bank und markt

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

10

15. Oktober 2024

DIE DIGITALE BANK

Digitaler Sonderdruck

Finanzdienstleister und IT-Partner im Sturm der Regulierung

Markus Laube

HERAUSFORDERUNG CYBERSICHERHEIT

Foto: pixabay / u_etaflffuni

Finanzdienstleister und IT-Partner im Sturm der Regulierung

Von Markus Laube

Foto: Adobe Stock/Maxim

DORA ist weit mehr als „nur" eine weitere Regularie in der Finanzbranche, sagt Markus Laube. Denn weil auch Dienstleister sich danach ausrichten müssen, wird DORA gewissermaßen zur Sollbruchstelle zwischen Finanzunternehmen und ihren technischen Dienstleistern. Damit gehören sämtliche Verträge auf den Prüfstand, damit das Sicherheitsmanagement nicht nur im eigenen Haus, sondern auch bei den Dienstleistern stimmt. Generell gilt es, Sicherheitsleitstellen und drei Verteidigungslinien aus Fachabteilungen, Spezialisten und externen Prüfungen zu etablieren. Red.

BAIT, MaRisk, DSGVO und nun auch noch DORA: Richtlinien und Regularien prägen das Geschäft in der Finanzbranche. Mit dem Digital Operational Resilience Act der Europäischen Union stehen Finanzdienstleister ab Januar 2025 unter noch genauerer Beobachtung durch Aufsichtsbehörden. Damit steigen auch die Anforderungen für IT-Partner deutlich – und das nicht nur in technischer Hinsicht.

Im Finanzdienstleistungssektor weht bekanntlich ein anderer Wind als in anderen Branchen. Hier regeln harte nationale und internationale Vorschriften, Richtlinien und Gesetze die Stabilität und Transparenz im Marktsegment. Ein regelrechter Sturm kommt auf bei Banken, Sparkassen oder Assekuranzen, wenn der Begriff Digital Operational Resilience Act (DORA) fällt. Die im September 2022 verabschiedete EU-Verordnung zielt darauf ab, die digitale Widerstandsfähigkeit von Finanzunternehmen zu stärken und sicherzustellen, dass Organisationen robust gegenüber Cyberangriffen, IT-Ausfällen und anderen Bedrohungen sind. Doch was vordergründig als eine weitere Regularie im Wirtschaftszweig anmutet, hat es besonders in sich. Und das liegt nicht nur an der knappen Deadline bis zum 17. Januar 2025.

DORA schreibt Finanzinstituten, Versicherungen, Zahlungsdienstleister und Investmentfirmen eine Fülle an rigorosen Vorschriften und Vorgaben ins Pflichtenheft. Dazu gehören:

IKT-Risikomanagement: Finanzinstitute müssen einen umfassenden Rahmen für das IKT-Risikomanagement implementieren. Dieser Rahmen soll die Identifikation, den Schutz, die Erkennung, die Reaktion und die Wiederherstellung von IKT-bezogenen Risiken abdecken. Regelmäßige Bewertungen und Aktualisierungen sind erforderlich, um sich an neue Bedrohungen und Schwachstellen anzupassen.

Governance und Organisation: Interne Governance-Strukturen für das IKT-Risikomanagement sollen eingerichtet werden. Die Unternehmensleitung trägt die Verantwortung für die Überwachung der IKT-Risiken. Dies umfasst die Entwicklung und Genehmigung der Digital Operational Resilience Strategy (DORS) sowie die Sicherstellung von Richtlinien zum Schutz der Datenvertraulichkeit, -integrität und -verfügbarkeit.

Management und Meldung IKT-bezogener Vorfälle: Finanzinstitute müssen Prozesse zur Erkennung, Verwaltung und Meldung signifikanter IKT-Vorfälle an die zuständigen Behörden einrichten. Die Vorfälle werden nach ihrem Einfluss und ihrer Schwere klassifiziert. Bei erheblichen Auswirkungen auf Kunden müssen diese ebenfalls informiert werden.

Foto: noris network

Markus Laube, Team Lead Governance, Risk & Compliance, noris network AG, Nürnberg

Testen der digitalen operationellen Resilienz: Die digitale Betriebsresilienz von Finanzinstituten muss regelmäßig getestet werden. Dazu gehören Bedrohungsanalysen und Penetrationstests, um die Effektivität der IKT-Systeme und -Kontrollen sicherzustellen. Häufigkeit und Umfang der Tests hängen von der Kritikalität und Komplexität der betroffenen IKT-Systeme ab.

Management des IKT-Drittparteienrisikos: Finanzinstitute müssen gründliche Risikoanalysen durchführen, bevor sie Drittanbieter engagieren, und sicherstellen, dass wichtige Vertragsbestimmungen vorhanden sind. Die Leistung und Sicherheitspraktiken von Drittanbietern müswsen kontinuierlich überwacht werden. Kritische Drittanbieter unterliegen einer zusätzlichen Aufsicht.

Informationsaustausch: DORA fördert den Informationsaustausch über Cyber-Bedrohungen und Schwachstellen zwischen Finanzinstituten. Diese Austauschvereinbarungen sollen die kollektive Resilienz verbessern und eine schnelle Reaktion auf neue Bedrohungen ermöglichen. Der Informationsaustausch muss den gesetzlichen und regulatorischen Anforderungen entsprechen, um Datenschutz und Vertraulichkeit zu gewährleisten.

Sollbruchstelle für Partnerschaft mit IT-Dienstleistern

Als wäre es mit der internen Transformation nicht genug, schreibt die neue EU-Verordnung also nun auch Partnerunternehmen wie Rechenzentren oder IT-Dienstleistern vor, die Zusammenarbeit strikt nach diesen Richtlinien auszurichten. Die Folge: DORA wird quasi zur Sollbruchstelle für die Partnerschaft zwischen IT-Dienstleistern und Finanzmarktteilnehmern wie Banken und Kreditinstituten, Versicherern und sogar Pensionsfonds oder Börsen und Handelsplattformen.

Denn DORA erwartet weit mehr als die Umsetzung der Cybersicherheit wie Datenverschlüsselung, physischem Zugangsschutz oder Anti-Ransomware-Mechanismen. Auch existierende und neue Verträge zwischen Finanzdienstleister mit Partnerunternehmen müssen im Einklang mit den neuen DORA-Vorschriften bis ins Detail analysiert und überarbeitet werden.

Mit Blick auf das Vertragsmanagement bestimmt DORA unter anderem Anforderungen an Verträge mit IKT-Drittparteien, die in das Vertragsmanagement der Finanzunternehmen Eingang finden müssen. In der Praxis bedeutet das: (Bestands-) Verträge kategorisieren, Soll-Anforderungen festlegen, Gap-Analysen durchführen und potenzielle Lücken schließen. Darüber hinaus verändert DORA die Anforderungen an die Verantwortung und Haftungsrisiken von Unternehmen und Geschäftsleiter im Hinblick auf IKT-Drittrisiken. Hier gilt es beispielsweise, den Umfang und die Bedingungen des Versicherungsschutzes zu überprüfen und gegebenenfalls anzupassen. Mehr noch: DORA sieht vor, dass Finanzunternehmen nur noch Verträge mit DORA-konformen IT-Dienstleistern schließen dürfen.

Vertrauen zwischen Banken und Dienstleistern entscheidend

Anders ausgedrückt: Das Vertrauen und der partnerschaftliche Aspekt werden mit DORA zur geschäftskritischen Komponente. Finanzdienstleister müssen künftig sicherstellen, dass auch lange nach Beginn der Zusammenarbeit der richtige Partner an ihrer Seite steht. Und sie müssen sich darauf verlassen können, dass ihr Dienstleister das Risikomanagement nicht auf die leichte Schulter nimmt – mit regelmäßigen Risikobewertungen und Schwachstellen-Scans, der Planung und Management von Sicherheitsvorfällen, externen Audits und internen Revisionsmechanismen und sogar bankenspezifischen Schulungen und „ISMS-Awareness-Trainings" für eigene Mitarbeiter – durch alle Abteilungen hinweg.

Doch auch das klassische Handwerkszeug samt Technologien von IT-Dienstleistern im Finanzumfeld ist vor DORA „nicht mehr sicher". Das gilt vor allem in den Bereichen Datenmanagement und IT-Sicherheit und orientiert sich stark an den steigenden Herausforderungen an den Datenschutz und die Datensicherheit auch und vor allem in KRITIS-Organisationen. Ob in Sachen Cyberbedrohungen mit fortschrittlichen Erkennungs- und Bedrohungssystemen, dem kontinuierlichen Monitoring und Echtzeitinformationen oder im Zusammenhang mit der Datenintegrität und Verfügbarkeit von Systemen – die EU versteht DORA als Universalwerkzeug.

SIEM: Sicherheit ohne Kompromisse

Für IT-Dienstleister, die ab Anfang des kommenden Jahres im Finanzsektor weiter tätig sein möchten, steht viel auf dem Spiel. Das gilt beispielsweise dann, wenn es um Sichtbarkeit und Transparenz zu Aktivitäten in den Systemen von Kunden geht. Hier hat sich ein Security-Information- & Event-Management (SIEM) bewährt. SIEM umfasst ein Security-Management-System, das volle Sichtbarkeit und Transparenz zu Aktivitäten innerhalb des Informationsverbundes bietet. In technischer Hinsicht erhalten Kollektoren Meldungen von Systemen wie Datenbanken, Servern oder Netzwerkkomponenten und „normalisieren diese". Mithilfe von Korrelationstechniken lassen sich dann die Logs automatisch in verwertbare und übersichtliche Informationen umwandeln – in Form von Diagrammen oder Dashboards. Wurden einmal wichtige Zusammenhänge gefunden, informiert das SIEM-System die verantwortlichen Mitarbeiter über die potenziellen Probleme.

Noch effektiveren Schutz bietet ein SIEM in Form eines Security Operation Centers (SOC). Beim SOC handelt es sich um eine Art Sicherheitsleitstelle, die sich um den Schutz der IT-Infrastruktur eines Unternehmens kümmert. Um diese Aufgabe leisten zu können, integriert, überwacht und analysiert das SOC alle sicherheitsrelevanten Systeme.

SIEM im SOC hat für Unternehmen aus der Finanzdienstleistungsbranche also gleich mehrere Vorteile. Einer der wichtigsten: Unternehmen aus dem Finanzumfeld erhalten die Möglichkeit, in Echtzeit auf Bedrohungen reagieren zu können. Das SOC von Noris Network beispielsweise umfasst ein Expertenteam, das Cybersicherheitsvorfälle rund um die Uhr überwacht, erkennt und behebt. Mit einer Strukturanalyse werden IT-Systeme und Anwendungen erfasst; eine anschließende Schutzbedarfsfeststellung konkretisiert die Risikobewertung. Über die Erstellung von „Use Cases" und deren „Rules" lässt sich definieren, welche Eventinformationen miteinander zu korrelieren sind und welche daraus resultierenden mög-

lichen Sicherheitsvorfälle zu mitigieren sind. Im Vulnerability- und Patch-Management werden Anpassungen durchgeführt und neue Anforderungen festlegt. Ganz im Sinne von DORA können dabei nicht nur die IT-Komponenten selbst überwacht werden. Bei Noris Network wurden sogar der Perimeterschutz der Hochsicherheitsrechenzentren und die Zutrittskontrollsysteme in das Security-Information- und Event-Management integriert.

3Lod: Dreifach hält besser

Ein weiteres bewährtes und seit DORA besonders relevantes Konzept hört auf die Bezeichnung Three Lines of Defence (3Lod). Der Ansatz unterstützt Organisationen dabei, Risiken systematisch zu managen, klare Verantwortlichkeiten festzulegen und die Effektivität interner Kontrollsysteme zu verbessern. Die drei Verteidigungslinien sind folgendermaßen aufgebaut:

– Die erste Linie führt operative Kontrollen durch.

– Die zweite Linie überwacht und unterstützt die erste Linie.

– Die dritte Linie bewertet die Effektivität der ersten beiden Linien unabhängig.

Die erste Verteidigungslinie besteht aus allen Fachbereichen, die das operative Geschäft verantworten und auf deren Tagesgeschäft sich unternehmerische Risiken auswirken können. Sie sind dafür zuständig, Risiken in ihrem operativen Geschäft frühzeitig zu erkennen, zu beurteilen, zu steuern, zu überwachen und zu reduzieren.

Die zweite Verteidigungslinie umfasst spezialisierte Funktionen oder Abteilungen, die das operative Management überwachen und unterstützen. Sie helfen bei der Festlegung von Richtlinien, Verfahren und Best Practices. Dazu gehören die Entwicklung und Überwachung von Risikomanagement- und Compliance-Programmen, die Durchführung von Risikoanalysen und Bewertungen, die Beratung und Schulung des operativen Managements in Bezug auf Risiko- und Compliance-Anforderungen sowie die Überprüfung der Einhaltung interner und externer Vorschriften.

Und die dritte Verteidigungslinie bietet eine unabhängige Überprüfung und Bewertung der Wirksamkeit des Risikomanagements und der Kontrollen durch die ersten beiden Linien. Sie ermöglicht eine objektive Sicherheit für das Management und die Aufsichtsbehörden und beinhaltet die Durchführung von Audits und Prüfungen von Prozessen und Kontrollen, die Bewertung der Effektivität und Effizienz des Risikomanagements, die Berichterstattung über die Ergebnisse an das Management und die Aufsichtsbehörden sowie die Empfehlung von Verbesserungen der Risikomanagementpraktiken und -kontrollen.

Fest steht: Mit DORA kommt ein regulativer Brocken auf die Finanzbranche zu. Rechenzentrumsbetreiber und IT-Dienstleister sind spätestens jetzt gefordert, die Umsetzung der Vorgaben rasch voranzutreiben – und die Partnerschaft auf ein stabiles Fundament zu stellen. ■

SICHERHEIT

Neue Malware-Attacken: NFC-Relais-Technik statt Smartphone-Rooting

Trotz aller Bemühungen, die Sicherheit im Online-Banking und Zahlungsverkehr zu gewährleisten, werden immer wieder neue Betrugsmethoden aufgedeckt. Im August berichtete Eset über eine erstmals im November 2023 beobachtete Malware namens Ngate, die Kunden von drei tschechischen Banken ins Visier nahm. Sie kann die Daten von Zahlungskarten, inklusive PIN der Opfer, über eine bösartige App, die auf deren Android-Geräten installiert wurde, an das gerootete Android-Telefon des Angreifers übermitteln.

Das Hauptziel dieser Kampagne war es, unautorisierte Geldabhebungen von Geldautomaten aus den Bankkonten der Opfer zu ermöglichen. Dafür wurden Nahfeldkommunikationsdaten (NFC) von den physischen Zahlungskarten der Opfer über ihre kompromittierten Android-Smartphones mithilfe der Malware ans Gerät des Angreifers weitergeleitet. Diese NFC-Relais-Technik wurde nach Angaben von Lukáš Štefanko von Eset, der die neuartige Bedrohung entdeckte, bisher bei keiner anderen Android-Malware gesehen. Es sei das erste Mal, dass eine derartige Malware im Umlauf entdeckt wurde, die ohne das sogenannte „Rooten" des Smartphones, also tiefere Änderungen am Betriebssystem, funktioniert.

Die Technik basiert auf einem Tool namens NFC Gate, das von Studenten der Technischen Universität Darmstadt entwickelt wurde, um NFC-Verkehr zu erfassen, zu analysieren oder zu verändern. Daher haben die Forscher diese neue Malware-Familie Ngate genannt.

Um die Android-Geräte ihrer Opfer zu kompromittieren, greifen die Betrüger auf eine Kombination aus bewährten Techniken wie Social Engineering und Phishing zurück. In diesem Fall erhielten die Opfer eine SMS, die angeblich von ihrer Bank stammte und sie aufforderte, eine App herunterzuladen, um ein angebliches Problem mit ihrem Konto zu beheben. Sobald sie diese App installiert hatten, wurde ihr Gerät von der Ngate-Malware infiziert.

Die Angreifer nutzen somit einmal mehr die Schwachstelle in der gesamten Sicherheitslandschaft, an der Banken und Sparkassen am wenigsten ansetzen können: die Kunden. Das einzige Mittel dagegen ist Aufklärung. Ob jedoch die Kreditwirtschaft allein genug tun kann, um die Menschen für die Risiken zu sensibilisieren und darüber aufzuklären, wie sie sich schützen und Betrug vorbeugen können, scheint immer fraglicher. Mehr Finanzbildung in den Schulen könnte dazu sicher einen Beitrag leisten. Doch damit werden die vielen Älteren, die möglicherweise besonders leichte Opfer von Social-Engineering-Methoden sind, nicht erreicht. Das BSI wird deshalb sehr viel stärker als bisher an die Öffentlichkeit gehen müssen. Auf die Dauer wird es deshalb ohne groß angelegte und breit gestreute Kampagnen, die alle Zielgruppen erreichen, nicht gehen. Red.