MACHBARKEITSGRENZEN ERWEITERN

ISM-Maßnahmen automatisieren

Rahmenwerke wie der „Sichere IT-Betrieb“ (SITB) sollen dabei unterstützen, das Sicherheitsniveau in Kreditinstituten zu erhöhen. Doch welche Kontrollen gilt es dabei wann und in welcher Form durchzuführen? Welche Aufgaben verursachen hier hohe Aufwände für den Informationssicherheitsbeauftragten (ISB)? Und wie lässt sich die Vielzahl an vorgeschriebenen Kontrollen trotz zunehmender Regulatorik und strapazierten Personalkapazitäten beherrschen, ohne Abstriche bei der IT-Sicherheit in Kauf nehmen zu müssen?

Das Aufgabengebiet des Informationssicherheitsbeauftragten ist umfangreich. Im Fokus steht die aktive, konsequente und nachhaltige Risikominimierung hinsichtlich der Identifizierung möglicher Schwachstellen des Unternehmens im IT-Umfeld. Ziel ist es, externe Cyber-Angriffe sowie interne Datenpannen zu verhindern. Der ISB ist das Bindeglied zwischen dem Vorstand bzw. der Geschäftsführung, der IT sowie den Mitarbeitenden des Unternehmens. Er hat die Aufgabe, das gesamte Team stetig für das Thema IT-Sicherheit zu sensibilisieren und entsprechend zu schulen. Darüber hinaus konzipiert der ISB ein möglichst lückenloses Information Security Management System (ISMS), entwickelt es konsequent weiter und sorgt für dessen Durchsetzung. Daneben gilt es, bestehende und neu einzuführende Systeme laufend zu analysieren und die IT-Sicherheitsmaßnahmen fortlaufend zu dokumentieren.

Hinzu kommen weitere Aufgaben, wie die aktive Absicherung eingesetzter Endgeräte oder die Etablierung von Präventiv- und Notfallmaßnahmen –

etwa bei neuartigen Bedrohungen. Aufgrund des Anforderungsprofils sowie des sensiblen Tätigkeitsbereichs ist eine Auslagerung der Aufgaben des ISB an einen externen Dienstleister für Banken und Sparkassen oft das Mittel der Wahl. Aber auch hier ist immer größte Sorgfalt gefragt.

Machbarkeitsgrenzen für den ISB

Das Rahmenwerk „Sicherer IT-Betrieb“ verpflichtet beispielsweise Sparkassen dazu, ihre IT-Systeme und -Prozesse so zu organisieren, dass die Integrität, Verfügbarkeit, Authentizität sowie Vertraulichkeit der Daten gewährleistet ist. Sowohl für Verbundsysteme als auch für Systeme von Drittanbietern muss der ISB sicherheitsrelevante Aktionen nachvollziehbar dokumentieren und entsprechende Maßnahmen einleiten.

In der Praxis bedeutet dies die vollständige, lückenlose Analyse von Logs und Ereignislisten aus den eingesetzten Anwendungen und Systemen. Dazu gehören Logins, Logouts, Passwortänderungen, fehlerhafte Passworteingaben, Nutzeranlagen, Nutzersperrungen, Nutzerlöschungen, Vergabe oder Veränderungen von Berechtigungen oder Logins von bestimmten Geolocations (etwa außerhalb des Unternehmens). Zahlreiche Systeme, wie Eurex, Swift, XETRA, B+S, SAS oder Cascade, um nur einige zu nennen, liefern laufend Ereignisprotokolle.

Die zahlreichen Ereignisse, die in teils unstrukturierten Logs zur Verfügung stehen, gilt es einzeln auszuwerten. Angesichts der schieren Menge eine auf Dauer schlicht kaum zu bewältigende Aufgabe – selbst ohne die Vielzahl an weiteren Tätigkeiten, mit denen der Informationssicherheitsbeauftragte betraut ist. Zudem birgt die manuelle Kontrolle auch die Gefahr, sicherheitsrelevante Ereignisse zu übersehen. Nicht zuletzt bleibt häufig die vollständige Dokumentation über die durchgeführten Tätigkeiten auf der Strecke.

Alle Vorgänge im Blick

Gerade für Finanzinstitute mit geringen Mitarbeiterkapazitäten ist eine manuelle Kontrolle aufgrund der vielseitigen Pflichten dauerhaft nicht umsetzbar. Die Lösung besteht aus intelligenten Werkzeugen, wie etwa der Erweiterung „ISM-Kontrollen“ für Foconis-Zak, die die Kontrolle der Ereignisse automatisch durchführen. Kommt es zu einer sicherheitsrelevanten Auffälligkeit – sei es eine fehlgeschlagene Anmeldung, eine Kennwortänderung durch Dritte oder ein Zugriff auf kritische Daten und Objekte – wird diese um detaillierte Informationen ergänzt. So erhält der Informationssicherheitsbeauftragte die Möglichkeit zur detaillierten Analyse der auffälligen Vorgänge sowie konkrete Handlungsempfehlungen. Anstatt also jedes Ereignis einzeln zu prüfen, muss der Informationssicherheitsbeauftragte nun nur noch Ergebnisse untersuchen, die entweder eine Auffälligkeit zeigen oder die hinsichtlich der Informationssicherheit relevant sind.

Im nächsten Schritt bearbeitet der ISB den Vorgang, indem er ihn revisionskonform dokumentiert, delegiert, mit Fristverlängerung zur späteren Prüfung speichert oder abschließt. Um Bearbeitungsfristen nicht zu versäumen, verfügen intelligente Tools über ein Eskalationsmanagement. Weiterer Vorteil: Dank Dokumentation ist auch eine schnelle, flexible Vorgangsrecherche oder Stichprobenkontrolle komfortabel durchführbar. Für die langfristige Funktionalität entscheidend ist, dass die automatisierte Lösung über eine konfigurierbare Architektur verfügt, die die Einbindung von Verbund-Systemen und individuellen Lösungen unterstützt. Dies verleiht zusätzliche Flexibilität und langfristigen Investitionsschutz.

Digitale Unterstützung: Mehr Sicherheit

Banken und Sparkassen, die auf eine intelligente Listenauswertung setzen, profitieren von einer höheren Kontrollqualität. Zugleich heben sie ihre Informationssicherheit auf ein neues Level. Die automatische Dokumentation sowie die Handlungsempfehlungen helfen dem Informationssicherheitsbeauftragten bei der Umsetzung der von ihm gesetzlich geforderten Auflagen. Die manuelle Durchsicht von Ereignissen ist nicht länger erforderlich und schont so wertvolle Mitarbeiterkapazitäten. Sind die eingesetzten Lösungen entsprechend flexibel gestaltet, lassen sich beliebige Systeme integrieren und garantieren auf diese Weise nachhaltig mehr Effizienz und Sicherheit.

Fazit

Informationssicherheit ist in Banken und Sparkassen ein hohes Gut. Dem ISB kommt daher eine Rolle mit hoher Verantwortung zu. Seine Aufgabenliste ist lang; die Komplexität der Pflichten nimmt – auch aufgrund immer strengerer Regularien – weiter zu. Gerade in Anbetracht der voranschreitenden Digitalisierung und des vorherrschenden Fachkräftemangels müssen die Verantwortlichen in den Finanzinstituten für Lösungen sorgen, die sowohl der Bedeutung der IT-Sicherheit Rechnung tragen als auch die Mitarbeiterkapazitäten nicht über Gebühr strapazieren. Automatisierte Überwachungsmethoden sind dabei eine effiziente Alternative. Sie minimieren den Kontrollaufwand, entlasten den Informationssicherheitsbeauftragten spürbar und maximieren gleichzeitig die Informationssicherheit.

Autor: Olaf Pulwey

Olaf Pulwey ist seit 1990 in der IT-Industrie als Unternehmer und Vorstand tätig. Seit 2005 ist er Mitglied des Vorstands bei Foconis, deren Vorsitz er im Sommer 2021 übernommen hat. Foconis unterstützt Banken und andere Unternehmen aus der Finanzwirtschaft dabei, geeignete Schlüsselkontrollen zu identifizieren und umzusetzen, um ein effizientes internes Kontrollsystem im Sinne des §25a KWG zu implementieren.