ZUTRITT

Resilienz im Finanzsektor

Physische Sicherheit als wichtiger Baustein für die DORA-Compliance

DORA (Digital Operational Resilience Act) ist eine sektorspezifische EU-Verordnung für Finanzorganisationen, die Anfang 2023 in Kraft trat und seit dem 17. Januar 2025 anzuwenden ist. Die Rolle des Physical Identity & Access Managements (PIAM) in diesem Zusammenhang erläutert Johanna Wünsch, Senior Marketing Managerin bei ID-ware.

Ziel des Digital Operational Resilience Acts (DORA) ist es, die IT-Sicherheit von Finanzorganisationen wie Banken, Versicherungen und Wertpapierfirmen zu stärken und sicherzustellen, dass der Finanzsektor in Europa in der Lage ist, im Falle einer schweren operativen Störung widerstandsfähig zu bleiben. DORA harmonisiert die Vorschriften für die operative Resilienz des Finanzsektors und gilt für 20 verschiedene Arten von Finanzunternehmen sowie für Drittanbieter von Informations- und Kommunikationstechnologie (IKT).

Da DORA als sektorspezifischer EU-Rechtsrahmen in Bezug auf die Umsetzung der NIS2-Richtlinie für Finanzunternehmen zu betrachten ist, gelten für die IKT-bezogenen Hauptbereiche die Bestimmungen von DORA anstelle der in der NIS2-Richtlinie vorgesehenen Bestimmungen.

Genau wie NIS2 zielt DORA darauf ab, Finanzorganisationen vor identitätsbasierten Cyberangriffen und unbefugtem Zugriff auf Informationen zu schützen, der natürlich auch physisch erfolgen könnte. Das Prinzip lautet: Nur die richtigen Personen dürfen zur richtigen Zeit Zugriff auf die richtigen Informationen haben.

Eine sichere und auditierbare PIAM-Plattform gewährleistet, dass physische Identitäten nur auf die Daten und Systeme zugreifen können, die sie zur Erfüllung ihrer jeweiligen Aufgabe wirklich benötigen, und somit sensible Informationen geschützt werden. Organisationen können z. B. die PIAM-Suite von ID-ware, einem international führenden Anbieter smarter Lösungen für Identifizierungs- und Authentifizierungsprozesse, zur Verbesserung ihres Risikomanagements einsetzen.

Johanna Wünsch, Senior Marketing Managerin bei ID-ware

Eine solche Plattform erhöht die Widerstandsfähigkeit sowie Auditierbarkeit und bietet Reporting für den gesamten Lebenszyklus von Ausweiskarten inklusive der

physischen Zutrittsrechte für Mitarbeiter, Besucher und Fremdfirmen.

Wie genau hilft eine PIAM-Plattform dabei, die fünf Hauptbereiche von DORA umzusetzen?

IKT-Risikomanagement

DORA erwartet von Finanzorganisationen, dass sie ein Rahmenkonzept für das IT-Risikomanagement einrichten, dokumentieren und mindestens einmal pro Jahr überprüfen. Wichtig ist die systematische Verwaltung von Zugriffs- und Zutrittsrechten – sowohl im digitalen als auch im physischen Bereich. Die Kontrolle über den gesamten Lebenszyklus von Identitäten und Zutrittsberechtigungen spielt eine zentrale Rolle. Eine PIAM-Plattform verwaltet den Lebenszyklus von Ausweiskarten für Mitarbeiter, Besucher und Fremdfirmen einschließlich physischer Zutrittsberechtigungen über mehrere Standorte hinweg, so dass jeder Schritt in Bezug auf Berechtigungen dokumentiert wird.

Die Einhaltung von Richtlinien stellt sicher, dass nur Personen mit berechtigten Rollen Zutritt zu eingeschränkten Bereichen haben. Die automatisierte Verwaltung von Zutrittsberechtigungen, z. B. der sofortige Entzug aller Berechtigungen über alle Systeme hinweg, wenn ein Mitarbeiter das Unternehmen verlässt, minimiert oder verhindert mögliche Risiken.

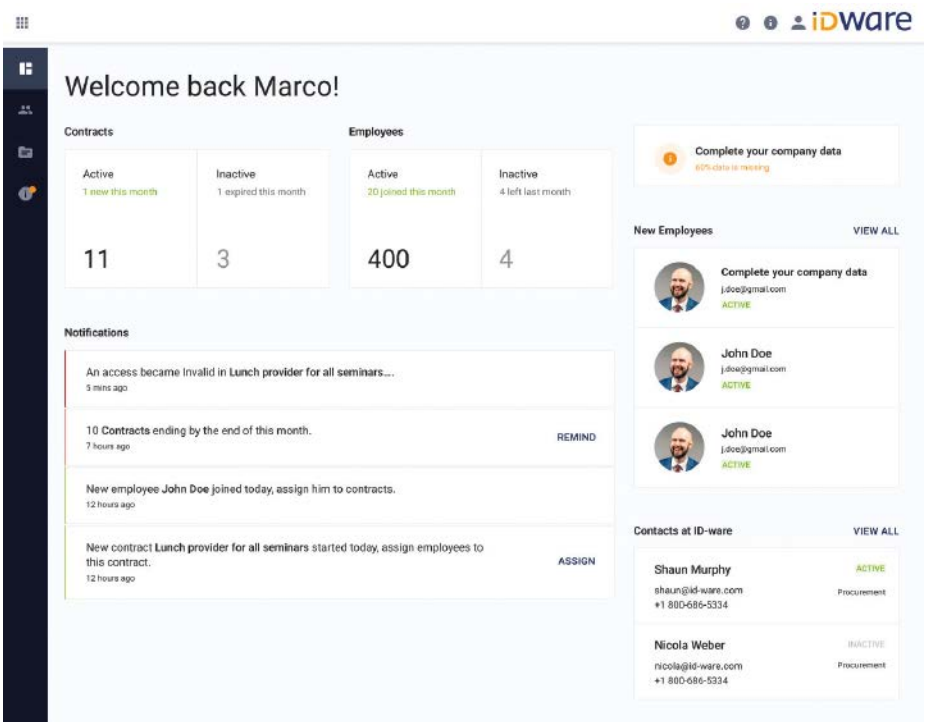
IKT-Drittanbieter-Risikomanagement

Die meisten Organisationen gewähren nicht nur internen Mitarbeitern Zutritt, sondern auch Fremdfirmen – z. B. dem Personal von Dienstleistern. Ein automatisiertes Contractor Management innerhalb einer PIAM-Plattform unterstützt Organisationen bei der Einhaltung der DORA-Anforderung, alle vertraglichen Vereinbarungen mit Dritten zu überwachen. Mehrere Standorte und unterschiedliche Fremdfirmen erhöhen das Risiko doppelter oder gefälschter Identitäten für Organisationen. Daher ist es wichtig, solche Risiken durch eine zentrale Kontrolle aller Aktivitäten der Fremdfirmen und ihrer physischen Zutrittsberechtigungen zu reduzieren.

Ein sicheres Contractor Management als Baustein einer PIAM-Plattform ermöglicht den klaren Überblick über alle Fremdfirmen und deren Status sowie Zutrittsberechtigungen an allen Standorten einer Organisation. Zeitgebundene, rollenbasierte physische Zutrittsberechtigungen können erteilt werden, um Risiken zu minimieren.

Testen der digitalen Ausfallsicherheit

Zur Einhaltung der DORA-Bestimmungen müssen Organisationen jährlich Tests durchführen, um sicherzustellen, dass alle Systeme wie vorgeschrieben funktionieren. Während sich DORA in erster Linie auf die digitale Ausfallsicherheit konzentriert, ist die physische Infrastruktur eng mit den digitalen Ressourcen verbunden. Eine robuste und zuverlässige PIAM-Plattform hilft dabei, diese Verbindung zu sichern, bietet höchste Verschlüsselungsstandards, unterstützt die Nachvollziehbarkeit und verbessert die gesamte betriebliche Ausfallsicherheit.



Ein sicheres Contractor Management innerhalb einer PIAM-Plattform unterstützt Organisationen bei der Einhaltung der DORA-Anforderungen

Meldung von IKT-bezogenen Vorfällen

DORA verlangt die sofortige Protokollierung aller IKT-bezogenen Vorfälle und deren Meldung an die Behörden. Eine intelligente PIAM-Plattform bietet umfassende Berichte mit dokumentierten Handlungsschritten, wodurch eine Berichterstattung ohne manuellen Aufwand automatisiert wird. Detaillierte Protokolle und Zutrittsaufzeichnungen werden bereitgestellt.

Austausch von Informationen über Cyber-Bedrohungen

Im Rahmen von DORA sind Finanzorganisationen dazu verpflichtet, Informationen über Cyber-Bedrohungen und -vorfälle mit Behörden und anderen Organisationen des Finanzsektors auszutauschen. Ziel ist die Verbesserung des Lagebilds sowie die Zusammenarbeit zur Erhöhung der Cybersicherheit.

Eine PIAM-Plattform unterstützt dabei, cyber-physische Konvergenz zu erreichen, d. h. physische und Cybersicherheitsmaßnahmen zum Schutz einer Organisation und ihrer Daten zu kombinieren. Ein sicheres Physical Identity and Access Management (PIAM) ist für den Schutz der IT-Infrastruktur unerlässlich. Darüber hinaus trägt die physische Zutrittskontrolle zum Schutz digitaler Ressourcen bei. Wenn ein Vorfall eintritt, können die Protokolle der PIAM-Plattform wichtige Erkenntnisse darüber liefern, wer physisch anwesend war und das System möglicherweise kompromittiert hat. Dank der automatisierten und umfassenden Berichtsmöglichkeiten einer intelligenten PIAM-Plattform können Informationen über Bedrohungen und Vorfälle mühelos mit anderen Finanzorganisationen ausgetauscht werden, um Sicherheitsmaßnahmen weiter zu verbessern.

Ganzheitliche Sicherheit – digital und physisch

Der Einsatz einer PIAM-Plattform steuert die physische Ebene, die zur Gewährleistung der digitalen Ausfallsicherheit laut DORA erforderlich ist. Dies trägt zur Verbesserung der operativen Resilienz von Finanzorganisationen bei: Die Sicherheit wird erhöht, das Risikomanagement unterstützt, und der Informationsaustausch über Bedrohungen und Vorfälle wird erleichtert. GIT

ID-ware Deutschland GmbH
www.id-ware.com