B1618 48. Jahrgang Ausgabe 1/2017

+SCHWERPUNKT+
Sicherheit

gi GELDINSTITUTE

Fachzeitschrift für IT-Entscheider und Manager

Cybercrime der nächsten Generation

Banken müssen umdenken

Jeremiah Grossman, Chief of Security Strategy von SentinelOne

Strategie:
Kreditentscheidung

Bank-IT:
Softwaretesting

Marketing & Vertrieb:
Kundengewinnung

Mit Access Governance auf MaRisk-Novelle vorbereitet

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat mit den MaRisk eine bindende Verwaltungsanweisung herausgegeben. MaRisk steht für „Mindestanforderungen an das Risikomanagement". Eine weitere Novellierung der MaRisk trat vor kurzem in Kraft. Von der Novelle betroffen ist auch das Überprüfen von Berechtigungen und Kompetenzen.

Autor:
Jürgen Bähr,
Geschäftsführer der G+H Systems GmbH in Offenbach

Banken müssen vergebene Berechtigungen noch präziser verwalten und dokumentieren als bisher. Um den neuen Auflagen entsprechen zu können, gewinnt das Thema Access Governance weiter an Bedeutung. Die letzte Novellierung der MaRisk stammt aus dem Jahr 2012. Aus Sicht der BaFin ist es nun an der Zeit, in einer weiteren Novellierungsphase die Themen Risikodaten und Risikoberichterstattung in den Fokus zu stellen – bzw. deren Aggregation. Das bedeutet u. a., dass alle Zugangsberechtigungen zu den digitalen Systemen einer Bank regelmäßig überprüft werden müssen. Hier greift das sogenannte Minimalprinzip. Es besagt: Alle Mitarbeiter dürfen ausschließlich die Zugangsberechtigungen besitzen, die sie für ihre tägliche Arbeit in der Bank auch tatsächlich benötigen. Die Banken sind verpflichtet, internen wie externen Revisoren diese Rechtestrukturen offenzulegen. Auch ist es für jede Bank selbst wichtig, jederzeit einsehen zu können, welche Berechtigungen beantragt wurden und ob der entsprechende Antrag bereits bearbeitet wurde. Da dieser Prozess für die Banken kritisch ist, sind papierbasierte Verfahren nicht mehr adäquat. Neben deutlich höheren Bearbeitungszeiten sind die erstellten Reports oftmals nach Fertigstellung bereits wieder überholt. Die MaRisk-Novelle fordert ausdrücklich, „internen Revisionen […] unverzüglich die erforderlichen Informationen zu erteilen, die notwendigen Unterlagen zur Verfügung zu stellen und Einblick in die Aktivitäten und Prozesse sowie die IT-Systeme des Instituts zu gewähren." Aus regulatorischer wie auch ökonomischer Sicht ist die Ablösung papierbasierter zugunsten elektronischer Verfahren aus vorteilhaft. Mittels daccord ist es Fachabteilungen zum Beispiel möglich, den Status einer Rechtevergabe per Knopfdruck als Report einem Vorgesetzten zu melden. Die Software dokumentiert außerdem lückenlos, wer wann welche Berechtigung erteilt oder gelöscht hat. Das erleichtert den Banken sowohl die tägliche Arbeit als auch die Einhaltung der neuen Vorschriften.

Die MaRisk-Novelle ändert die Risikoberichterstattung

Zukünftig noch intensivere Nutzung geplant

Beispielhaft voran geht hier die Degussa Bank. Sie hat schon vor dem Inkrafttreten der erwähnten MaRisk-Novelle auf eine digitale Lösung gesetzt und sorgt damit für mehr Transparenz bei der Vergabe von Benutzerberechtigungen. Für die Bank fällt damit der enorme Aufwand der papierbasierten Prozesse sukzessive weg. Das entlastet die Mitarbeiter und vermeidet Fehler. Im Falle einer Überprüfung können mit daccord Auswertungen einfach auf Personen- oder Systemebene durchgeführt werden. Gegenüber dem alten papierbasierten Prozess bringt die Automatisierung der Zertifizierungs- und Rezertifizierungsprozesse von kritischen und unkritischen Systemen eine weitere erhebliche Entlastung der Mitarbeiter mit sich. Denn daccord überwacht diese Vorgänge und informiert automatisiert die jeweiligen System- bzw. Personenverantwortlichen. Der Großteil der Systeme der Degussa Bank profitiert bereits von dieser digitalen Lösung. In den angeschlossenen Systemen konnten die Benutzerrechte schnell und unkompliziert ausgelesen und auf dieser Basis bereinigt werden. Der nächste Schritt stellt die Bildung eines Rollen- und Rechtemodells dar, in dem einem Mitarbeiter die für die Ausübung seiner Tätigkeit notwendigen Rollen & Rechte zugewiesen werden. Benutzerrechte werden auf diese Weise zu handlichen Gruppen zusammengefasst. Das ermöglicht der Bank die Prüfung der Einhaltung des Minimalprinzips, welches die MaRisk-Novelle ausdrücklich fordert. Die Degussa Bank plant bereits, den Einsatz der Software zu erweitern.