

## INTERVIEW

# Bei Datenschutz auf Nummer sicher

Werden Bedrohungen übersehen oder bestimmte Vorschriften oder Regeln nicht befolgt, kann sich dies mittel- oder unmittelbar für das Unternehmen in hohen betriebswirtschaftlichen Schäden niederschlagen. Security Information and Event Management (SIEM) bietet wichtige Mechanismen, solchen Schäden entgegenzuwirken.

Das Interview führte Dr. Andreas Bergler



ALFRED KOCH, Senior Manager Advisory  
bei der KPMG AG



NORBERT DRECKER, Geschäftsführer  
von Twinsec

ITB: Herr Koch, was macht SIEM so unverzichtbar?

KOCH: In dem Maß, wie Bedrohungen von innen und außen wachsen sowie Vorschriften und Regularien zunehmen, müssen Unternehmen die Überwachung, Alarmierung und Protokollierung von sicherheitsrelevanten Ereignissen professionalisieren. Die Herausforderung besteht darin, Wesentliches von Unwesentlichem zu unterscheiden, um später in der Event-

flut niemals den Überblick zu verlieren. Nur so ist das Kontroll-, Alarmierungs- und Protokollierungssystem effektiv und effizient einsetzbar. Um eine angemessene Sicherheit etablieren zu können, müssen natürlich sämtliche Anforderungen und Vorgaben bezüglich Security, Compliance und Datenschutz von der Geschäftsführung vorliegen.

ITB: Wie sollte das Unternehmen so ein Projekt anpacken?

KOCH: Es sollte nachvollziehen, wie die Geschäftsprozesse laufen, welche Daten dabei bewegt werden und welche Mitarbeiter daran beteiligt sind. Die Ausgangsfrage hier: Wie kritisch sind die einzelnen Datenbestände für Security, Compliance und den Datenschutz? Diese Frage lässt sich nur aus geschäftlicher Sicht beantworten. Denn nur hier können mögliche Sicherheitsmängel zu finanziellen Risiken in Beziehung gesetzt werden. Auch die Wechselwirkungen von Risiken und deren Gesamtfolgen können aus dieser Warte besser analysiert und quantifiziert werden. Außerdem wird entlang der Geschäftsprozesse transparent, wer mit geschäftskritischen oder sensiblen Daten arbeitet, um auch dort den Sicherheitshebel anzusetzen. Nur Top-down klärt sich das Bild, wo es überhaupt lohnt, Vorkehrungen zu treffen. Bei gesetzlichen Vorschriften ist dies anders. Sie müssen in jedem Fall befolgt werden. Die Vorkehrungen, die getroffen werden sollten, sind erst einmal nicht technischer Natur.

ITB: Als da sind?

**KOCH:** Neben technischen Events, die auf Sicherheitsmängel hinweisen können, erweist sich die Einführung bestimmter Prozesse und Regeln als hilfreich. Es sollte hinterfragt werden, welche davon bereits bestehen, welche verändert oder ergänzt werden sollten und was für einen sichereren und besser nachvollziehbaren Umgang mit den Daten eingeführt werden sollte. Angemessene Prozesse und Regeln tragen wesentlich zu mehr Security, Compliance und Datenschutz bei.

**ITB:** Wie findet man die passenden Kontroll-, Alarmierungs- und Protokollierungslösungen?

**KOCH:** Mit der Kenntnis der schutzwürdigen und risikobehafteten Datenbestände kann auf deren Position innerhalb des IT-Geflechts geschlossen werden. Dadurch wird klar, welche Systeme als Event-Geber von Interesse sind. Das können innerhalb der IT-Infrastruktur bestimmte Applikationen, Dienste, Datenbanken, Middleware-Komponenten, Betriebssysteme sowie Netzwerk- und Netzwerkperipherie-Komponenten sein. Die wichtigen Event-Geber sollten in Form einer IT-Landkarte dokumentiert werden. Andere, für Security, Compliance und Datenschutz nicht relevanten Systeme können die Projektverantwortlichen bei der Ausgestaltung einer SIEM-Lösung aussparen. Diese überlegte und gezielte Vorgehensweise wirkt von vornherein einer Flut an Events an der zentralen Konsole entgegen.

**ITB:** Herr Drecker, wie wichtig ist es, die Fachabteilungen ins SIEM-Projekt einzubinden?

**DRECKER:** Diese Einbindung kann gar nicht hoch genug bewertet werden. Die Fachabteilungen kennen am besten ihre Datenbestände, die damit verbundenen Sicherheitsrisiken sowie ihre Security-, Compliance- und Datenschutzaufgaben. Außerdem entscheidet sich in den Fachabteilungen, in welcher Qualität künftig die Einhaltung dieser Auflagen umgesetzt wird. Natürlich setzt die Einbindung aller Fachabteilungen, die an Security, Compliance und Datenschutz mitwirken, im Projektverlauf eine professionelle Koordination und eine permanente Prüfung der Zwischenergebnisse voraus. Eine dieser Fachabteilungen ist der IT-Bereich, in dessen Obhut künftig das SIEM-System stehen wird.

**ITB:** Inwieweit unterscheidet sich die Einbindung der IT-Abteilung von der anderer Fachabteilungen?

**DRECKER:** Die IT-Abteilung sollte erst ins Projekt involviert werden, wenn das gesamte fachliche Konzept steht und der Zuschnitt der künftigen SIEM-Lösung bekannt ist. Dann sollten auch hier die Prozesseigner bestimmt und entlang der Prozesse angeordnet werden. Nur so verschaffen sich die Projektverantwortlichen ein genaues Bild darüber, wer an welchen Informations- und Alarmierungsprozessen mitwirken soll. Das ist allerdings nur möglich, wenn zuvor genau festgelegt worden ist, welche Events, daneben Transaktionen und Aktivitäten, überwacht und protokolliert werden sollen. Die zuvor entwickelte IT-Landkarte für

einen bedarfsgerechten Zuschnitt der SIEM-Lösung – soviel wie notwendig, aber nicht mehr als nötig – leistet dafür hervorragende Dienste. Darüber hinaus empfehle ich, Alarmierungsregeln für besonders kritische Ereignisse festzulegen und zu dokumentieren. Das steigert später, dann, wenn es darauf ankommt, nochmals den Durchblick an der Konsole und die Reaktionsgeschwindigkeit beim Risiko-Ausschluss. Natürlich sollte die Produktentscheidung für das SIEM-Toolset erst dann getroffen werden, wenn der gesamte Lösungszuschnitt steht, also das technische Bedarfsprofil genau bekannt ist. Das erspart unnötige Investitionen, gestaltet den Betriebsaufwand so gering wie möglich und trägt zur Investitionssicherung bei.

**ITB:** Was macht die SIEM-Lösung mit ihren Werkzeugen zu einem verlässlichen Frühwarnsystem und zu einer revisions-sicheren Protokollierungsinstanz?

**DRECKER:** Dadurch, dass die Analysen und Auswertungen direkt ins Kontrollsystem mit den dort hinterlegten Sicherheits-, Compliance- und Datenschutzregeln einfließen, entsteht automatisch ein Frühwarnsystem. Über die Zeit erstellt so die SIEM-Lösung eine umfassende Protokollierung und eine revisions-sichere Ablage. Die für Security, Compliance und Datenschutz angesammelten, aussagekräftigen Informationen können darüber hinaus in Form eines Langzeitarchivs für historische Analysen und Auswertungen herangezogen werden. □

SIEM-Systeme müssen passgenau auf die Unternehmensbedürfnisse zugeschnitten werden, bevor die Produktentscheidung selbst ansteht.