5 wichtige DORA-Anforderungen

und wie Ihnen starke Identities bei der Umsetzung helfen

Die rasante Digitalisierung des europäischen Finanzsektors hat den Weg für viele Innovationen bereitet, die Angriffsfläche für Cyber-Bedrohungen aber auch deutlich vergrößert. Die Europäische Union reagiert darauf mit dem Digital Operational Resilience Act (DORA), 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 Forderungen des DORA adressieren.

1 Ein Framework zum Management der 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 muss eine Backup-Policy und eine Recovery-Strategie definiert werden, um die Ausfallzeiten im Falle eines Incidents zu minimieren.

Warum Identitäten so wichtig sind

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 Zugangsrechte im Unternehmen und bei der Anbindung externer Dritter, 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 sollte in einen umfassenden Incident-Management-Prozess eingebunden sein, der dazu dient, IKT-Incidents zu identifizieren, zu managen und zu melden – und darüber hinaus die Ursachen zu ermitteln und zu beseitigen, um zukünftige Vorfälle zu verhindern.

Warum Identitäten so wichtig sind

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 Incidents 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.

Warum Identitäten so wichtig sind

Eine Identity-Plattform wie Okta ist in doppelter Hinsicht von Bedeutung: Zum einen weist sie proaktiv auf das Gefahrenpotenzial überprivilegierter Accounts hin; zum anderen kann sie aber auch selbst zum Gegenstand des Tests werden, um die Abläufe bei der Bereitstellung von Accounts und Berechtigungen zu validieren – und auf diese Weise zu gewährleisten, dass die Prozesse und die Sicherheitsmechanismen optimal konfiguriert sind.

17. Januar 2025
Die DORA-Vorgaben treten in Kraft

4 Third-Party-IKT-Risiken

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.

Warum Identitäten so wichtig sind

In einer Welt, in der komplexe Lieferketten zu den gefährlichsten Schwachstellen vieler Unternehmen gehören, kommt Identitäten eine Schlüsselrolle zu: Sie ermöglichen es, verbindliche Zugangsrechte zu definieren, und garantieren 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

5 Informationsaustausch

Um die Cyber-Resilienz über die gesamte Branche hinweg zu verbessern, sind Finanzunternehmen verpflichtet, Informationen über Cyber-Bedrohungen auszutauschen – etwa Daten zu Kompromittierungen, Taktiken und Techniken. Dabei müssen die gemeinsam genutzten Informationen durchgehend angemessen geschützt werden – sprich: unter Beachtung der Vertraulichkeitsprinzipien, des Schutzes personenbezogener Daten und der Leitlinien der Wettbewerbspolitik.

Warum Identitäten so wichtig sind

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 geteilt werden. Dies trägt zu einem kollaborativen und sicheren Miteinander in der Finanzbranche bei.

x2
Die Cyberattacken auf europäische Finanzdienstleister haben sich zwischen Q2 2022 und Q2 2023 mehr als verdoppelt.

Quelle: Akamai, State of the Internet

Möchten Sie mehr über die DORA-Compliance wissen?

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

Zum Download