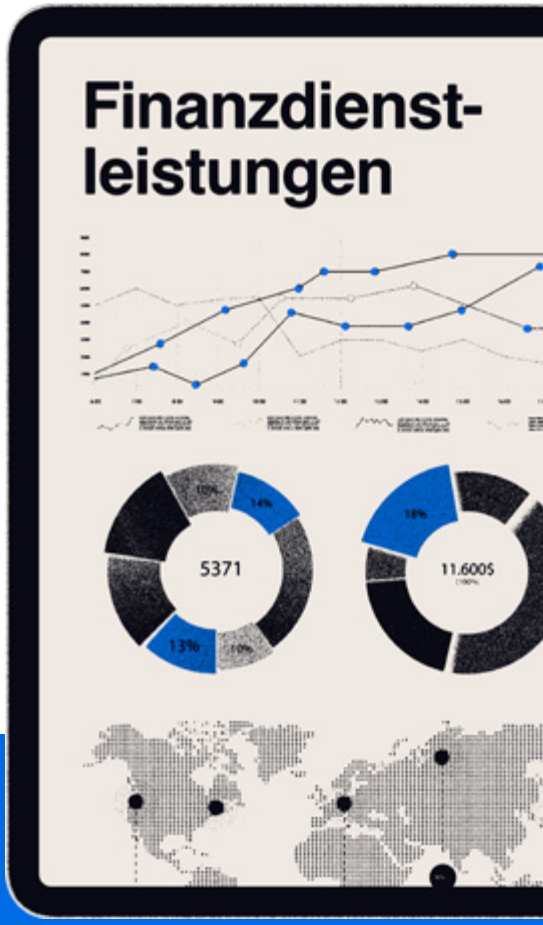
DER DIGITAL OPERATIONAL RESILIENCE ACT (DORA) UND RUBRIK

rubrik

So kann Rubrik der Finanzbranche dabei helfen, die neuesten Standards der Europäischen Union für Cyber-Resilienz zu erfüllen

Der Digital Operational Resilience Act (DORA) ist eine Verordnung der Europäischen Union, die darauf abzielt, die Cyber-Resilienz von Finanzunternehmen zu verbessern. Das Gesetz, das am 17. Januar 2025 in allen EU-Mitgliedstaaten in Kraft treten wird, verpflichtet Finanzunternehmen, ihre Resilienz gegen Cyberangriffe und andere Betriebsstörungen zu verbessern, indem sie die herkömmliche, auf Erkennung und Abwehr basierende Ansätze durch stärker auf Resilienz und Wiederherstellung ausgerichtete Ansätze ersetzen.

Die der Verordnung unterliegenden Finanzinstitute – darunter Banken, Versicherungsunternehmen, Investmentfirmen, Kryptowährungsbörsen und Handelsplattformen – sowie andere Organisationen, die für diese Institute wichtige Dienstleistungen erbringen, können mit Geldbußen von bis zu 2 % ihres gesamten weltweiten Jahresumsatzes belegt werden, wenn sie die DORA-Verordnung nicht einhalten.(1) Die Höhe der Geldbuße hängt von der Schwere des Verstoßes und der Kooperation des Finanzunternehmens mit den Behörden ab.



Stärken Sie Ihre betriebliche Ausfallsicherheit, um auf die DORA-Verordnung vorbereitet zu sein

Finanzunternehmen sollten die folgenden Fragen beantworten, um ihre betriebliche Ausfallsicherheit zu stärken und die DORA-Vorschriften umzusetzen:

1. Wie groß ist Ihr Vertrauen in Bezug auf die betriebliche Ausfallsicherheit Ihres Unternehmens?
2. Vorfälle sind unvermeidbar. Wie genau sieht der Reaktions- und Wiederherstellungsplan Ihres Unternehmens aus?
3. Wie schnell können Sie Ihre IBS (Important Business Services, wichtige Geschäftsservices) nach einem großen Ausfall wiederherstellen?
4. Wie häufig führen Sie Risikobewertungen durch? Nehmen Sie kontinuierliche Verbesserungen bei Ihren IBS vor?
5. Sind Sie in der Lage, größere Vorfälle der richtigen Behörde zu melden?

SO KANN RUBRIK SIE BEI DER UMSETZUNG VON DORA UNTERSTÜTZEN

Die DORA-Verordnung basiert auf 5 Säulen

Risikomanagement im Bereich der Informations- und Kommunikationstechnologie (IKT), Berichterstellung über IKT-bezogene Vorfälle, betriebliche Resilienz und Tests, Management des Risikos durch Drittparteien und Informationsaustausch. Rubrik kann Unternehmen dabei helfen, sich an die folgenden Kernsäulen von DORA anzupassen:

1

IKT-Risikomanagement

Unternehmen, die unter diese Verordnung fallen, müssen über einen internen Governance- und Kontrollrahmen für ein wirksames IKT-Risikomanagement verfügen, von der Identifizierung kritischer Ressourcen bis hin zur Reaktion auf Cyberrisiken und Wiederherstellung.

So kann Rubrik helfen: Die Plattform von Rubrik ist als einheitliches System konzipiert, um einen einzigen Kontrollpunkt für die Verwaltung und den Schutz von Daten unabhängig davon zu bieten, wo sie gespeichert sind.

2

Meldung von Vorfällen im Zusammenhang mit IKT

Unternehmen, die unter die Verordnung fallen, müssen Systeme zum Erkennen, Handhaben und Melden von IKT-bezogenen Vorfällen festlegen.

So kann Rubrik helfen: Unternehmen können die globale Transparenz und das Richtlinienmanagement, den API-first-Ansatz und die umfangreichen Integrations- und Protokollierungsfunktionen von Rubrik nutzen, um die Klassifizierung und Meldung von IKT-bezogenen Vorfällen zu unterstützen.

3

Betriebliche Resilienz und Tests

Unter die Verordnung fallende Unternehmen sind verpflichtet, Tests zur digitalen betrieblichen Resilienz durchzuführen.

So kann Rubrik helfen: Mit der Plattform von Rubrik können Unternehmen als Teil eines breiteren Ökosystems Resilienz in Disaster-Recovery-Szenarien erreichen, indem sie branchenführende Backup-, Wiederherstellungs- und wichtige Data-at-Rest-Sicherheitsfunktionen integrieren, um die aktive Erkennung von Datenbedrohungen und Audit-Fehlern zu unterstützen. Unternehmen können auch die Richtlinienautomatisierung nutzen, um die betriebliche Resilienz von Funktionen ihrer Backup-Daten zu testen und sicherzustellen, die Bestandteil des IKT-Risikomanagement-Frameworks sind.

4

Management des Risikos durch Drittparteien:

Unternehmen, die unter die Verordnung fallen, müssen ihr IKT-Drittparteirisiko als Teil ihrer gesamten IKT-Risikomanagement-strategie aktiv managen.

So kann Rubrik helfen: Um einen effektiveren Ansatz für Management und Bewertung des Risikos durch Drittparteien zu unterstützen, können Kunden die in der Rubrik-Plattform gespeicherten Daten untersuchen, um Risiken im Zusammenhang mit der Erkennung sensibler Daten und der Analyse von Datenklassifizierungen zu identifizieren. Außerdem können Unternehmen Rubriks Funktionen zur Bedrohungssuche nutzen, um Risiken in Bezug auf IOCs und Ransomware-Malware zu identifizieren und alle Funde sofort dem breiteren Ökosystem der Risikomanagement-Plattform zu melden, um ein besseres Verständnis und eine bessere Abdeckung als Teil einer umfassenden IKT-Risikomanagement-Strategie zu erreichen.

5

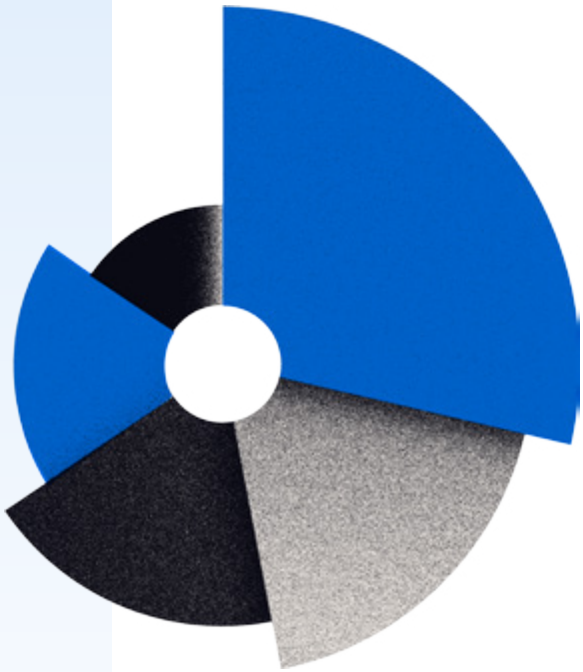
Informationsaustausch

Unternehmen werden ermuntert, sich am Austausch von Informationen und Erkenntnissen über Cyber-Bedrohungen innerhalb vertrauenswürdiger Communitys aus Finanzunternehmen zu beteiligen, um die digitale Resilienz der Branche zu verbessern.

So kann Rubrik helfen: Durch ein einheitliches Transparenz-Framework und ein umfassendes API-first-Design kann Rubrik dazu beitragen, die Anforderung zu erfüllen, von der Plattform erkannte und überwachte Bedrohungsinformationen an Tools und Berichterstellungssysteme von Drittanbietern weiterzugeben, sodass Unternehmen Daten zu Bedrohungsinformationen (in Bezug auf die Erkennung von Ransomware, IOC-Bedrohungssuche und Bedrohungsüberwachung) mit anderen vertrauenswürdigen Finanzinstituten austauschen können.

WEITERE INFOS ÜBER RUBRIK

Rubrik vereinfacht die Bereitstellung betrieblicher Resilienz durch eine einzige Plattform für Datensicherheit im Unternehmen, in der Cloud und in SaaS-Anwendungen. Unsere Plattform automatisiert die Verwaltung von Datenrichtlinien und die Durchsetzung der Datensicherheit über den gesamten Lebenszyklus der Daten. Wir unterstützen Unternehmen dabei, die Datenintegrität zu wahren, für eine Datenverfügbarkeit zu sorgen, kontinuierlich Datenrisiken und -bedrohungen zu überwachen und Unternehmensdaten wiederherzustellen, wenn die Infrastruktur angegriffen wird. Im Falle von Katastrophen, Sicherheitsverletzungen und Ausfällen auf Unternehmensebene setzen Finanzdienstleister vertrauensvoll auf Rubrik, um betriebliche Ausfallsicherheit und Geschäftskontinuität umfassend sicherzustellen.



Unternehmen in Europa müssen mit Konsequenzen rechnen, wenn sie sich nicht an die neuesten Cybersicherheitsregeln und -verordnungen halten. Von sektorspezifischen Verordnungen bis hin zu europaweit geltenden Gesetzen müssen Unternehmen einen proaktiven Plan für ihre Datensicherheitsbereitschaft entwickeln, um diese Verordnungen zu erfüllen.

Kontaktieren Sie uns, um mehr darüber zu erfahren, wie Rubrik Organisationen dabei helfen kann, sich an den Kernsäulen von DORA auszurichten, und wie wir Finanzunternehmen dabei unterstützen können, ihre Datensicherheitsbereitschaft proaktiv zu verbessern, um sich an Datenvorschriften anzupassen.

Unser Kunden-Lookbook lesen

Data Security Talks auf Abruf ansehen

Rubrik für Finanzdienst-leistungen