Bewährte Werkzeuge für das IT-Sicherheitsmanagement

Von automatisierten ISM-Kontrollen können Sparkassen gleich mehrfach profitieren: Einerseits reduzieren sie den Aufwand für den IT-Sicherheitsbeauftragten. Andererseits schafft es die IT-gestützte Auswertung in aller Regel deutlich besser als der Mensch, sicherheitsrelevante Vorgänge aufzudecken.

Für Sparkassen herrschen strenge Regularien im Bereich IT-Sicherheit. So sind sie etwa verpflichtet, die Ausgestaltung der eingesetzten IT-Systeme auf gängige Standards abzustellen und die zugehörigen Ereignisse und Prozesse sicherheits- und risikoorientiert zu überwachen. Das Rahmenwerk „Sicherer IT-Betrieb" (SITB) aus dem Sparkassen-Verbund unterstützt Institute dabei, die vielseitigen Anforderungen zu erfüllen, das Sicherheitsniveau anzuheben und aktuelle IT-Risiken auf ein Minimum zu reduzieren. Darüber hinaus müssen die Integrität, Verfügbarkeit, Authentizität sowie Vertraulichkeit der Daten sichergestellt sein. Die Gewährleistung der Nachvollziehbarkeit aller sicherheitsrelevanten Ereignisse hat dabei oberste Priorität. Das Ziel: Sämtliche Ereignisse erfassen, potenzielle Bedrohungen zum Anstoß entsprechender Maßnahmen identifizieren und alle Prozesse und Tätigkeiten revisionssicher dokumentieren.

Manuelle Kontrolle? Unmöglich!

Mit detaillierten Kontrollen und akribischer Dokumentation der IT-Protokolle soll eine lückenlose Überwachung etabliert werden. Doch die hohen Anforderungen an die IT-Sicherheit betreffen nicht nur Sparkassen. Auch für Verbund- und Drittanbietersysteme gilt das Rahmenwerk SITB. So hat sich in der Praxis folgendes Vorgehen bewährt: Erstellt der Informationssicherheitsbeauftragte (ISB) eines Kreditinstituts etwa der Sparkassenfinanzgruppe das Informationssicherheitsmanagement (ISM)-Konzept, bewertet er sogleich alle im Einsatz befindlichen Anwendungen und stuft deren individuellen Schutzbedarf ein. Dabei sollte er gemäß den BAIT die Zahl der Anwendungen, bei denen die Protokolle oder Logs geprüft werden müssen, bereits so weit wie möglich reduzieren. Je nach Software umfassen diese neben allen Anmelde-Ereignissen auch sämtliche vorgenommenen Änderungen. Dadurch entstehen jeden Tag Tausend Zeilen an Informationen – und das in unzähligen Dokumenten, in den verschiedensten Strukturen und Formaten. Selbst wenn nur kritisch protokollierte Interaktionen betrachtet werden, wird schnell klar: Diese Datenmengen sind umfangreich und sogar für Experten schwer lesbar. Nur geübte Blicke können in und zwischen den Zeilen risikorelevante Unregelmäßigkeiten aufspüren – und das aufgrund der Masse auch nur oberflächlich. Eine Kontrolle, um gar nicht erst von einer Vollkontrolle zu sprechen, sowie die Bearbeitung dieser Ereignisse ist manuell heute einfach nicht mehr stemmbar. Mehr noch: Alle relevanten Ereignisse in diesem Zusammenhang lückenlos, nachvollziehbar und dokumentiert zu kontrollieren, ist per Hand schlicht unmöglich.

Moderne Werkzeuge helfen

Sparkassen können von bewährten Werkzeugen profitieren, die eine konsequente Umsetzung des sicheren IT-Betriebs mit intelligenten und automatisierten Überwachungstechniken ermöglichen. Entsprechende Lösungen schaffen es dabei auch, den heute wohl wichtigsten Erfolgsfaktor positiv zu beeinflussen: die Mitarbeiterkapazitäten. Bei der Automatisierung der ISM-Kontrollen unterstützt eine intelligente, elektronische Listenauswertung nicht nur den ISB. Auch der Kontrollaufwand im Bereich der IT-Sicherheit schrumpft damit auf ein Minimum, beschränkt sich dieser doch lediglich noch auf die Sichtung der als potenzielle Bedrohung erkannten Ereignisse.

Um die Informationssicherheit nach einem standardisierten ISM zu gewährleisten, sollte der SITB-Standard verbindlich eingesetzt werden. Die aufwändige Überprüfung der Daten lässt sich mit intelligenten Lösungen automatisieren. Institute sind mit Systemen gut beraten, die gemäß ISM-Konzept die zu kontrollierenden Protokolle lückenlos verarbeiten und nur per Definition auffällige Sachverhalte dem ISB zur Vorlage bringen.

Lösung trifft wichtige Vorentscheidungen

Ergänzend zu den idealerweise bereits im Standard definierten Kontrollen werden die Systeme bereits in der Einführungsphase darauf trainiert, über eine gezielte Parametersteuerung der Kontrollverfahren eine Vorentscheidung darüber zu treffen, welche Ereignisse die Aufmerksamkeit des ISM bedürfen und welche nicht. Die betroffenen Protokolle, Logs und Ereignislisten werden in der Regel als Textliste oder CSV-Datei von den eingesetzten Anwendungen bereitgestellt, die bei dem entsprechenden Kreditinstitut zum Einsatz kommen. Diese Dateien werden direkt aus dem Verzeichnis des ISB heraus aufgegriffen und gemäß den hinterlegten Kontrollen verarbeitet, was bisher manuell geschehen musste. Im Anschluss an die Verarbeitung informiert das System den ISB über sämtliche Auffälligkeiten – jedes Ereignis erhält hierbei einen eigenen Vorgang, sodass Auffälligkeiten sukzessive überprüft, bearbeitet und dokumentiert werden können.

Je nach Art des Vorgangs, kann der ISB vom Verursacher beziehungsweise Auslöser eine Stellungnahme einfordern. Ein Beispiel wäre der klassische Fall eines vergessenen Passworts, was zu mehrfachen falschen Anmeldeversuchen und schließlich zur Sperrung eines Benutzerkontos führte. Die verursachende Person kann nun über den Vorgang informiert werden, sodass dem Ereignis die Information beiliegt, dass es sich um einen aufgeklärten Fall handelt, dem neben dem Vorfall selbst der oder die Protagonist(en) zugeordnet werden konnte(n). Neben der manuellen Kontrolle der Log-Einträge entfällt so auch die aufwändige manuelle Ursachenforschung und das Einholen von Stellungnahmen über die internen Kommunikationskanäle. Bei der Bearbeitung kann der ISB diese Vorgänge dokumentieren, delegieren, abschließen oder mit einer zu beantragenden Fristverlängerung speichern. So können einzelne Sachverhalte auch zu einem späteren Zeitpunkt noch überprüft werden. Das unterlegte Eskalationsmanagement kümmert sich darüber hinaus um die Einhaltung von Bearbeitungsfristen. ■

www.foconis.de

Autor **Olaf Pulwey** ist Mitglied des Vorstands der FOCONIS AG.