

Security Event Management (SEM) im Finanzumfeld

Die sich ständig verändernde Bedrohungslage in der IT-Sicherheit führt zu einem stetigen Strom von neuen Abwehrsystemen, was die Komplexität der Sicherheitsinfrastruktur laufend erhöht. SEM wirkt der steigenden Komplexität entgegen und hilft den Überblick zu behalten. *Rolf Hefti*



Rolf Hefti

ist Leiter Produktmanagement
beim Sicherheitsspezialisten
terreActive AG
rolf.hefti@terreActive.ch
www.terreActive.ch

Sicherheit war schon immer ein zentraler Bestandteil eines Finanzinstitutes. Ob Bank oder Versicherung, alle wichtigen und vertraulichen Informationen lagern als elektronische Daten auf Servern und Datenspeichern aller Art. Natürlich wurde in den letzten Jahren vieles unternommen, um gerade die IT-Sicherheit zu verbessern und so den Missbrauch oder Verlust von Daten zu verhindern. Laut der aktuellen Studie «2005 Global Security Survey» von Deloitte wird IT-Sicherheit zur Chefsache. Die meisten Unternehmen haben eine etablierte Organisation, die sich mit dem Thema beschäftigt, wobei immer mehr Security Officers direkten Zugang zum obersten Management erhalten.

Gleichzeitig hat die Steigerung von Qualität und Häufigkeit der Sicherheitsrapporte einen positiven Einfluss auf die Sicht und das Beurteilungsvermögen der IT-Risiken durch den Verwaltungsrat. Diese Entwicklung kann auf den ständig wachsenden Druck von aussen, durch Vorgaben wie SOX oder Basel II, zurückgeführt werden und wird sich in den nächsten Jahren kontinuierlich verstärken.

Niemand will heute als unsicher gelten. Gerade in der Finanzbranche kann sich eine Sicherheitslücke verheerend auswirken. Zum Glück sind genügend Mittel vorhanden, um den ständig ändernden Anforderungen gerecht zu werden. Doch wie weit kann sich der Verwaltungsrat auf die Aussagen der Reports verlassen und welche Fragen sollte er sich dabei stellen? Beispielsweise sollte man die Informationsbasis der Reports überprüfen und die Erkenntnisse periodisch durch externe Audits kontrollieren. Weiter muss man die richtigen Kennzahlen überwachen, was bei einer sich laufend ändernden Bedrohungslage nicht einfach ist.

Das unsichtbare Risiko

Obwohl eine bessere IT-Sicherheit generell wünschenswert ist, dürfen die ständig wachsenden Anforderungen an die internen Ressourcen der Unternehmen nicht vergessen

werden. Bekannte Bedrohungsbilder werden laufend durch neue ersetzt, was wiederum neue Abwehrmassnahmen bedingt. Aktuell ist mit Produkten wie Application-Firewalls ein neues Kapitel aufgeschlagen worden. Doch wie soll eine gleich bleibende Betriebsorganisation die neuen Lösungen ständig integrieren und sinnvoll betreiben können? Dieser ständige Wettlauf überfordert immer mehr Unternehmen und führt zu einer Überlastung der Verantwortlichen.

Security Event Management (SEM) nimmt sich diesem Thema an und versucht, über Tools und Services dieser Entwicklung entgegenzuwirken.

Obwohl sich laut Deloitte die IT-Sicherheitsverantwortlichen auch 2005 noch am meisten vor Viren und Würmern fürchten, gibt es eine nur schwer messbare Entwicklung hin zu «unsichtbaren» Risiken, die vermehrt auch von innerhalb der Unternehmen ausgehen. Laut neusten Studien nehmen die internen Vorfälle laufend zu und gerade bei solchen Angriffen sind die genauen Kenntnisse der Umgebung eine grosse Hilfe. Diese Insider können ihre Spuren einfach vertuschen und so unerkannt bleiben.

Gewisse Banken gehen deshalb heute schon so weit, dass die sensibelsten Daten nicht mit dem lokalen Netzwerk verbunden sind. Eine abgeschlossene und physisch getrennte Welt bietet die höchste Sicherheit. Doch so weit kann man nicht überall gehen, bleibt doch ohne Zugriff auch vielfach der Nutzen der Daten auf der Strecke. So kommt man wieder zur ursprünglichen Fragestellung: Wie schützt man sich vor Gefahren, die man nicht kennt?

Schutztruppe unterstützen

Dazu muss man seine IT-Infrastruktur genau kennen und auch das typische Verhalten derselben verstehen. Wer ist wann in der zentralen Applikation eingeloggt, oder welche Transaktionen werden wann durchgeführt? Gleichzeitig braucht man Funktionen, um die-

ses sogenannte «Normalverhalten» aufzuzeigen und festzuhalten. Nur so kann man später ein Abweichen feststellen. SEM-Lösungen und -Services helfen, diese Fragen zu beantworten, und bieten die Basis, Angriffe zu erkennen. Ohne diese Hilfe ist auch die schlagkräftigste Schutzorganisation bei der Bekämpfung der «unsichtbaren Angriffe» machtlos.

Am ehesten lässt sich das Zusammenspiel von SEM-Lösung und -Organisation mit einem Beispiel aus dem Gebäudeschutz aufzeigen. Heute hat sicher jede Bank eine Alarmanlage, die einen Einbruch erkennt und sofort die spezialisierte Schutztruppe, meist Polizei oder Sicherheitsdienst, aufbietet. SEM arbeitet auch wie eine Alarmanlage, die einen vermeintlichen Angriff erkennt und dann die entsprechenden Alarme der Schutztruppe übergibt.

Die SEM-Lösung muss dazu über eine gewisse Zeit in Betrieb sein und von Spezialisten mit den nötigen Informationen gefüttert werden. Dies ist nicht eine einmalige Angelegenheit, denn die Einbrecher haben nicht wie im realen Leben eine klare Gestalt, sondern können immer wieder in neuer Form auftreten. Die Sicherheit wird schlussendlich durch die Qualität der Organisation und das Know-how der Schutztruppe definiert. Doch ohne eine leistungsfähige SEM-Lösung bleiben die besten Augen blind.

Eine SEM-Lösung analysiert ständig das Verhalten der IT-Infrastruktur und verfügt dazu über die folgenden Grundfunktionen:

- Normalisierung und zentralisierte Eventdaten-Speicherung
- Zentrale Archivierung der Daten
- Manuelle Analyse und Berichterstellung
- Datenkorrelation und automatisierte Event-Generierung
- Reports für Compliance, Audits und Management

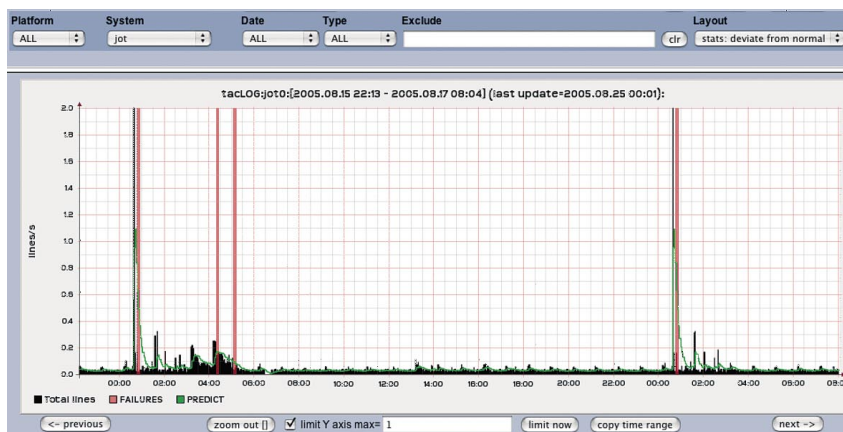


Abbildung 2: Die grafische Darstellung der Abweichungen vom Normalbetrieb

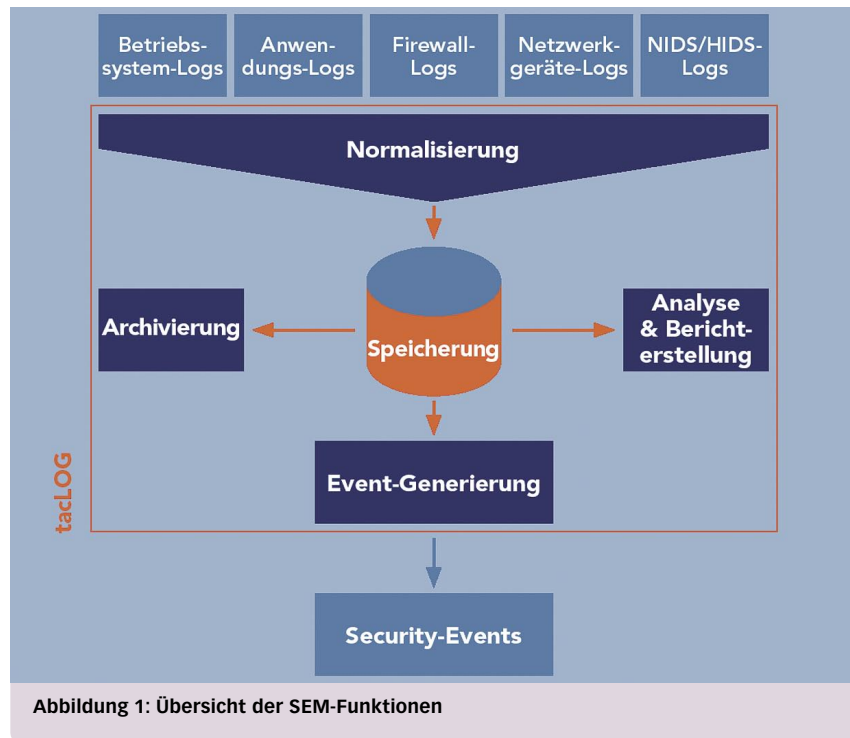


Abbildung 1: Übersicht der SEM-Funktionen

Die Performance der Lösung ist entscheidend, weil auf einen Vorfall sofort und nicht erst im Nachhinein reagiert werden muss.

Zusätzlich zu den Real-Time-Auswertungen nehmen die Reportingfähigkeiten für Audits und die Erfüllung von regulatorischen Vorgaben wie SOX oder Basel II ständig an Wichtigkeit zu. Auch das Management will wissen, welche Bedrohungen tatsächlich existieren und wie sie sich entwickeln. Richtig eingesetzt, erlaubt die SEM-Lösung nicht nur das Ertappen von Einbrechern auf der frischen Tat, sondern spart auch enormen Aufwand bei der Erfüllung der vielseitigen Reportinganforderungen.

Eine der schwierigsten Aufgaben ist das Erkennen von «unbekanntem Angriffen». Dabei

muss der Vorfall als Abweichung vom «Normalbetrieb» erkannt werden, was für den Verantwortlichen nur durch eine optimierte Visualisierung der enormen Datenmengen möglich wird. Die grafischen Hilfsmittel ermöglichen erst eine schnelle Eingrenzung des Problemfalls und erlauben auch historische Daten schnell mit den aktuellen Informationen zu vergleichen. Ist eine Abweichung gefunden, müssen über «drill down»-Funktionen die einzelnen Daten zurückverfolgt werden können, um möglichst schnell den Grund des Vorfalls zu kennen.

Typische SEM-Services innerhalb eines Projekts sind:

- Beratungen, SEM-Konzepte und -Architekturen
- Security Event Reporting
- Managed SEM-Lösungen

Eine erfolgreiche Implementation von SEM-Lösungen ist keine einfache Sache. Der grösste Nutzen liegt im umfassenden Einsatz über die gesamte IT-Infrastruktur hinweg. Dabei sind immer auch verschiedene Abteilungen mit unterschiedlichen Interessen betroffen. Nur eine starke Projektführung kann alle Interessen hinter dem Projekt vereinen und es erfolgreich umsetzen. Im späteren Betrieb können externe Spezialisten die Schutzorganisation durch punktuelle Unterstützung effizienter und leistungsfähiger machen. Denn SEM hat nicht nur das Ziel, die IT-Sicherheit zu verbessern, sondern soll auch die internen Ressourcen entlasten.