig. In der Folge werden drei Szenarien erläutert, wie sie in konkreten Projekten vorgekommen sind.

### • Archivierung

In diesem Fall, wo das Netzwerk (LAN, WAN und Internetzugang) und die Basisdienste (DNS, Web-Proxy, E-Mail) einer grösseren Organisation an einen externen Partner vergeben wurden, ist im SLA ver-



Mit der Visualisierung der Log-Volumina und der Logs pro Sekunde wird versucht, die Abweichung vom Normalzustand zu eruieren

einbart, dass alle Logs der betreuten Systeme für eine bestimmte Zeitdauer (mindestens 180 Tage) archiviert werden müssen. Mit dem in der Einleitung beschriebenen Ansatz der Zentralisierung und Integration in ein Archivierungssystem konnte die Archivierungsanforderung einfach und effizient erreicht werden. Interessanterweise konnten gleichzeitig mit der Integration aller Log-Informationen zur Archivierung Fehlverhalten (beispielsweise falsche Zeitserver-Konfiguration) in der Infrastruktur erkannt werden, die nie aufgefallen waren, da den Logs keine Beachtung geschenkt wurde. Ein wichtiger Zusatznutzen von SEM zur Qualitätssteigerung von IT-Infrastrukturen.

#### • Audit Trail

Im Szenario «Beweissicherung» stehen regulatorische Vorgaben im Vordergrund. Dabei geht es darum, relevante Systemadministrationszugriffe und -manipulationen aufzuzeichnen. Oft haben Systemadministratoren im Banken- und Finanzumfeld uneingeschränkten Zugang zu Anwendungen und Systemen. Um die Administratoren zu entlasten, wurden im vorliegenden Fall die relevanten Daten von den Systemen an ein zentrales SEM-System geschickt und dort unwiderruflich gespeichert. Im Gegensatz zum vorangegangenen Fall mussten hier die Rohdaten ausgewertet und durch Modellierung entsprechender Events verdichtet werden. Als Events abgebildet wurden alle Aktivitäten, die mit erlaubtem und unerlaubtem Systemzugang, der Anpassung an Konfigurationsdaten und dem Manipulieren (Starten, Stoppen) von Prozessen zu tun hatten.

#### • Security Monitoring

In der Königsdisziplin des SEM wird versucht, aufgrund der gesammelten Daten auf sicherheitsrelevante Ereignisse zu schliessen, um Missbrauch zu erkennen. Während viele Sicherheitsevents aus bekannten Angriffsmustern abgeleitet werden können, besteht die grosse Herausforderung in der Erkennung von bis dato unbekanntem Angriffen. Ein viel versprechender Ansatz dafür ist die Erkennung der Abweichung vom Normalzustand. Doch was ist der Normalzustand? Je nach Grösse der Umgebung ist dies nicht einfach zu definieren, weshalb sich für diesen Ansatz überschaubare und stabile, nur wenigen Änderungen unterworfenen Umgebungen besonders gut eignen. Um die Abweichung zum Normalzustand eruieren zu können, haben sich die Visualisierung der Log-Volumina und der Logs pro Sekunde bewährt. Diese Kennzahlen werden grafisch über die Zeit dargestellt und erlauben so einen schnellen Überblick über das Verhalten, die sich als Unregelmässigkeiten in den periodischen Mustern erkennen lassen.

#### Ein SEM-Tool ist nur die halbe Miete

Obwohl obige Betrachtung zeigt, welche Möglichkeiten schon heute bestehen, ist das Entwicklungspotenzial noch sehr gross. Die Entwicklung fokussiert auf die grafische Darstellung und Auswertung der Daten, wobei nicht selten mehrere Gigabyte Daten visualisiert werden müssen. Ein weiterer Bereich ist die statistische Auswertung dieser Datenmenge, beispielsweise um seltene Ereignisse zu finden, die mit grosser Wahrscheinlichkeit von Bedeutung sind. Diese anspruchsvollen

Aufgaben entsprechen dem sprichwörtlichen Suchen der Nadel im Heuhaufen. Sie werden die Produktlieferanten und Integrationsfirmen noch lange beschäftigen.

Bei der Einführung und der Auseinandersetzung mit SEM ist es wichtig zu berücksichtigen, dass die Wahl des Produkts nur ein Teil der Lösung darstellt. Ebenso wichtig sind die Definition der Anforderungen und der Entscheidung, welches Szenario realisiert werden soll. Auch die Wahl eines Integrationspartners, der in der Lage ist, das Thema nicht nur technisch, sondern auch strategisch und konzeptionell zu begleiten, ist entscheidend. Gilt es doch, den Umfang so zu definieren, dass in kürzester Zeit erste Resultate vorliegen, die die IT-Sicherheit des Kunden nachhaltig verbessern. ■