51. Jahrgang | Fritz Knapp Verlag | die-digitale-bank.de

bm
bank und markt

10

15. Oktober 2022

DIE DIGITALE BANK

Digitaler Sonderdruck

INNOVATION UND SICHERHEIT

DATEN IM FOKUS

Entlastung für den ISB – Informationssicherheit automatisieren

Von Olaf Pulwey

Entlastung für den ISB – Informationssicherheit automatisieren

Von Olaf Pulwey

Für wenige Branchen hat die IT-Sicherheit den gleichen Stellenwert wie für Banken. Einerseits sind sie bevorzugte Angriffsziele für Cyberkriminelle, gleichzeitig leben sie vom Vertrauen der Kunden in die Datensicherheit. Die fortschreitende Digitalisierung verleiht dem Thema eine zusätzliche Dringlichkeit. Rahmenwerke, wie der „Sichere IT-Betrieb" (SITB), gelten auch für Verbundsysteme sowie die Systeme von Drittanbietern. Weil die manuelle Prüfung aufgrund der Vielzahl an Systemen und Ereignissen längst unmöglich geworden ist, sind automatisierte Kontrollen für die Finanzinstitute mittelfristig unabdingbar, so der Autor. Dann wird der IT-Sicherheitsbeauftragte zur zweiten Verteidigungslinie, die nur noch die kritischen Vorfälle prüfen muss. Red.

Die Bedeutung umfassender IT- und Informationssicherheit in Banken und Sparkassen ist immens: Cyberangriffe können nicht nur mit verheerendem finanziellem Schaden einhergehen. Schlimmer noch: Der drohende allgemeine Vertrauensverlust verursacht obendrein einen Imageschaden, von dem sich die Häuser mitunter nicht mehr erholen können.

Hinzu kommt, dass spätestens seit Beginn der Corona-Pandemie mit dem Trend zum dezentralen Arbeiten auch in der Finanzbranche übliche hybride Arbeitsweisen das IT-Risiko weiter erhöhen. Werkzeuge, wie das Rahmenwerk „Sicherer IT-Betrieb" (SITB), sollen thematisch dafür sensibilisieren und das Sicherheitsniveau in Banken und Sparkassen nachhaltig steigern.

Das Problem: Manuelle Kontrollen sind zum einen aufgrund der schieren Menge an Ereignissen und zum anderen wegen der Vielfältigkeit der jeweils im Einsatz befindlichen Systeme längst unmöglich. Informationssicherheitsbeauftragte (ISB) benötigen darum konsequente, vollumfängliche und bestenfalls maximal automatisierte Unterstützung, um der auch hier stets strenger werdenden Regulatorik zu entsprechen.

Die Schattenseiten der Digitalisierung

Die Finanzbranche wird immer digitaler. Das veränderte Verhalten der Kunden sorgt für neue Anforderungen, denen die Verantwortlichen mit elektronischen Lösungen Rechnung tragen müssen. Sich ausweitende hybride rbeitsweisen auch bei den Kunden verstärken die Bedeutung von zuverlässiger, sicherer IT.

Banken und Sparkassen profitieren von der Digitalisierung in Form eines enormen Effizienzgewinns. Wird die Digitalisierung richtig umgesetzt, sind die Einsparung von Kosten und Mitarbeiterkapazitäten erheblich. Dennoch gehen mit der Entwicklung auch neue Herausforderungen einher:

– Da Vertrauen im Geschäftsmodell von Banken und Sparkassen eine zentrale Rolle spielt, hat (IT-)Sicherheit einen besonderen Stellenwert.

– Gleichzeitig sind Banken und Sparkassen durch ihre Funktion und Arbeitsweise (beispielsweise hohe Geldsummen und Speicherung sensibler Daten) vermehrt begehrte Ziele immer raffinierterer Angriffe von außen.

– Dezentrale Arbeitsweisen schaffen unter Umständen offene Flanken, die die Täter geschickt (und oft unbemerkt) ausnutzen.

Mit ausreichend Ressourcen hätten Banken und Sparkassen eine Chance, diesen Gefahren zu begegnen. Doch diese Ressource haben die meisten In-

Olaf Pulwey, CEO,
FOCONIS AG,
Vilshofen

stitute nicht. Der allgemeine Fachkräftemangel, stetig steigende Anforderungen und der daraus resultierende nachhaltige Aus- und Weiterbildungsbedarf setzen die Finanzinstitute unter Druck. Gleichzeitig nimmt die Regulatorik im Bereich Informationssicherheit rasant zu. Die sehr komplexen und sensiblen Anforderungen machen eine Auslagerung der entsprechenden Tätigkeiten, wie beispielsweise die Beauftragung eines externen Informationsbeauftragten, schwierig.

„Sicherer IT-Betrieb"

Angesichts der großen – und wachsenden – Bedeutung der Informationstechnologie sind die heute geltenden strengen Vorgaben für Banken und Sparkassen durchaus nachvollziehbar und sinnvoll. Dazu gehört etwa die Verpflichtung zur Ausgestaltung der IT-Systeme und -Prozesse auf übliche Standards sowie zur Bildung von Prozessen für die Protokollierung und Überwachung.

Das Rahmenwerk „Sicherer IT-Betrieb" (SITB) hat etwa unter anderem das Ziel, die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten von Sparkassen zu gewährleisten. Die Verantwortlichen müssen insbesondere darauf achten, sicherheitsrelevante Aktionen mit dem Ziel der Verhinderung beziehungsweise Identifikation entsprechender Vorfälle nachvollziehbar zu machen. Ein gezieltes Monitoring soll die Basis für eine konsequente Maßnahmensteuerung sein. Dies gilt sowohl für Verbundsysteme als auch für die Lösungen von Drittanbietern.

Automatisierte Überwachung

Um diesen wichtigen Anforderungen nachhaltig nachzukommen, ohne gleichzeitig dauerhaft die Mitarbeiterkapazitäten zu belasten, bedienen sich die Institute bewährter Lösungen, wie beispielsweise der Erweiterung „ISM-Kontrollen" für Foconis-ZAK. Damit ist es möglich, die Kontrolle der Ereignisse aus zahlreichen Systemen maximal zu automatisieren. Jedes Kontrollergebnis wird dabei um detaillierte Informationen ergänzt, die den Informationssicherheitsbeauftragten direkt unterstützen. So kann er jederzeit nicht nur auffällige Vorgänge im Detail analysieren und direkte Handlungsempfehlungen umsetzen. Auch die Vorgangsrecherche oder Stichprobenkontrolle im Prüfungsfall gelingt dank der vollständigen Dokumentation lückenlos auf Knopfdruck.

Systeme und Anwendungen wie OSPlus, Simcorp Dimension (SCD), Parisplus, Ilores, und Eurex geben täglich Ereignisprotokolle aus, deren umfängliche Analyse im Sinne der geltenden Regulatorik ist. Intelligente Lösungen mit einer modernen Konfigurations-Architektur ermöglichen jederzeit die Einbindung weiterer Verbundsysteme. Auch eine Unterstützung individuell eingesetzter Lösungen ist auf diese Weise denkbar.

Spürbare Entlastung für den Informationsbeauftragten

Ob fehlgeschlagene Anmeldung, eine Passwortänderung außerhalb der Geschäftszeiten oder eine Änderung von Berechtigungen: Kommt es zu einer sicherheitsrelevanten Auffälligkeit, wird diese durch selbsterklärende, angereicherte Einzelkontrollvorgänge dokumentiert. Der Informationssicherheitsbeauftragte in seiner Rolle als „second Line of Defence" muss nun nur noch diejenigen Ergebnisse kontrollieren, die mit Blick auf die Informationssicherheit Relevanz haben oder die durch eine automatisierte Vorabprüfung festgestellte, konkrete Auffälligkeit zeigen. Bei der Bearbeitung gilt es, diese Vorgänge revisionskonform zu dokumentieren, zu delegieren, abzuschließen oder mit einer zu beantragenden Fristverlängerung zu speichern. Ein Eskalationsmanagement sorgt dabei für die Einhaltung von definierten Bearbeitungsfristen.

Die automatisierte Kontrolle von Ereignislogs aus verschiedensten Quellen entlastetet denInformationssicherheitsbeauftragten nachhaltig, erhöht zugleich die Kontrollqualität und steigert die Sicherheit des Unternehmens. Manuelle Ereignisdurchsichten gehören dank intelligenter Listenauswertung der Vergangenheit an. Die automatische Dokumentation der Kontrollen, der Ergebnisse der Kontrollen sowie konkrete Handlungsempfehlungen und deren dokumentierte Umsetzung unterstützen den Informationssicherheitsbeauftragten beim Nachweis der Tätigkeiten im Rahmen der gesetzlichen Auflagen. Wirksamkeit, Wirtschaftlichkeit und Ordnungsmäßigkeit sind hierbei die geltenden Prämissen.

Unter dem Strich lässt sich festhalten: Nicht nur, um geltende Regularien zu erfüllen, sondern auch, um finanziellen Schäden oder gar Imageverlust vorzubeugen, muss IT-Sicherheit bei Banken und Sparkassen höchste Priorität genießen. Die fortschreitende Digitalisierung verleiht dem Thema eine zusätzliche Dringlichkeit. Rahmenwerke, wie „Sicherer IT-Betrieb" (SITB), gelten auch für Verbundsysteme sowie die Systeme von Drittanbietern.

Die manuelle Prüfung hat sich aufgrund der Vielzahl an Systemen und Ereignissen längst als unmöglich erwiesen. Um trotz steigender Anforderungen und knapper Personalbestände die Sicherheit der EDV und Prozesse im Griff zu behalten, sind automatisierte Kontrollen für die Finanzinstitute mittelfristig unabdingbar. Die Verantwortlichen steigern auf diese Weise das Sicherheitsniveau ihrer Institute nachhaltig. ■