



# Sicherheit, Compliance und Datenschutz auf hohem Niveau

Die Bedrohungslage für Unternehmen verschärft sich. Gefahren für Sicherheit, Compliance und Datenschutz drohen von vielen Seiten: durch hoch komplexe Geschäfts- und IT-Abläufe, eigene Mitarbeiter, durch Geschäftspartner und Kunden. Doch weder in punkto Sicherheit und Compliance noch Datenschutz können sich Unternehmen Kompromisse leisten. Ein Kontroll- und Alarmierungssystem, das Hand und Fuß hat, wird damit für sie immer unverzichtbarer.

Die Achillesferse vieler Kontroll- und Alarmierungsansätze: Sie werden zu stark aus der Technik heraus vorangetrieben und fokussieren sich fast ausschließlich auf technische Aspekte. Häufig ist zu beobachten, dass nur Logs und Ereignisdaten bestimmter Systeme und Applikationen erfasst und lediglich isoliert für diese Systeme und Applikationen geprüft und ausgewertet werden. Selbst wenn Logs und Ereignisdaten unterschiedlicher Systeme und Komponenten mittels Korrelations-Engines in Beziehung gesetzt werden, bleiben die Analysen und Auswertungen oft technisch-funktional ausgerichtet. Rückschlüsse auf die gesamte IT einschließlich Geschäftsmodell und der Geschäftsprozesse sind somit

kaum möglich. Dies zeigt, dass eine angemessene Qualität der Sicherheit-, Compliance- und der Datenschutzmaßnahmen erst durch eine integrierte, ganzheitliche Betrachtungsweise erreicht werden kann.

## Top-down vorgehen

Das heißt im Umkehrschluss, ein professionelles Kontroll- und Alarmierungssystem sollte nicht bottom-up, sondern top-down von den Geschäftsprozessen ausgehend geplant und umgesetzt werden. Für die Zielerreichung – Sicherheit, Compliance und Datenschutz nach Anforderungsmaß – sind neben Logs und Ereignisdaten andere, nicht-technische Zusammenhänge wie Prozesse und Regeln bestimmend. Daher

sollte top-down hinterfragt werden, welche Prozesse bestehen, welche Prozesse verändert oder ergänzt und welche Regeln zusätzlich eingeführt und befolgt werden müssen.

Diese Maßnahmen können bereits in einem hohen Maß zu mehr Sicherheit, Compliance und Datenschutz beitragen. Den verbleibenden Risiken sollte aus der Technik heraus, genauer gesagt, durch die Einführung und den Einsatz eines SIEM (Security-Information- and Event-Management)-Systems, entgegengewirkt werden. Potenzielle Sicherheits-, Compliance- und Datenschutzrisiken werden im Projekt prozess- und dadurch geschäftsnah analysiert. Prozessveränderungen, Regeln und technische

## Geschäft und Technik müssen nahtlos zusammenwirken

SIEM ist keine Lösung von der Stange. Ganz im Gegenteil: Sie sollte professionell geplant, umgesetzt und laufend an die Erfordernisse des Geschäfts, der Organisation und der IT angepasst werden. Diese Machart ruft förmlich nach kompetenter Unterstützung.



**Norbert Drecker**  
Geschäftsführer von Twinsec.

„Meist wird ein zu technischer Projektweg eingeschlagen“

Sie ist auch entscheidend für die künftige Qualität der Analysen und Auswertungen und somit für das Maß an Sicherheit, Compliance und Datenschutz, das im Unternehmen erreichbar ist.

**funkschau:** Viele Unternehmen sind bereits hier überfordert?

**Norbert Drecker:** Ja. Meist wird in den Unternehmen, animiert durch IT-ProduktHersteller, ein zu techniklastiger Projektweg eingeschlagen. Das geht auf Kosten des Wirkungsgrads der Kontroll- und Alarmierungslösung. Die anvisierten Sicherheits-, Compliance- und Datenschutzziele, eben weil zu techniklastig, werden nicht erreicht. Diese falsche Bottom-up-Vorgehensweise geht außerdem auf Kosten des Budgets, weil es die Investitionen und Aufwendungen unnötig in die Höhe treibt. Anders mit kompetenter Unterstützung: Sie wird für ein erfolgreiches Projekt Prozesse, Regeln und IT-Informationen richtig gewichten, professionell zusammenführen und koordinieren und daraus die richtigen Schlüsse ziehen. Nur auf diese Weise entsteht eine Kontroll- und Alarmierungslösung, die hinreichend greift und das Budget nicht unnötig strapaziert.

**funkschau:** Haben nicht viele externe Berater und Dienstleister ähnliche Probleme wie die Unternehmen: entweder zu technologie- oder zu geschäftslastig?

**Alfred Koch:** Genau deshalb ist es wichtig, sich Methodik und Projektvorgehensweise der externen Unterstützung genau anzusehen.

Wenn beispielsweise über die Einführung einer SIEM-Lösung nachgedacht wird, ist sicherzustellen, dass das künftige Kontroll- und Alarmierungssystem ein integrierter Teil des unternehmensweiten Compliance- und Sicherheitssystems wird. Die einzelnen Elemente sollen sich, ausgehend von den Prozessen und Abläufen bis hin zur unterstützenden IT-Technik, zu einem harmonischen Ganzen zusammenfügen, keinesfalls isoliert wirken.

**funkschau:** Auch dieser Nutzen muss durchdrungen werden – richtig?

**Alfred Koch:** Für ein erfolgreiches Projekt ist es erforderlich, das Maß an Sicherheit, Compliance und Datenschutz, das erreicht werden soll, genau zu kennen. Dort, wo gesetzliche Bestimmungen und Regelungen einzuhalten sind, bestimmen diese das Maß. Ansonsten gilt: Nur top-down lassen sich Nutzen, Machbarkeit und Rentabilität der Kontroll- und Alarmierungslösung effizient ermitteln und quantifizieren. Oder anders gesagt: Aufwand und Kosten für Sicherheit, Compliance und Datenschutz sollen in einem für das Unternehmen vertretbaren Verhältnis zum Nutzen stehen, ohne dass dies zu Einschränkungen bei der Abdeckung von gesetzlichen Anforderungen führt. Genau das wird von uns im Projektvorfeld genauestens geprüft.

**funkschau:** Wie wichtig ist die Kompetenz einer Wirtschaftsprüfungsgesellschaft für die Herausbildung von mehr Sicherheit und Compliance?

**Alfred Koch:** Neben nationalen Regelungen wirken immer häufiger internationale Vorschriften, wie das EU-Recht, direkt die Gestaltung und Rahmenbedingungen interner Unternehmensrichtlinien und -vorgaben hinein. Daher empfiehlt sich gerade im immer komplexer werdenden Umfeld Sicherheit, Compliance und Datenschutz der Einsatz von Beratern an, die auf die Erfahrung und Kompetenz einer international tätigen Wirtschaftsprüfungsgesellschaft zurückgreifen können. Wird dieses gebündelte Wissen und Know-how in den Projekten genutzt, können Unternehmen eine kostspielige Überfrachtung ihres Kontroll- und Alarmierungssystems vermeiden.



**Alfred Koch**  
Senior Manager Advisory bei KPMG.

„Prozesse, Abläufe und unterstützende IT-Technik fügt SIEM zu einem harmonischen Ganzen.“

Vorkehrungen werden angemessen gewichtet. Die IT-Log- und -Ereignisflut wird von vornherein eingedämmt. Es wird nicht mehr als notwendig für das komplette Kontroll- und Alarmierungssystem investiert und ausgegeben. Es entsteht insgesamt eine für die Verantwortlichen und Zuständigen transparente Kontroll- und Alarmierungslösung mit Breitenwirkung: mehr Sicherheit, mehr Compliance und mehr Datenschutz.

### Strukturiert planen und umsetzen

Doch wie die umfassende Kontroll- und Alarmierungslösung in Szene setzen? – Dafür hat sich folgende Vorgehensweise bewährt:

- orientiert an den Geschäftsprozessen die Anforderungen aus den diversen Compliance- und internen Regelwerken sowie den Datenschutz (konform dem Datenschutzgesetz) ermitteln und festlegen,
- die fachlichen und technischen Prozesseigner bestimmen und entlang der Prozesse zuordnen,
- den Sicherheits-, Compliance- und Datenschutzrisiken entlang der Prozessketten identifizieren, dabei die fachlichen und technischen Prozesseigner einbinden,
- die einzelnen Risiken ob ihrer potenziellen Auswirkungen auf das Geschäft respektive auf die Einhaltung von Gesetzen, Vorschriften und Regeln hinterfragen,
- die Sicherheits-, Compliance- und Datenschutzvorfälle definieren und bemessen, deren Umsetzung für das Unternehmen wirtschaftlich relevant ist beziehungsweise die per Gesetz eingehalten werden müssen,
- diese Vorfälle entlang der Geschäftsprozesse nach Abhängigkeiten und Wechselwirkungen ordnen, um so die Risiken genauer bestimmen, bemessen und geeignete Maßnahmen und Policies ableiten zu können sowie
- Identifikation der Maßnahmen, die im Einzelnen ergriffen werden müssen, wie die Information oder Alarmierung bestimmter Personen.

Durch diese klar strukturierte Vorarbeit kristallisieren sich Kontrollsysteme (Prozesse, Prozessverantwortliche) sowie Sicherheits-/Compliance-/Datenschutzregeln (einschließlich der zu alarmierenden Personen) heraus. Im Rahmen von SIEM wird dann festgelegt, welche Ereignisse, Transaktionen und Aktivitäten zu überwachen und zu dokumentieren sind. Ebenso werden die Regeln für mögliche Alarmierung bei Eintritt besonders kritischer Ereignisse festgelegt. Relevante Informationsgeber können Applikationen, Dienste, Datenba-

sen, Middleware, Betriebssysteme sowie Netzwerk- und Netzwerkperipheriekomponenten sein. Auch hier hilft die klare Geschäftsprozessorientierung, die richtigen Informationen aus den richtigen Systemen und Komponenten zu extrahieren und ins SIEM-System zu überführen.

Die Analysen und Auswertungen des SIEM-Systems sollten wiederum ins Kontrollsystem mit seinen Sicherheits-, Compliance- und Datenschutzregeln sowie den Alarmierungsprozessen einfließen. Das Kontrollsystem wird dadurch zu einem echten Frühwarn- und Monitoringsystem erweitert. Quasi nebenbei liefert die so geschaffene Kontroll- und Alarmierungslösung eine revisionssichere Ablage unter Berücksichtigung aller Datenschutzerfordernisse. Dieser nachweislich dokumentierte Informationsbestand kann sowohl für zusätzliche historische Analysen und Auswertungen als auch als Langzeitarchiv dienen.

### Fachabteilungen einbinden

Wichtig ist, schon beim Start des Projekts die Fachabteilungen einzubinden. Ihr fachliches Know-how und ihre fachliche Sicht der Risiken ist für den künftigen Lösungszuschnitt der Kontroll- und Alarmierungslösung sowie ihre Wirtschaftlichkeit unverzichtbar. Außerdem werden über die Fachabteilungen die Risikopotenziale für die Projektverantwortlichen transparenter. Wichtig ist außerdem, das fachliche Wissen und die potenziellen Risiken der Fachabteilungen in line mit den Geschäftsprozessen zu bringen, an denen deren Mitarbeiter mitwirken. Denn nur Ende-zu-Ende können Sicherheits-, Compliance- und Datenschutzrisiken für das Unternehmen richtig bemessen und final bewertet werden. Dies setzt eine permanente Koordination der Projektaktivitäten über alle Fachabteilungen voraus, das hohe Projektziel stets vor Augen: die erforderlichen Prozesse, Regeln und Informationen für mehr Sicherheit, Compliance und Datenschutz im Unternehmen bereitzustellen.

### Strategische Aufhängung beachten

Nicht vergessen werden sollte die strategische Aufhängung des Projekts direkt unter der Unternehmensführung. Denn die Geschäftsziele und Business-Pläne sind für eine angemessene Analyse und Bewertung von Sicherheits-, Compliance- und Datenschutzrisiken sowie deren potenziellen Folgen bestimmend. Hinzu kommt der hohe strategische Stellenwert für das Unternehmen. Auch deshalb sollte das Projekt auf oberster Führungsebene angesiedelt werden.

Nicht vernachlässigt werden sollte eine detaillierte Dokumentation der Kontroll- und Alarmierungslösung mit ihren Prozessen und Regeln, einschließlich der technischen Informationen und Zusammenhänge, welche die SIEM-Lösung beisteuert. Denn nichts ist so beständig wie der Wandel, unabhängig davon, ob er von der IT, den Geschäftsprozessen oder der Organisation ausgeht. In jedem Fall ändert sich die Risikolage für das Unternehmen sowohl mit Blick auf Sicherheit und Compliance als auch auf den Datenschutz. In allen drei Fällen verhilft eine ausführliche und gut strukturierte Dokumentation dazu, die Kontroll- und Alarmierungslösung immer wieder gezielt, schnell und gut dokumentiert an die neuen Gegebenheiten anzupassen.

### SIEM keinesfalls unterbewerten

Mit zunehmendem Automatisierungsgrad bei den Geschäftsprozessen wird die Bedeutung der Technik und damit von SIEM als gezieltem IT-Informationslieferanten, als Analyse- und Auswertungs-Tool sowie als Alarmierungsinstanz zwangsläufig wachsen. So besehen sollte diese technische Seite der Kontroll- und Alarmierungslösung mit Blick in die nahe Zukunft und eine investitionssichere Auslegung keinesfalls unterschätzt werden. Je mehr Prozesse und Technik Hand in Hand gehen werden, umso mehr wird die Kontroll- und Alarmierungslösung auf Informationen, Analysen, Auswertungen und Eskalationen aus der IT heraus angewiesen sein.

Ohne eine angemessene Einpassung von SIEM in die Gesamtlösung würde eine IT-Blackbox drohen. Sie würde die Gefahr nicht mehr transparenter, kontrollierbarer und beherrschbarer Abläufe und Aktionen bis hinauf auf Geschäftsebene in sich bergen, auf Kosten der Sicherheit, von Compliance und des Datenschutzes. Ganz anders mit SIEM: Je mehr mit fortschreitender Automatisierung Logs und Ereignisse aus der IT bestimmend für das Geschäft, für Sicherheit, Compliance und Datenschutz sein werden, um so mehr wird SIEM in voller Breite zu mehr Transparenz, Kontrolle und Beherrschbarkeit beitragen. SIEM deckt darüber hinaus auf, ob nicht autorisierte Veränderungen an Konfigurationen oder Manipulationen an Protokollierungen vorgenommen wurden. (RL)



**Alfred Koch**

Senior Manager Advisory bei KPMG



**Norbert Drecker**

Geschäftsführer von Twinsec