yubico

E-BOOK ZUR DORA-KONFORMITÄT

Sorgen Sie mit dem YubiKey für DORA-Konformität

Europäische Finanzaufsichtsbehörden (englisch: European Supervisory Authorities, ESA)/leitende Aufsichtsorgane:

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

In Kraft getreten am 16. Januar 2023 | Aufsicht gemäß DORA begann am 17. Januar 2025

Ungefähre Zahl der Betroffenen:

Strafen bei Nichteinhaltung können verhängt werden gegen:

- Finanzinstitute
- Verantwortliche Einzelpersonen
- Vorstandsmitglieder
- Kritische Drittanbieter von Dienstleistungen (CTPPs)

Fast ein Fünftel aller globalen Cyberangriffe in den letzten 20 Jahren waren auf den Finanzsektor gerichtet.[3] Obwohl die durchschnittlichen Kosten eines Cyberangriffs (0,45 Millionen Euro) oder einer Datenschutzverletzung (5,53 Millionen Euro) meist nicht zur Insolvenz führen, ist das Risiko extremer Verluste gestiegen (bis zu 2,27 Milliarden Euro), wodurch die Zahlungsfähigkeit der betroffenen Unternehmen sowie die globale finanzielle Stabilität bedroht werden.[4]

Technologische Abhängigkeiten, wie die gemeinsame Nutzung von Drittanbieter-Informations- und Kommunikationstechnologien (IKT), erhöhen das Risiko systemischer Auswirkungen über Unternehmen, Sektoren und Ländergrenzen hinweg. So können beispielsweise 8 % der weltweiten Cybervorfälle im Finanzsektor im Jahr 2023 auf den Zero-Day-Angriff MOVEit zurückgeführt werden, was die weitreichenden Auswirkungen von Drittanbieter- (Lieferketten-) Angriffen verdeutlicht.[5]

Was ist DORA?

Die EU-Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA, Digital Operational Resilience Act)[6] zielt darauf ab, das IKT-Risiko innerhalb des europäischen Finanzsektors und seiner zugehörigen Lieferketten zu mindern, sodass er Cybervorfällen standhalten, entsprechend reagieren und sich davon erholen kann. Damit ist finanzielle Stabilität auch bei schwerwiegenden Betriebsunterbrechungen gewährleistet.

DORA legt einen umfassenden Rahmen für das Management interner und externer Risiken fest. Die Verordnung wurde entwickelt, um die regulatorische Komplexität zu reduzieren und gleichzeitig die Regeln für betriebliche Resilienz und Risikomanagement, die möglicherweise bereits in früheren EU-Gesetzen erschienen sind, zu harmonisieren und zu verbessern.

Wer muss DORA einhalten?

DORA soll für fast alle Finanzinstitute und die von ihnen beauftragten Drittanbietern von IKT-Diensten (TPPs, Third-Party Providers) einschließlich Cloud-Dienstanbietern, Datenverarbeitern und anderer IKT-Dienste gelten. Die davon betroffenen IKT-Drittanbieter können sich überall auf der Welt befinden, nicht nur an Standorten innerhalb der Europäischen Union.

Seit Jahresbeginn 2025 werden einige IKT-Drittanbieter als kritisch (CTPPs, Critical Third-Party Providers) eingestuft. Damit sind jene IKT-Drittanbieter gemeint, die kritische oder wichtige Funktionen mehrerer Finanzinstitute unterstützen und deren Ausfall einen systemischen Einfluss auf die Stabilität, Kontinuität oder Qualität der Finanzdienstleistungen haben könnte.[7] Die Europäischen Aufsichtsbehörden üben die direkte Aufsicht über die CTPPs aus, wobei die CTPPs eine Tochtergesellschaft innerhalb der EU gründen und die Kosten der Beaufsichtigung proportional zum Umsatz tragen müssen.

Finanzinstitute[8]

Kreditinstitute	Zahlungsinstitute	Dienstleister für Kontoinformationen	Elektronische Geldinstitute	Wertpapierfirmen
Dienstleister für Kryptoanlagen	Wertpapiersammelbanken	Zentrale Gegenparteien	Handelsplätze	Handelsregister
Verwalter alternativer Investmentfonds	Verwaltungsgesellschaften	Dienstleister für Datenberichte	Versicherungs- und Rückversicherungsunternehmen	Versicherungsvermittler, Rückversicherungs- und Zusatzversicherungsvermittler
Einrichtungen für die betriebliche Altersversorgung	Kreditrating-agenturen	Administratoren von kritischen Benchmarks	Crowdfunding-Dienstleister	Verbriefungsregister

Beispiele für IKT-Drittanbieter[9]

Direkt oder indirekt (Subunternehmer)

Software- und Anwendungs-dienste (Standardsoftware oder kundenspezifische Entwicklung)	Netzwerkinfrastruktur-dienste (außer Telekommunikations-dienste)
Rechenzentren	IKT-Beratung und verwaltete IKT-Dienstleistungen
Informationssicherheits- und Cybersicherheitsdienste	Cloud-Computing-Anbieter
Datenanalyse- und Datendienste (einschließlich Dateneingabe, Datenspeicherung und Datenverarbeitung)	Sonstige[10]

Welche Strafe droht bei Missachtung?

Für CTPPs, die wegen Nichteinhaltung der Vorschriften benachrichtigt werden, räumt DORA dem Aufsichtsorgan die Befugnis ein, die Einhaltung der Vorschriften mit einem täglichen Zwangsgeld (für maximal sechs Monate) von bis zu 1 % des täglichen durchschnittlichen weltweiten Umsatzes aus dem vorangegangenen Geschäftsjahr zu erzwingen.

Für Finanzunternehmen, die gegen die Vorschriften verstoßen, werden die zuständigen Behörden in jedem Mitgliedstaat „verhältnismäßige und abschreckende“ verwaltungs- und/oder strafrechtliche Sanktionen festlegen und durchsetzen. Diese Sanktionen können gegen ein Finanzunternehmen, die für den Verstoß verantwortlichen juristischen Personen und/oder gegen Mitglieder der Geschäftsführung verhängt werden.

DORA-Anforderungen

DORA legt Anforderungen für Finanzunternehmen fest, um die Sicherheit von Netzwerk- und Informationssystemen zu gewährleisten und deren Resilienz zu fördern. Dies geschieht durch die Festlegung von Anforderungen für diese fünf Säulen:

IKT-Risikomanagement	**Meldung von IKT-Vorfällen**	**Prüfung der digitalen betrieblichen Resilienz**	**Austausch von Wissen und Informationen**	**IKT-Drittanbieterrisiken TPP | CTPP**
Strategien, Richtlinien und Hilfsmittel zum Schutz von Daten und IKT-Vermögenswerten	Management und Meldung von IKT-Vorfällen	Regelmäßige Tests je nach Größe und Bedeutung des Unternehmens	Formalisierte Vereinbarungen über den Austausch von Informationen	Minderung des Drittanbieterrisikos durch vertragliche Regelungen und Überwachung

Auch wenn sie von ihren IKT-Dienstleistern über vertragliche Bestimmungen ähnliche DORA-konforme Anstrengungen zum Risikomanagement einfordern, tragen letztendlich die Finanzunternehmen selbst die Verantwortung für die Genehmigung, Verwaltung und Kontrolle der Nutzung von IKT-Diensten. Diese Maßnahme zielt darauf ab, hinsichtlich der IKT-Drittanbieterrisiken die „Rechenschaftspflicht zu stärken“.[11]

DORA-Anforderungen an die Authentifizierung

Im Rahmen des vorgeschriebenen Risikomanagementrahmens wird den betroffenen Unternehmen die Festlegung von „Konzepten und Protokollen für starke Authentifizierungsmechanismen“ abverlangt, die auf „einschlägigen Normen basieren“ und „Schutzmaßnahmen für kryptografische Schlüssel“ begünstigen.[12]

Die technischen Regulierungsstandards zur Unterstützung von DORA wurden im Einklang mit internationalen Normen für das IKT-Risikomanagement entwickelt, darunter die Richtlinie zur Netz- und Informationssicherheit (NIS), nunmehr NIS 2, und das NIST Cybersecurity Framework.[13] In diesen Standards wird außerdem klargestellt, dass die Authentifizierungsmethoden dem Risiko angemessen sein und sich an Best Practices für Fernzugriff, privilegierten Zugriff und Zugriff auf kritische oder wichtige Funktionen orientieren müssen.[14]

So erkennen Sie Authentifizierungsrisiken

Um die risikobasierten Authentifizierungsanforderungen von DORA zu erfüllen, müssen die betroffenen Unternehmen einen Authentifikator auf der Grundlage seiner Stärke auswählen und sich dabei nach dem globalen NIST-Standard[15] oder eIDAS richten.[16] In diesen Richtlinien wird berücksichtigt, dass **nicht alle Arten der MFA gleich sind**, repräsentiert durch Authentifizierungsstufen bzw. Vertrauensniveaus (AALs/LoAs).

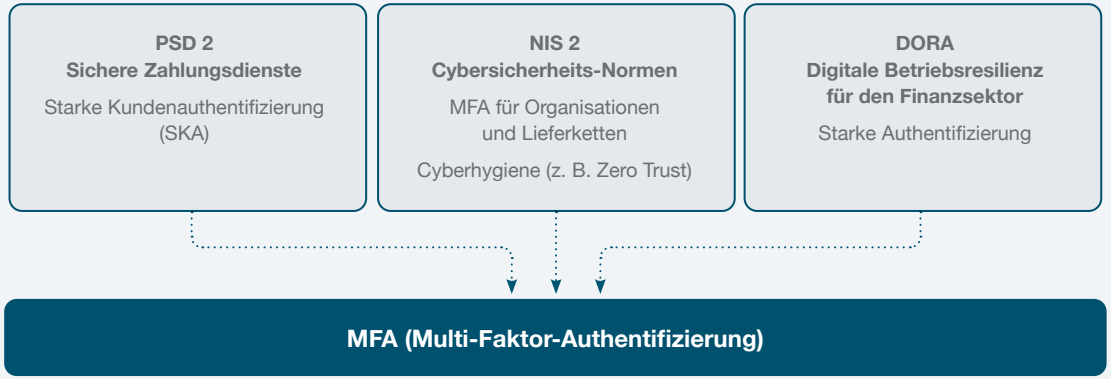
Zwar ist jede Form der MFA besser als nur ein Passwort (AAL1/LoA Low), doch ältere Formen der MFA (AAL2/LoA Substantial) wie SMS, Authentifizierung per Mobilgerät und Einmalkenncodes (OTP) verzeichnen eine Angriffsdurchdringungsquote von 10 bis 24 %[17], während ein Phishing-resistenter, hardwarebasierter Authentifikator (AAL3/LoA High) mehr Sicherheit bietet und das Risiko einer Kompromittierung des Kontos verringert.[18]

AAL1	AAL2	AAL3
[1] **Ein-Faktor-Authentifizierung** [2] z. B. Benutzername und Passwort	**Zweistufige Authentifizierung** z. B. 2FA, synchronisierte Passkeys, gerätegebundene Passkeys auf Allzweckgeräten	**Hardwarebasierte Multi-Faktor-Authentifizierung** z. B. gerätegebundene Passkeys auf Hardware-Sicherheitsschlüsseln
		
• Geringes Maß an zuverlässiger Sicherheit • Sehr anfällig für Phishing • Gefährdet Unternehmen	• Phishing-resistente 2FA/MFA • Sicherer als ein Passwort, aber anfällig für Angriffe • Schneller einsatzbereit für Unternehmen, aber Lücken bei der betrieblichen Effizienz und Audit-/Compliance-Anforderungen	• Phishing-resistente MFA • Höchste Sicherheit und höchste Zuverlässigkeit • Erfüllt die Anforderungen an Unternehmenssicherheit, Betriebseffizienz und Audit/Compliance • Unterstützt FIDO und Smart Card/PIV • Validiert durch FIPS 140-2

Mehr erfahren Sie in unserem NIS-2-Leitfaden
Leitfaden lesen

Wie wirkt sich NIS 2 auf DORA aus?

DORA ist Teil eines Dreiklangs von Vorschriften zur Stärkung des digitalen Schutzes und zur Sicherung kritischer digitaler Infrastrukturen, angefangen bei den Verbrauchern und der Zahlungsdienstrichtlinie (PSD), nunmehr PSD 2, bis hin zu Organisationen und ihren Lieferketten mit DORA und NIS 2. Alle drei dienen dem Risikomanagement und schreiben eine starke Authentifizierung vor. Da DORA auf NIS 2 abgestimmt wurde, sollten Finanzorganisationen – die als kritische Unternehmen gelten – die umfassenderen Anforderungen von NIS 2 einhalten und dabei eine starke MFA (AAL3/LoA High) sowie Zero-Trust-Prinzipien einführen.



Entscheidend ist, dass die DORA-Anforderungen in Bereichen mit Überschneidungen Vorrang vor den NIS-2-Anforderungen haben, während die NIS-2-Anforderungen in anderen Bereichen weiterhin gelten.[19] Die spezifischeren MFA-Anforderungen von NIS 2 zusammen mit Cyberhygiene-Praktiken wie Zero Trust bedeuten also, dass betroffene Unternehmen auf die ausschließliche Verwendung von Phishing-resistenter MFA auf AAL2 oder höher hinarbeiten sollten.

Schnellere DORA-Konformität mit dem YubiKey

Der YubiKey ist ein Hardware-Sicherheitsschlüssel, der entwickelt wurde, um Organisationen mit Phishing-resistenten Benutzern zu schaffen. Als Hardware Root of Trust bietet der YubiKey Phishing-resistente Authentifizierung mit höchster Sicherheit. Der YubiKey wird in Schweden von Yubico, einem schwedischen Unternehmen, hergestellt und programmiert und ist nach FIPS und FIDO zertifiziert.

Der YubiKey unterstützt sowohl Smart Card/PIV als auch FIDO2-Protokolle sowie FIDO U2F, OTP/TOTP und OpenPGP. Er ist damit Ihr idealer Partner für Ihre Cybersicherheitsreise und eignet sich für eine Vielzahl von Geschäftsszenarien.

- Privilegierter Zugriff
- Umgebungen mit Einschränkungen für Mobilgeräte
- Gemeinsam genutzte Workstations
- Remote-Beschäftigte
- Büroangestellte
- Zugriff von Dritten
- Endkunden

Sorgen Sie für die Einhaltung der DORA-Anforderungen, indem Sie noch heute den YubiKey einführen. Um eine hohe Sicherheit in Ihrer Lieferkette der IKT-Drittanbieter zu gewährleisten, müssen alle Dienstleister eine Phishing-resistente MFA für ihre eigenen Benutzer und Systeme implementieren.

Kontaktieren Sie uns
yubi.co/kontakt

Mehr erfahren
yubi.co/finance

Quellen

[1] PwC, DORA and its impact on UK financial entities and ICT service providers, (Zugriff am 7. Oktober 2024)

[2] Joint Committee of the European Supervisory Authorities, ESAs Report on the landscape of ICT third-party providers in the EU, (18. September 2023)

[3] The International Monetary Fund, Global Financial Stability Report, (April 2024)

[4] Ibid; Verizon, 2024 Data Breach Investigations Report, (1. Mai 2024)

[5] Verizon, 2024 Data Breach Investigations Report, (1. Mai 2024)

[6] Amtsblatt der Europäischen Union, VERORDNUNG (EU) 2022/2554, (14. Dezember 2022)

[7] Gemeinsamer Ausschuss der europäischen Aufsichtsbehörden, JS SC DOR-23-54, (26. Mai 2023)

[8] Amtsblatt der Europäischen Union, VERORDNUNG (EU) 2022/2554, (14. Dezember 2022)

[9] Gemeinsamer Ausschuss der europäischen Aufsichtsbehörden, Bericht der Europäischen Aufsichtsbehörden über die Landschaft von IKT-Drittunternehmen in der EU, (18. September 2023)

[10] DORA definiert sonstige IKT-Dienste als: „digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste“. Amtsblatt der Europäischen Union, VERORDNUNG (EU) 2022/2554, (14. Dezember 2022)

[11] Gemeinsamer Ausschuss der europäischen Aufsichtsbehörden, JC 2023 84, (17. Januar 2024)

[12] Amtsblatt der Europäischen Union, VERORDNUNG (EU) 2022/2554, (14. Dezember 2022)

[13] Gemeinsamer Ausschuss der europäischen Aufsichtsbehörden, JC 2023 86, (17. Januar 2024)

[14] Ibid.

[15] NIST, NIST SP 800-63-4 Digital Identity Guidelines, (Dezember 2022)

[16] Europäische Kommission, eIDAS Levels of Assurance (LoA), (2014)

[17] Kurt Thomas und Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (17. Mai 2019)

[18] Amt für Veröffentlichungen der Europäischen Union, Durchführungsverordnung der Kommission (EU) 2015/1502, (September 2015)

[19] Amtsblatt der Europäischen Union, Leitlinien der Kommission zur Anwendung von Artikel 4 Absätze 1 und 2 der Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie), (18. September 2023)

yubico

Über Yubico

Yubico (Nasdaq Stockholm: YUBICO), Erfinder des YubiKey, bietet den Goldstandard für eine Phishing-resistente Multi-Faktor-Authentifizierung (MFA), die Kontoübernahmen vorbeugt und sichere Anmeldungen einfach und für alle möglich macht. Seit seiner Gründung im Jahr 2007 hat das Unternehmen federführend an der Festlegung globaler Standards für den sicheren Zugriff auf Computer, Mobilgeräte, Server, Browser und Internetkonten mitgewirkt. Yubico hat wesentlich zur Entwicklung der offenen Authentifizierungsstandards FIDO2, WebAuthn und FIDO Universal 2nd Factor (U2F) beigetragen. Das Unternehmen ist ein Pionier bei der Bereitstellung einer hardwarebasierten passwortlosen Authentifizierung in Form von hochsicheren Passkeys für Kunden in über 160 Ländern.

Die Lösungen von Yubico ermöglichen eine passwortlose Anmeldung mit der sichersten Form der Passkey-Technologie. YubiKeys funktionieren out-of-the-box mit Hunderten von Verbraucher- und Unternehmensanwendungen und -diensten und vereinen hohe Sicherheit mit Schnelligkeit und Benutzerfreundlichkeit.

Im Rahmen seiner Mission, das Internet für alle sicherer zu machen, spendet Yubico über die gemeinnützige Initiative Secure it Forward YubiKeys an Organisationen, die besonders gefährdete Personen unterstützen. Yubico hat seinen Hauptsitz in Stockholm und Santa Clara, Kalifornien. Für weitere Informationen über Yubico besuchen Sie uns bitte unter www.yubico.com