Datenblatt

DORA: Wie Specops Sie bei der Compliance unterstützt

DORA: Kurzübersicht

Was ist DORA? Der Digital Operational Resilience Act (Verordnung (EU) 2022/2554) ist ein verbindlicher EU-Rechtsrahmen zur Stärkung der Cybersicherheit und digitalen Resilienz im Finanzsektor.

Welche Bereiche deckt DORA ab? Der Schwerpunkt liegt auf dem IKT-Risikomanagement, der Identitäts- und Zugriffskontrolle, der Erkennung und Meldung von Vorfällen, der Prüfung der operativen Widerstandsfähigkeit, dem Risikomanagement bei Drittanbietern sowie dem Austausch von Informationen über Cyberbedrohungen.

Für wen gilt DORA? DORA gilt für Banken, Versicherungen, Wertpapierfirmen, Zahlungs- und E-Geld-Institute, Krypto-Asset-Dienstleister sowie kritische IKT-Drittdienstleister, die im EU-Finanzsektor tätig sind oder diesen unterstützen.

Ist DORA dasselbe wie NIS2? Nein, denn während die NIS2-Richtlinie branchenübergreifend für kritische Sektoren gilt, richtet sich DORA speziell an Finanzdienstleister und hat für die betroffenen Finanzunternehmen Vorrang vor NIS2. Beide Regelwerke verfolgen das Ziel einer höheren Cyberresilienz, DORA stellt jedoch strengere und detailliertere Anforderungen an den Finanzsektor.

Gibt es Sanktionen bei Nichteinhaltung? Ja. Finanzunternehmen können mit Geldbußen von bis zu 2 % des weltweiten Jahresumsatzes oder bis zu 1 % des durchschnittlichen täglichen weltweiten Umsatzes belegt werden. Verantwortliche Personen können mit Strafen von bis zu 1 Million Euro belangt werden.

Warum Specops für DORA?

DORA-Anforderungen	Wie Specops die Compliance unterstützt
Passworttransparenz ***DORA-Artikel 8: Identifizierung*** Finanzunternehmen müssen IKT-Risiken, einschließlich Schwachstellen im Zusammenhang mit Benutzeranmeldedaten und Zugriffsrechten, innerhalb ihrer gesamten IT-Umgebung identifizieren und bewerten.	**Specops Password Auditor** (kostenloses Tool) Es führt einen schreibgeschützten Scan Ihrer Active-Directory-Umgebung durch und identifiziert kompromittierte, leere, veraltete sowie niemals ablaufende Passwörter. Zudem erstellt es exportierbare Berichte für Compliance- und Audit-Zwecke.
Kompromittierte Zugangsdaten ***DORA Artikel 9(4)(d): Schutz und Prävention*** Finanzunternehmen müssen Richtlinien und Verfahren für starke Authentifizierungsmechanismen implementieren, einschließlich Kontrollen, die sicherstellen, dass die für den Zugriff auf IKT-Systeme verwendete Zugangsdaten weder kompromittiert noch schwach sind.	**Specops Password Policy mit Breached Password Protection** Die meisten Lösungen verhindern die Verwendung kompromittierter Passwörter nur beim Passwortwechsel oder -zurücksetzen. Specops hingegen überprüft Ihr Active Directory kontinuierlich und schützt so vor der Verwendung von Passwörtern aus unserer stetig wachsenden Datenbank mit mehr als 6 Milliarden kompromittierten Passwörtern.

DORA-Anforderungen	Wie Specops die Compliance unterstützt
Starke MFA ***DORA Artikel 9(4)(d): Schutz und Prävention*** Finanzunternehmen müssen Richtlinien und Verfahren für starke Authentifizierungsmechanismen implementieren, insbesondere für den Remote-Zugriff auf Netzwerke, privilegierte Zugriffe sowie den Zugriff auf Systeme, die kritische Geschäftsfunktionen unterstützen.	**Specops Secure Access** Ergänzt Windows-Anmeldungen, RDP- und VPN-Zugriffe um phishing-resistente MFA. Unterstützt Single Sign-on (SSO) für SaaS-Anwendungen über OIDC und SAML und integriert sich nahtlos in SIEM-, SOC- und Analytics-Plattformen.
Service-Desk-Überprüfung ***DORA Artikel 9(4)(c) und 9(4)(d): Schutz und Prävention*** Zugriffskontrollen und starke Authentifizierung müssen sich auch auf operative Prozesse erstrecken. Dazu gehört insbesondere der Service Desk, bei dem Fehler bei der Identitätsprüfung ein unmittelbares IKT-Risiko darstellen.	**Specops Secure Service Desk** Service-Desk-Mitarbeiter verifizieren die Identität der Anrufer mittels MFA (über 20 Verifizierungsmethoden), bevor Kontoaktionen durchgeführt werden. Jede Interaktion wird vollständig protokolliert und revisionssicher dokumentiert. Integration mit ITSM-Lösungen sowie SIEM-, SOC- und Analytics-Plattformen.
Überprüfung mit hohem Sicherheitsniveau ***DORA Artikel 9(4)(c) und 9(4)(d): Schutz und Prävention*** Die Anforderungen an eine starke Authentifizierung gelten auch für die Identitätsprüfung beim Zugriff auf IKT-Systeme, insbesondere bei risikobehafteten Vorgängen wie der Wiederherstellung von Konten oder privilegierten Zugriffsrechten.	**Specops Verified ID** Es werden amtliche Ausweisdokumente geprüft und eine biometrische Lebenderkennung (Liveness Check) durchgeführt, um Identitätsverifizierungen mit höchstem Vertrauensniveau zu ermöglichen.
Sichere Passwortzurücksetzungen ***DORA Artikel 9(4)(c) & 9(4)(d): Schutz und Prävention*** Zugriffskontrollen und Anforderungen an eine starke Authentifizierung müssen über den gesamten Identitätslebenszyklus hinweg angewendet werden. Dies gilt insbesondere für Passwortzurücksetzungen, die nicht weniger sicher sein dürfen als die primäre Authentifizierung.	**Specops uReset** Self-Service-Passwortzurücksetzung mit MFA-Absicherung. Benutzer können ihre lokalen, zwischengespeicherten Anmeldedaten sicher aktualisieren – unabhängig von Standort, Gerät oder Browser und sowohl innerhalb als auch außerhalb des VPNs. Integration mit SIEM-, SOC- und Analytics-Plattformen.

Vereinbaren Sie einen Beratungstermin mit Ihrem Specops-Team, um gemeinsam die nächsten Schritte zu besprechen

Jetzt Termin vereinbaren