Helmut Semmelmayer

BAIT, MaRisk, KRITIS – die aktuellen **Anforderungen** an die **Informationssicherheit**

Die außergewöhnlichen Umstände der vergangenen beiden Jahre haben nicht nur in vielen Unternehmen die Digitalisierung vorangetrieben, auch Cyberangriffe und Schadsoftware wie Ransomware wurden dadurch beflügelt. Zu diesem Ergebnis kommt etwa die Studie „The State of Ransomware 2021" der IT-Sicherheitsfirma Sophos, für die 550 Entscheidungsträger aus Finanzunternehmen weltweit befragt wurden: 34 Prozent aller Firmen gaben an, im vergangenen Jahr Ziel von Ransomware gewesen zu sein. Im DACH-Raum lag der Wert mit 46 Prozent sogar deutlich höher. Bei einem erfolgreichen Angriff sind nicht nur für das betroffene Unternehmen, sondern auch für Wirtschaft und Gesellschaft enorme Konsequenzen zu befürchten. Kein Wunder also, dass die Absicherung von IT-Systemen von Politik und Behörden immer stärker vorangetrieben wird. Zu diesem Zweck hat die deutsche Bundesregierung 2021 etwa das bestehende IT-Sicherheitsgesetz durch eine Novelle angepasst. Aufgrund ihrer wesentlichen Bedeutung für die Bargeldversorgung und den Zahlungsverkehr zählen auch Finanzinstitute ab einer gewissen Größe zu den kritischen Infrastrukturen (KRITIS), die die Auflagen des IT-Sicherheitsgesetzes 2.0 erfüllen müssen.

Durch das neue IT-Sicherheitsgesetz wird in erster Linie die Kommunikation mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) intensiviert. So wurde etwa die Frist für die Registrierung beim BSI und dem Einrichten einer Kontaktstelle drastisch gekürzt: Nach Überschreiten eines KRITIS-Schwellenwertes mussten sich Betriebe bislang erst im Folgejahr melden, jetzt ist die Registrierung bereits am folgenden Tag vorgesehen. Eine Meldepflicht gibt es nun zudem für sogenannte kritische Komponenten, also IT-Produkte, deren Ausfall den normalen Betrieb einer Organisation erheblich beeinträchtigen würde. Das BSI kann den Einsatz kritischer Komponenten untersagen, wenn diese zum Beispiel aufgrund bekannter Sicherheitslücken als nicht vertrauenswürdig eingestuft wurden. Darüber hinaus kann das BSI künftig zur Beseitigung von Störungen Informationen direkt von betroffenen Unternehmen anfordern.

Meldepflichten und Angriffserkennung

Auch auf technischer Ebene gibt es eine Neuerung: Der verpflichtende Einsatz von Systemen zur Angriffserkennung. Dabei handelt es sich um Software, die verdächtige Vorfälle wie ungewöhnlichen Netzwerkverkehr oder wiederholte Zugriffsversuche automatisch erkennt und protokolliert. Man spricht in Fachkreisen von Security Incident & Event Management (SIEM). Die entsprechenden Daten müssen allerdings durch eine menschliche Kontrollinstanz ausgewertet werden, um echte Bedrohungen von Fehlalarmen zu unterscheiden. Etwa Zugriffsversuche von einem Mitarbeiter, der sich wegen eines dringenden Projekts spätabends einloggt.

Neben der Verwendung einer SIEM-Lösung braucht es daher in der Praxis auch ein laufend besetztes Security Operations Center (SOC), um relevante Sicherheitsvorfälle erkennen und der Meldepflicht gegenüber dem BSI nachkommen zu können. Für KRITIS-Betriebe ist eine großzügige Übergangsfrist für die Umsetzung der Angriffserkennung vorgesehen, für Finanzdienstleister sind SIEM und SOC aber aufgrund der BAIT-Novelle schon jetzt verpflichtend.

Die Novellen der Mindestanforderungen an das Risikomanagement (MaRisk) und der Bankaufsichtlichen Anforderungen an die IT (BAIT) rücken vor allem Wirksamkeitskontrollen für Sicherheitsmaßnahmen stärker in den Fokus. Hintergrund der Anpassung sind mehrere Leitlinien der Europäischen Bankaufsichtsbehörde (EBA), die sich mit Risikopositionen, Outsourcing im Finanzsektor und Informationssicherheitsrisiken beschäftigen. Zum Angleich an diese internationalen Vorgaben wurden zahlreiche Abschnitte von BAIT und MaRisk angepasst. Da es sich bei den Novellen um eine Konkretisierung bestehender Vorgaben handelt, ist keine Übergangsfrist für die Umsetzung der Änderungen vorgesehen. Davon ausgenommen sind Anpassungen bestehender Auslagerungsverträge, detaillierte Informationen hierzu liefert das Übersendungsschreiben der Bundesbank.

Auf technischer Ebene sind vor allem die neu ergänzten BAIT-Kapitel von Relevanz. Hinzugekommen ist etwa der Bereich operative Informationssicherheit, der einerseits Maßnahmen festlegt, um den Schutz von IT-Systemen im laufenden Betrieb zu gewährleisten, und andererseits regelmäßige Kontrollen vorschreibt. Zu den vorgesehenen Schutzmaßnahmen zählen etwa die sichere Konfiguration von Geräten, die Segmentierung des Netzwerks, die Verschlüsselung von Daten und auch die physische Absicherung von sensiblen Bereichen wie Rechenzentren (Perimeterschutz).

Um Bedrohungen rechtzeitig erkennen zu können, fordert BAIT neben der Protokollierung und Auswertung sicherheitsrelevanter Ereignisse durch das Security Incident & Event Management auch weitere Kontrollen der Informationssicherheit. Durch Gap-Analysen dokumentieren Institute Abweichungen von den vorgesehenen Schutzzielen. Im Rahmen von Schwachstellenscans überprüft eine dafür entwickelte Software IT-Systeme automatisch auf bekannte Sicherheitslücken. Bei Penetrationstests versuchen externe Spezialisten, in das System einzudringen, und decken so mögliche Einfallstore auf. All diese Tests müssen nicht nur in regelmäßigen Intervallen, sondern auch anlassbezogen durchgeführt werden.

Laufende Überwachung der IT

Der zweite neue Abschnitt der BAIT-Novelle beschäftigt sich mit dem IT-Notfallmanagement. Hier werden in Abstimmung mit dem allgemeinen Notfallmanagement (MaRisk AT 7.3) spezifische Ziele und Vorgaben für IT-Notfallpläne festgelegt. Ein geeignetes Konzept muss sowohl den Notbetrieb als auch den Wiederanlauf und die volle Wiederherstellung der Geschäftsprozesse umfassen. Das Festlegen der Parameter für die Wiederherstellung, etwa der vorgesehenen Anlaufzeit, obliegt den Instituten. Die Wirksamkeit des Notfallkonzepts muss aber mindestens jährlich getestet werden.

Dabei sorgen insbesondere zwei Vorgaben für Komplikationen: Zum einen muss das IT-Testkonzept sowohl Kontrollen einzelner Komponenten als auch von Systemverbünden und deren Zusammenfassung zu ganzen Prozessen abdecken, was die Zahl an unterschiedlichen Testvarianten stark erhöht. Zum anderen sind beim Notfallmanagement auch Abhängigkeiten durch externe Auslagerungen in der IT zu beachten. Hier ist eine Abstimmung mit den betreffenden Dienstleistern und das Entwickeln von Alternativstrategien notwendig. Bei der Gestaltung der Auslagerungsverträge haben Finanzdienstleister künftig darauf zu achten, dass die Sicherheitsmaßnahmen mindestens den Zielvorgaben des Instituts selbst entsprechen.

Tests und Kontrollen: Das ist der rote Faden, der sich durch die Anpassungen von KRITIS, BAIT und MaRisk zieht. Auch wenn gewissenhafte Finanzdienstleister schon jetzt zahlreiche der neuen Anforderungen abdecken, dürften die Vorgaben an das Testregime für viele Institute eine Verschärfung bedeuten. Durch die Überprüfung von Notfallplänen und Schutzmaßnahmen ergeben sich dabei insbesondere organisatorische Herausforderungen.

Während rein technische Schutzmaßnahmen vergleichsweise einfach durch IT-Verantwortliche umgesetzt werden können, erfordern die vorgesehenen Kontrollen viel Planung und Koordination. Es gilt Testkonzepte zu erstellen, Fachabteilungen einzubinden und über Auswirkungen auf den IT-Betrieb zu informieren, externe Security-Dienstleister zu finden und zu briefen, Ergebnisse zu protokollieren und laufend an die Geschäftsleitung zu berichten. Für Finanzinstitute, die unter die KRITIS-Verordnung fallen, kommt zusätzlich die Abstimmung mit dem BSI hinzu. Der Aufgabenbereich von Sicherheitsverantwortlichen wächst also weiter.

Herausforderungen an Organisationen

Nicht nur die Politik richtet ihre Aufmerksamkeit verstärkt auf den Bereich Informationssicherheit, auch Banken und Finanzdienstleister müssen sich dem Thema intensiver widmen, um mit steigenden gesetzlichen Anforderungen Schritt halten zu können. Hier stellt sich oft eine Ressourcen-Frage: Wie kann mehr Zeit in die Organisation von Tests und die Auswertung von Sicherheitsprotokollen fließen, wenn IT-Abteilungen bereits mit ihren bestehenden Aufgaben ausgelastet sind?

Die einfachste Möglichkeit, Sicherheitsverantwortliche für diese neuen Pflichten freizuspielen, ist daher die Investition in geeignete Softwarelösungen, welche den Zeitaufwand von Routineaufgaben in der IT deutlich reduzieren oder diese sogar gänzlich automatisieren können. Entsprechende Produkte existieren für die unterschiedlichsten Bereiche, von der Kontrolle von Endgeräten und Sicherheitseinstellungen bis hin zur Segmentierung des Netzwerks und Backup-Lösungen. Eine IAM-Lösung stellt sicher, dass der Zugang zu Daten und Ressourcen in allen verknüpften Systemen korrekt konfiguriert ist. Durch automatische Anpassungen und Überprüfungen sowie die vollständige Dokumentation aller Änderungen trägt Identity und Access Management nicht nur zur Compliance bei, sondern entlastet zugleich die IT. So lassen sich gesetzliche Vorgaben an die Informationssicherheit bestmöglich erfüllen.

Helmut Semmelmayer

Mitglied der Geschäftsführung, Tenfold Software GmbH, Wien

Cyberangriffe gehören zu den gegenwärtig größten operationellen Risiken im Finanzsektor. Das liegt unter anderem daran, dass die Cyberkriminellen, auch Hacker genannt, immer professionellere Methoden für ihre Attacken entwickeln. An Einfallsreichtum mangelt es den Kriminellen hierbei auch nicht, weshalb die Zahlen von registrierten Cyberattacken kontinuierlich zunehmen. Angesichts dieser gestiegenen Bedrohungslage setzt sich die Verschärfung gesetzlicher IT-Sicherheitsstandards 2021 weiter fort. Als Teil der kritischen Infrastrukturen (KRITIS) ist der Finanzsektor etwa von der Novelle des IT-Sicherheitsgesetzes betroffen, die im April beschlossen wurde. Des Weiteren hat die Bundesanstalt für Finanzdienstleistungsaufsicht im August nach längerer Konsultation aktualisierte Versionen der Verwaltungsvorschriften MaRisk und BAIT veröffentlicht. Der Autor des vorliegenden Beitrags informiert über die wichtigsten Neuerungen für Finanzinstitute. (Red.)