

Mit Security Information and Event Management auf der sicheren Seite

## Wachsender Druck zur Selbstkontrolle

geldinstitute hat sich mit Alfred Koch, Senior Manager Advisory bei der KPMG AG, und Norbert Drecker, Geschäftsführer von TWINSEC, über die Planung, Umsetzung und Einführung eines Security-Information- und Event-Management-(SIEM-)Systems unterhalten.

Die Banken sehen sich mit einem zunehmenden Compliance-Druck konfrontiert. So fordern Politik und Gesellschaft angesichts der Staatsschulden- und Eurokrise, die Geldinstitute und Finanzmärkte stärker zu regulieren. Parallel wächst der Druck auf die Institute, mehr Transparenz in ihre Geschäfte zu bringen und mit mehr Eigenkapital auf steigende Risiken bei schwer zu kalkulierenden Finanzmarktgeschäften zu reagieren. Gleichzeitig steigt der Außendruck auf die Institute, in puncto Datensicherheit und Datenschutz nichts anbrennen zu lassen.

Security Information and Event Management, kurz: SIEM, kann in den Geldinstituten angesichts dieser Entwicklung eine Schlüsselrolle einnehmen. SIEM eröffnet Überwachungs-, Alarmierungs- und Protokollierungsfunktionen, um die steigenden Compliance-, Sicherheits- und Datenschutzerfordernungen nachweislich zu erfüllen.

**Herr Koch, die Zahl der Regelungen, die Banken bis in letzter Konsequenz befolgen müssen, wird wohl deutlich zunehmen – oder?**

**Alfred Koch:** Angesichts der Schulden- und Eurokrise, der immer hektischeren Ausschläge an den Finanzmärkten und einer sich wenig erholenden Weltwirtschaft ist mit regulatorischen Eingriffen für Banken auf EU-Ebene zu rechnen. In den USA müssen die Institute ja bereits Kreditgeschäfte und Investment-Banking als separate Profitcenter trennen. Die notwendige Eigenkapitalquote für US-Banken wurde per Gesetz kräftig angehoben. Und, ganz aktuell: Ein nicht zweckgebundener, also spekulativer, Derivatehandel mit Rohstoffen wird in den USA voraussichtlich untersagt werden.

Die Etablierung der neuen europäischen Finanzaufsichtsbehörde, ESFS (European Financial Stability Facility) mit allen Unterbehörden weist hier auf ähnliche Überlegungen hin. Eine organisatorische Trennung von Kredit- und Investmentgeschäften und damit ein Abschied von Universalbanken wird aktuell intensiv diskutiert. Kontrovers diskutiert wird zudem eine



Alfred Koch, Senior Manager Advisory bei der KPMG AG.

Eigenkapitalquote, die weit über die Vorgaben von Basel III hinausreicht und vor allem kurzfristig aufgebaut werden soll. Laut der Absichtserklärungen des Eurogipfels sollen europäische Banken bis Mitte 2012 eine Eigenkapitalquote von neun Prozent erreichen. Auch der spekulative Derivatehandel mit Rohstoffen wird innerhalb der EU immer lauter in Frage gestellt. Ungedekte Leerverkäufe von Staatsanleihen wurden bereits in einigen Eurostaaten, zum Beispiel in Deutschland, verboten oder zumindest ausgesetzt. Nicht zu vergessen die Diskussion, inwieweit Banken und andere Finanzmarktteilnehmer über die Einführung einer Transaktionssteuer ihren Part zur Krisenfinanzierung beisteuern sollten.

*„Das SIEM-System der Wahl sollte die notwendige Flexibilität mitbringen, um nicht nur die heute bestehenden Regelungen umzusetzen. Dazu zählen Basel III, MaRisk (Mindestanforderungen an das Risikomanagement), SolvV (Solvabilitätsverordnung) der Säulen I und II für Stresstests sowie MiFID (Markets in Financial Instruments Directive) für einen geregelten Wertpapierhandel und Anlegerschutz.“ Alfred Koch*

**Was bedeutet dies für deutsche Geldinstitute?**

**Alfred Koch:** Sie werden vermutlich ihr bisheriges Kontrollinstrumentarium erweitern oder neu ausrichten müssen, um jederzeit und in voller Breite die Einhaltung von Regelungen überwachen und verbindlich dokumentieren zu können. Das technische Instrumentarium von SIEM – überwachen, auswerten, alarmieren und protokollieren – bietet dafür hervorragende Ansatzpunkte. Es greift permanent und automatisch auf die relevanten System- und Event-Logs zurück und qualifiziert sie in für die Befolgung von Regelungen oder für das Geschäft wichtige alarmträchtige Ereignisse.

**Muss damit nicht auch das SIEM-System technisch die Spanne zwischen heute und morgen abdecken?**

**Alfred Koch:** Genau darum geht es: Das SIEM-System der Wahl sollte die notwendige Flexibilität mitbringen, um nicht nur die heute bestehenden Regelungen umzusetzen. Dazu zählen Basel III, MaRisk (Mindestanforderungen an das Risikomanagement), SolvV (Solvabilitätsverordnung) der Säulen I und II für Stresstests sowie MiFID (Markets in Financial Instruments Directive) für einen geregelten Wertpapierhandel und Anlegerschutz. Auch die möglichen Anforderungen von morgen müssen sich schnell und angemessen in die SIEM-Systeme und Prozesse integrieren lassen. Bereits jetzt werden zum Beispiel alle Kreditinstitute gemäß Säule II nicht nur verpflichtet, wahrscheinliche, sondern auch außergewöhnliche plausible Ereignisse technisch in ihre Stresstests einzubeziehen.

Die richtige Wahl des SIEM-Systems einschließlich der Prozesse und Governance ist somit für die Bank eine strategische Entscheidung, mit direkten kurz-, mittel- und langfristigen Auswirkungen auf die Qualität der Regelkonformität und somit letztlich auch auf deren Geschäft, Rating und Reputation. Richtig ausgewählt, deckt das SIEM-System auf Dauer nicht nur die regulatorischen Compliance-Anforderungen ab, sondern verbessert zugleich „Datensicherheit“ und „Datenschutz“ verlässlich.

**Herr Drecker, worauf sollten die Entscheider bei der Auswahl des SIEM-Systems achten?**

**Norbert Drecker:** Das Analystenhaus Gartner gibt für die Auswahl eines professionellen SIEM-Systems wesentliche Hilfestellungen. So sollte es mit seinen Grundfunktionalitäten in der Lage sein, sich flexibel den Geschäfts- und organisatorischen Veränderungen anzupassen. Dafür sollten nach Gartner die Entscheider besonders ihr Augenmerk auf die Anschaffungskosten, den Ausrollprozess, die technische Unterstützung der IT-Organisation sowie die Integrationsfähigkeit gegenüber der System- und Applikationsinfrastruktur legen. Außerdem empfiehlt das Analystenhaus, eine zwei- bis dreijährige Roadmap zu entwickeln, in die auch künftig geforderte oder wahrscheinliche Funktionen Eingang finden sollten. Außerdem rät Gartner den Verantwortlichen für ihre Einsatzzwecke die Grundfunktionalitäten wie System- und Event-Log-Erfassung, Korrelationsmaschine, Event Mapping nach vorgegebenen Regeln für die Klassifizierung von Informationen sowie Monitoring und Reporting genau zu prüfen.

**Längst nicht alle Geschäftsprozesse der Bank laufen durchgehend IT-gestützt ab. Dazwischen gibt es viele manuelle Brüche. Greift damit nicht an diesen Stellen das automatische Sammeln von System- und Event-Logs als Informationsgeber für Compliance, Datensicherheit und Datenschutz zwangsläufig zu kurz?**

**Norbert Drecker:** Ja. Deshalb ist es bei der Pro-

jektierung des SIEM-Systems so wichtig, für die Arbeitsschritte, die nicht IT-gestützt ablaufen, geeignete Vorkehrungen zu treffen. Mit Blick auf die Einhaltung von Compliance-, Sicherheits- und Datenschutzanforderungen müssen angemessene Abläufe und Verfahrensregeln definiert und realisiert werden. Und sie müssen anschließend von den Mitarbeitern nachweislich eingehalten werden, was regelmäßige Prüfungen voraussetzt.

Nur wenn beide Seiten, die technische und die nichttechnische, nahtlos und garantiert zusammenspielen, wird die Bank die gesetzten Projektziele, mehr Regelkonformität in allen Bereichen – Compliance, Datensicherheit, Datenschutz – erreichen können.

**Was sollte bei der Analyse der Geschäftsprozessabschnitte bedacht werden, die IT-gestützt ablaufen?**

**Norbert Drecker:** Sie sollten, ebenso wie die nicht IT-gestützten Abläufe, top-down analysiert werden. Nur so wird deutlich, welchen Stellenwert einzelne Abschnitte einzeln wie in ihrer Abfolge für Compliance, Datensicherheit und Datenschutz haben. Top-down wird für die Projektverantwortlichen außerdem transparent, welche Systeme, Anwendungen, Dienste, Datenbanken, Middleware-Komponenten, Betriebssysteme, Netzwerkkomponenten, Peripheriekomponenten für Event-ogs und System-Logs herangezogen werden sollten, weil Nutzer darauf zurück- oder zugreifen.

Die Top-down-Vorgehensweise ebnet den Weg zu einer schlanken Überwachungs-, Alarmierungs- und Protokollierungslösung und erspart so dem Geldinstitut unnötige Investitionen und Aufwendungen. Und, zwar trivial, aber wichtig zu bedenken: Wenn die Maßnahmen nach einer Alarmierung nicht klar definiert werden und



**Norbert Drecker**, Geschäftsführer von TWINSEC.

später umsetzbar sind, kann man sich die angestrebte Lösung gleich ganz sparen.

**Können Sie genauer darauf eingehen, wie dieses schlanke Kontroll- und Alarmierungssystem erreicht werden kann?**

**Norbert Drecker:** Eine wichtige Aufgabe derartiger Projekte ist es, genau abzuwägen, wo eine technische Integration von Systemen als Informationsquelle in die SIEM-Lösung wirtschaftlich sinnvoll ist und wo nicht. Dort, wo die Risiken gering ausfallen oder im Fall ihres Auftretens nur geringe wirtschaftliche Auswirkungen für die Bank nach sich ziehen, kann aus Kosten-Nutzen-Aspekten oft auf eine Integration verzichtet werden. Das Gleiche gilt für die Bereitstellung von Informationen aus nicht IT-gestützten Abläufen und Regeln für das Kontroll- und Alarmierungssystem. Gehen die Projektverantwortlichen auf diese Weise vor, senkt das Unternehmen das Risiko von zu komplexen Gesamtlösungen und reduziert zugleich das Risiko zu hoher Projektinvestitionen und später zu hoher Betriebskosten.

Mit Blick auf die Einhaltung rechtlicher Bestimmungen ist dies anders. Solche Regelungen müssen verbindlich und nachprüfbar befolgt werden, auch wenn die Kosten dagegensprechen. ■

Das Interview führte Hadi Stiel, freier Journalist und Kommunikationsberater in Bad Camberg.

*„Das Analystenhaus Gartner gibt für die Auswahl eines professionellen SIEM-Systems wesentliche Hilfestellungen. So sollte es mit seinen Grundfunktionalitäten in der Lage sein, sich flexibel den Geschäfts- und organisatorischen Veränderungen anzupassen.“* **Norbert Drecker**