5 wichtige DORA-Anforderungen

und wie starkes Identity-Management bei der Umsetzung hilft

Die rasante Digitalisierung des europäischen Finanzsektors hat den Weg für viele Innovationen bereitet, aber auch die Angriffsfläche für Cyberbedrohungen deutlich vergrößert. Die Europäische Union hat darauf mit dem Digital Operational Resilience Act (DORA) reagiert, der eine verbindliche Roadmap zur Verbesserung der Cybersicherheit in der Branche definiert.

Der Schlüssel zur Einhaltung der Bestimmungen ist ein strategischer Umgang mit digitalen Identitäten. Hier erfahren Sie, wie Sie 5 zentrale DORA-Vorgaben adressieren.

1 Ein Framework zum Managen von IKT-Risiken

DORA verpflichtet Unternehmen und Institute, ihre IKT-Systeme zu mappen, alle IKT-Features und -Assets zu identifizieren und kontinuierlich zu überwachen sowie robuste Mechanismen zur Erkennung von Anomalien und zur Verhinderung von Systemausfällen zu implementieren. Unterstützend dazu müssen eine Backup-Richtlinie und eine Recovery-Strategie definiert werden, um im Falle eines Zwischenfalls die Ausfallzeiten zu minimieren.

Warum Identity-Management wichtig ist

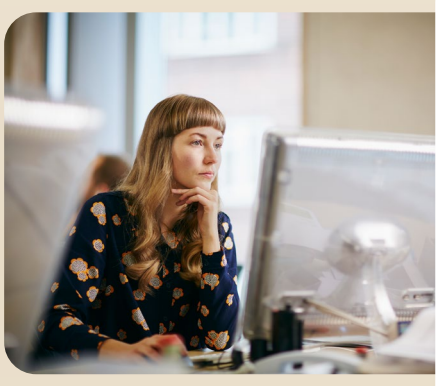
Eine moderne Identity-Lösung, die sowohl Ihre Mitarbeiter- als auch Ihre Kundenidentitäten schützt, ist eine zentrale Komponente zeitgemäßer Risikomanagement-Frameworks. Sie bietet Ihnen lückenlose Transparenz über die Zugriffsrechte im Unternehmen sowie über Dritte, die auf Ihre Services zugreifen.

2 Meldung sicherheitsrelevanter IKT-Vorfälle

Eine der zentralen Forderungen von DORA ist die zeitnahe Dokumentation und Meldung sicherheitsrelevanter IKT-Vorfälle. Diese Schritte sollten in einen umfassenden Incident-Management-Prozess eingebunden sein, der dazu dient, IKT-Vorfälle zu identifizieren, zu managen und zu melden – und darüber hinaus die Ursachen zu ermitteln und zu beseitigen, um zukünftige Vorfälle zu verhindern.

Identity-Management wichtig ist

Lückenlose Transparenz über die Aktivitäten auf Ihren Systemen ist heute unverzichtbar – einschließlich der Dokumentation, wie, wo und wann ein Zugriff erfolgte. Eine Identity-Plattform stellt Ihnen diese forensischen Informationen zur Verfügung und macht es Ihnen damit leicht, Vorfälle präzise und zeitnah den zuständigen Behörden zu melden.



3 Digitale Bewertung der operativen Resilienz

Finanzinstitute müssen ihre IKT-Systeme regelmäßig testen, um zu validieren, ob sie auf eventuelle Vorfälle vorbereitet sind, um etwaige Schwachstellen und Lücken zu identifizieren und um zeitnah auf Vorfälle reagieren zu können. Der Schutz kritischer IKT-Systeme und -Anwendungen sollte jährlich von unabhängigen Dritten getestet und bewertet werden.

Identity-Management wichtig ist

Eine Identity-Plattform wie Okta ist in doppelter Hinsicht von Bedeutung: Sie weist sie proaktiv auf das Gefahrenpotenzial überprivilegierter Accounts hin. Und außerdem können Sie mit der Plattform selbst Tests durchführen, um verschiedene Abläufe und die Provisionierung von Zugriffsrechten zu überprüfen. Auf diese Weise können Sie gewährleisten, dass die Prozesse und die Sicherheitskontrollen optimal konfiguriert sind.

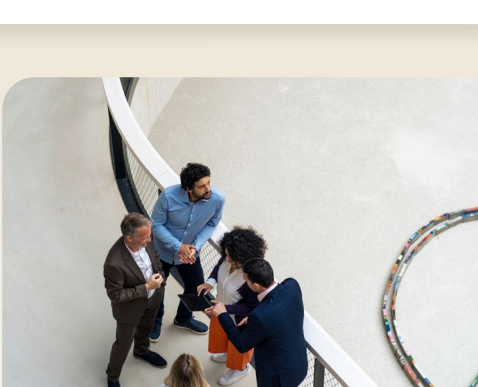
17. Januar 2025
Das Datum, an dem DORA in Kraft getreten ist.

4 IKT-Risikomanagement für Dritte

DORA betrifft nicht nur Finanzunternehmen, sondern auch die für diese tätigen IKT-Anbieter. Dies erfordert ein aktives Risikomanagement für Drittanbieter, bei dem deren Unternehmen die volle Verantwortung für die Einhaltung aller rechtlichen und finanziellen Vorgaben übernehmen. Zudem gilt es darauf zu achten, dass nicht zu viele Aufgaben bei einem Anbieter gebündelt werden.

Identity-Management wichtig ist

In einer Welt, in der komplexe Lieferketten zu den gefährlichsten Schwachstellen vieler Unternehmen gehören, kommt Identity-Management eine Schlüsselrolle zu: Es ermöglicht die Definition verbindlicher Zugriffsrechte und garantiert lückenlose Transparenz über das Unternehmen hinaus. So bleiben Sie durchgehend über potenzielle Schwachstellen Ihrer Lieferanten informiert und können schneller auf Bedrohungen reagieren.



2 % des Jahresumsatzes
Bußgeld bei Nicht-Einhaltung von DORA-Vorgaben

x2
Cybersicherheit ist für europäische Banken weiterhin das größte Risiko. 82 % der CROs (Chief Risk Officers) sagen, dass dies die größte Bedrohung für ihr Unternehmen darstellt.

Quelle: EY

5 Informationsaustausch

Um die Cyberresilienz in der gesamten Branche zu verbessern, sind Finanzunternehmen verpflichtet, Informationen über Cyberbedrohungen auszutauschen, z. B. Daten zu Kompromittierungen, Taktiken und Techniken. Dabei müssen die gemeinsam genutzten Informationen durchgehend angemessen geschützt werden, d. h. unter Beachtung der Vertraulichkeitsprinzipien, des Schutzes personenbezogener Daten und der Leitlinien der Wettbewerbspolitik.

Identity-Management wichtig ist

Eine Identity-Plattform, die Ihre Daten, Identities und Berechtigungen durchgehend überwacht, liefert wertvolle Einblicke in neue Bedrohungen. Automatische Benachrichtigungen bei ungewöhnlichen Aktivitäten und robuste Identity-Prozesse stellen sicher, dass kritische Informationen jederzeit optimal geschützt sind und verantwortungsvoll weitergegeben werden. Dies trägt zu einem kollaborativen und sicheren Miteinander in der Finanzbranche bei.

Möchten Sie mehr über die DORA-Compliance wissen?

Wenn Sie mehr über DORA und darüber erfahren möchten, wie Identity-Management Sie bei der Einhaltung der Bestimmungen unterstützen kann, lesen Sie unser Whitepaper:
Digitale Identitäten und DORA: Stärkung von Cybersicherheit und Resilienz im Finanzsektor

Whitepaper herunterladen