

# Top-Down zu mehr Sicherheit

Sicherheit, Compliance und Datenschutz gewinnen für Unternehmen an Bedeutung. Werden die drei Flanken nicht hinreichend gedeckt, drohen mittel- oder unmittelbar geschäftliche Nachteile und Schäden.

> Eine wohlgedachte Kontroll- und Alarmierungslösung trägt im Unternehmen zu mehr Sicherheit, Compliance und Datenschutz und somit zur Abwendung finanzieller Schäden bei. IT-DIRECTOR unterhielt sich mit Alfred Koch, Senior Manager IT Advisory bei KPMG, und Norbert Drecker, Geschäftsführer von Twinsec, über die dafür nötige Grundvoraussetzung: den richtigen Zuschnitt der Komplettlösung.

**IT-DIRECTOR:** Mit welchen Schwierigkeiten sehen sich Unternehmen bei der Errichtung eines Kontroll- und Alarmierungssystems konfrontiert?

**A. Koch:** Mit fortschreitender Automatisierung von Prozessen und dem Einsatz von Maschine-zu-Maschine-Komponenten (M2M) zur Steuerung von Abläufen verändern sich in der Regel die Rahmenbedingungen für die Sicherheits-, Compliance- und Datenschutzsysteme. Eine technische Kontroll- und Alarmierungslösung kann hier sicher einen wertvollen Beitrag zur effizienten Gestaltung leisten. Dies jedoch nur, wenn es gelingt, sie in vorhandene Sicherheits- und Kontrollstrukturen zu integrieren.

**IT-DIRECTOR:** Können Sie konkreter werden?

**A. Koch:** Bei wesentlichen Prozessänderungen sollte zunächst untersucht werden, welche neuen bzw. veränderten Risiken sich ergeben und welche Auswirkungen sie auf Governance, Prozesse und Regelwerke der unternehmensinternen Kontroll- und Überwachungssysteme haben. Im nächsten Schritt kann dann entschieden werden, welche Anpassungen und Ergänzungen der Sicherheits-, Compliance- und Datenschutzmaßnahmen erforderlich sind und ob der Einsatz einer technischen Kontroll- und Alarmierungslösung wie SIEM (Security Information and Event Management) zielführend ist.



**Alfred Koch**, Senior Manager  
IT Advisory bei KPMG



**Norbert Drecker**, Geschäftsführer  
von Twinsec

**IT-DIRECTOR:** Wie sollten Unternehmen ihr Projekt vor diesem Hintergrund aufziehen?

**A. Koch:** Nutzen und Qualität einer SIEM-Lösung hängen davon ab, ob aus der Flut an IT-Ereignissen und IT-Transaktionen genau die für das Unternehmen relevanten Ereignisse überwacht, protokolliert und gemeldet werden. Dies gelingt am besten, wenn die Projektverantwortlichen sowohl über ein klares Verständnis der Geschäftsprozesse und der mit dem Geschäftsmodell und den Prozessen verbundenen Risikopotentiale verfügen und Klarheit hinsichtlich zu erfüllender gesetzlicher Anforderungen und Auflagen besteht.

**IT-DIRECTOR:** Inwieweit profitieren Unternehmen von der Top-Down-Vorgehensweise?

**A. Koch:** Sie beugen so einer Informationsflut aus der IT heraus vor. Die künftigen Analysen, Auswertungen und Reaktionen orientieren sich eng an den Geschäftsprozessen. Genau hier entscheidet sich, in welchem Maß das Unternehmen von den zu etablierenden Sicherheits-, Compliance- und Datenschutzmaßnahmen profitiert.

Eine angemessene Gewichtung und Dimensionierung aller drei Säulen – Prozesse, Regeln, IT-Informationen – und eine insgesamt für die Verantwortlichen transparente Kontroll- und Alarmierungslösung sind weitere Vorteile der Top-Down-Vorgehensweise.

**IT-DIRECTOR:** Bedeutet Top-Down auch, dass das Projekt bei der Geschäftsführung aufgehängt werden sollte?

**A. Koch:** Unbedingt. Geschäftsstrategien und Businesspläne haben wesentlichen Einfluss auf die Risikobewertung und auf eine angemessene Ausprägung der Sicherheits-, Compliance- und Datenschutzmaßnahmen. Das Vorhaben ist also buchstäblich ein strategisches Projekt, bei dem direkt an die Unternehmensführung berichtet werden sollte.

**IT-DIRECTOR:** *Nicht jede Maßnahme wird lohnen. Investitionen auf der einen Seite und der Nutzen auf der anderen müssen in einem budgetverträglichen Verhältnis stehen. Wie kommen Unternehmen diesem Nutzen am besten auf die Spur?*

**A. Koch:** Auch dafür ist die skizzierte Top-Down-Vorgehensweise der richtige Ansatz. Über die Geschäftsprozesse können betriebswirtschaftliche Kriterien für die Bemessung und Bewertung des Sicherheits-, Compliance- und Datenschutznutzens herangezogen werden. Noch mehr: Entlang der Geschäftsprozesse können auch die Wechselwirkungen potentieller Risiken ermessen und beurteilt werden. Top-Down wird also deutlich, welche Risiken für das Unternehmen relevant sind und welche lediglich geringe Schadenspotentiale bergen. So erhält die Kontroll- und Alarmierungslösung einen schlanken, wirtschaftlichen und rentablen Zuschnitt, weil nur handfeste Risiken und Wechselrisiken angepackt werden. Bei gesetzlichen Vorschriften ist dies anders. Deren Einhaltung ist vom Unternehmen durch geeignete Prozesse, Regeln sowie Kontroll- und Überwachungsmechanismen in jedem Fall sicherzustellen.

**IT-DIRECTOR:** *Herr Drecker, plädieren auch Sie für die Top-Down-Vorgehensweise?*

**N. Drecker:** Ja. Gerade bei Sicherheit, Compliance und Datenschutz mit oft nur mittelbarem geschäftlichen Nutzen sollten die Investitionen einer betriebswirtschaftlichen Bewertung standhalten. Werden zu viele Prozesse, Regeln und IT-Informationsgeber etabliert, gehen später im Betrieb nicht nur der Überblick und die Aussagefähigkeit verloren. Das Kontroll- und Alarmierungssystem wird dadurch auch zu kostspielig und pflegeaufwendig. Anders mit dem Top-Down-Ansatz: Alle Risiken und deren potentiellen Folgen können aus kaufmännischer Sicht bemessen und bewertet werden. Anschließend kann man einzelne Risiken bewerten, angehen oder schlicht akzeptieren. Es können angemessene Policies zur Kompensation der Risiken aufgesetzt oder Maßnahmen zur Kontrolle der Risiken eingeführt werden.

**IT-DIRECTOR:** *Inwieweit sollten die Fachabteilungen bei derartigen Projekt mitwirken?*

## „Geschäftsstrategien und Businesspläne haben wesentlichen Einfluss auf die Risikobewertung.“

**Alfred Koch** von KPMG

**N. Drecker:** Ihre Beteiligung an diesen Projekten ist unverzichtbar. Die Fachverantwortlichen kennen den Status quo sowie das Anforderungsprofil für mehr Sicherheit, Compliance und Datenschutz innerhalb ihres Wirkungsbereichs am besten. Nicht-technische Prozesse und Regeln fallen ebenfalls in ihre Zuständigkeit. Über die Fachabteilungen wird das tatsächliche Risiko- und Bedrohungspotential im Unternehmen deutlich. Die Prozesseigner, die bei Regelverstößen alarmiert werden müssen, sind ebenfalls in den Fachabteilungen angesiedelt. Außerdem ist eine übergreifende Koordination von Prozessen und Regeln nur in enger Projektzusammenarbeit mit den Fachabteilungen möglich, die an den jeweiligen Geschäftsprozessen mitwirken.

**IT-DIRECTOR:** *... und die IT-Abteilung?*

**N. Drecker:** Sie ist eine der Fachabteilungen als Lieferant für System Logs und Ereignisdaten. Auch ihre Rolle als technischer Unterstützer muss Geschäftsablauf für Geschäftsablauf nachvollzogen, analysiert und festgehalten werden. Auf ihre technische Zuarbeit sollte im Projekt aber erst abgehoben werden, nachdem das fachliche Konzept einschließlich aller erforderlichen Prozesse und Regeln steht.

**IT-DIRECTOR:** *Welche Technik empfehlen Sie, um dort, wo erforderlich, die notwendigen System Logs und Ereignisdaten abzurufen, sie zu analysieren und im Problemfall aus der IT heraus per Alarm zu eskalieren?*

**N. Drecker:** SIEM ist dafür der geeignete Lösungszuschnitt. Es fließen nur die Log- und Ereignisdaten aus unterschiedlichen Systemen und Komponenten ins SIEM-System ein, die Geschäftsprozesssteile stützen. So entsteht über die Zeit eine revisions sichere Ablage. Diese kann für historische Analysen rund um Sicherheit, Compliance und den Datenschutz im Sinne der Forensik genutzt werden. Die erhobenen Daten werden automatisch zur Echtzeitüberwachung analysiert und ausgewertet. Falls für Sicherheit, Compliance oder für den Datenschutz kritisch, werden beispielsweise per E-Mail sofort die richtigen Personen alarmiert, um weitergehende Analysen durchzuführen und/oder gezielte Maßnahmen zu ergreifen. <

## „Werden zu viele Prozesse, Regeln und IT-Informationsgeber etabliert, geht später im Betrieb der Überblick verloren.“

**Norbert Drecker**, Twinsec-Geschäftsführer

HADI STIEL