

# Risiken besser unter Kontrolle

Security Information and Event Management (SIEM) kann für mehr Sicherheit, Compliance und Datenschutz im Bankensektor sorgen. Doch wie finden Finanzinstitute den richtigen Zuschnitt dieser kombinierten Überwachungs-, Alarmierungs- und Protokollierungslösung?

**BANKMAGAZIN:** Herr Koch, wie sollte die Bank ein SIEM-Projekt am besten anpacken?

**Koch:** Am Anfang sollte die Analyse stehen, wie kritisch einzelne Datenbestände für Security, Compliance und Datenschutz sind. Diese Analyse sollte von den Geschäftsprozessen der Bank ausgehen. So ist es am besten möglich, potenzielle Risiken und ihre möglichen Folgen für die Geldgeschäfte einzuordnen, zu quantifizieren und zu bewerten. Zudem können aus Geschäftsprozesssicht die Wechselwirkungen von Risiken und deren Folgen aufgedeckt und angemessen beurteilt werden.

**BANKMAGAZIN:** Wie hilft dies den Projektverantwortlichen weiter?

**Koch:** Gefahren und Schäden können auch von internen Mitarbeitern ausgehen, ob beabsichtigt oder unbeabsichtigt. Das gilt für Security, Compliance und Datenschutz gleichermaßen. Also sollten an den Schnittstellen zwischen „Mensch“ und „IT“

geeignete Vorkehrungen in Form festgelegter Prozesse und Regeln getroffen werden, an die sich die Mitarbeiter später halten müssen. Solche Vorkehrungen können in einem hohen Maß zu mehr Sicherheit, Compliance und Datenschutz innerhalb des Geldinstituts beitragen.

**BANKMAGAZIN:** Wie gelangen die Projektverantwortlichen zum richtigen Zuschnitt der SIEM-Lösung?

**Koch:** Durch die Top-down-Analyse erkennen die Projektverantwortlichen, bei welchen Datenbeständen es sich lohnt, den technischen Sicherheitshebel in Form des SIEM-Systems mit seiner integrierten Überwachungs-, Alarmierungs- und Protokollierungsintelligenz anzusetzen. Bei gesetzlichen Vorschriften ist dies anders: Sie müssen stets eingehalten werden. Von einzelnen Geschäftsprozessen ausgehend kann auf den Speicherort dieser Datenbestände innerhalb der IT geschlossen werden. Ebenso auf die Systeme, die diese

Datenbestände verarbeiten oder übertragen. Das können sowohl Applikationen als auch Dienste, Datenbanken, Middleware-Komponenten, Betriebssysteme, Netzwerk- und Peripheriekomponenten sein.

**BANKMAGAZIN:** Herr Drecker, diese Systeme dienen später als Informationsgeber für die SIEM-Lösung?

**Drecker:** Ja. Alle anderen Systeme können als Event-Geber bei der Ausgestaltung der SIEM-Lösung ausgespart werden. Der Lösungszuschnitt ist so von vorneherein schlank und für die Bank wirtschaftlich. Das Überwachungspersonal kann später im Betrieb gezielt auf wichtige, alarmträchtige Ereignisse reagieren.

**BANKMAGAZIN:** Was sollte organisatorisch für eine erfolgreiche Abwicklung des Projekts bedacht werden?

**Drecker:** Es ist wichtig, die Fachabteilungen von Anfang an einzubeziehen. Sie kennen für ihren Fachbereich am besten die Security-, Compliance- und Datenschutzerfordernungen. Um über alle drei Etappen eine angemessene und verlässliche Sicherheit etablieren zu können, muss natürlich auch die Geschäftsführung aktiv werden. Von ihr müssen gemäß der Geschäftsstrategie die generellen Anforderungen und Vorgaben für die SIEM-Projekte kommen. ↙

Mit Alfred Koch (links), Senior Manager Advisory bei der KPMG AG, und Norbert Drecker (rechts), Geschäftsführer von TWINSEC, sprach Hadi Stiel, freier Journalist und Kommunikationsberater in Bad Camberg.

