eBOOK

DORA erfolgreich umsetzen: Strategien zur digitalen operationalen Resilienz

Wie Commvault-Lösungen Sie bei der Erfüllung regulatorischer Anforderungen unterstützen können.

Commvault®

CONTENTS

Overview

Ab dem 17. Januar 2025 müssen Finanzunternehmen in der Europäischen Union die Vorgaben des Digital Operational Resilience Act erfüllen, mit dem die Cyber-Resilienz im gesamten Sektor verbessert werden soll. Er betrifft Banken, Versicherungsgesellschaften und Drittdienstleister aus dem Bereich der Informations- und Kommunikationstechnologien (IKT)..

Glücklicherweise bietet Commvault Lösungen an, die Ihr Unternehmen bei der Verbesserung Ihrer Compliance-Maßnahmen unterstützen. Sie umfassen:

- Die Identifizierung kritischer Informationsbestände zur Risikominderung und Minimierung der Auswirkungen von Datenverlusten.
- Ein in das bestehende Sicherheitssystem integriertes Frühwarnsystem für verdächtige Aktivitäten.
- Eine Air-Gap-gesicherte Cyber Resilience Recovery-Plattform mit Zero Trust für alle Workloads.
- Reduzierte Komplexität und Kosten für eine saubere Wiederherstellung sowie Recovery Tests.
- Workload-, Cloud- und Hypervisor-übergreifende Portabilität, um Workloads und Daten zwischen Clouds oder Rechenzentren zu verschieben.

Es ist für alle Beteiligten essentiell, die zentralen Bestimmungen sowie ihre Auswirkungen auf das Finanzökosystem, zu kennen. Sehen wir uns die fünf wichtigsten Säulen von DORA an und wie die Lösungen von Commvault Ihnen dabei helfen können, diese einzuhalten.

01 Anforderungen an das Risikomanagement

In Kapitel II (Artikel 5–16) legt DORA die Überwachungsaktivitäten und andere Sicherheitsverfahren und -strategien fest, die Finanzunternehmen einrichten und aufrechterhalten sollten, um ein angemessenes IKT-Risikomanagement zu gewährleisten. Diese Maßnahmen sollten den gesamten Lebenszyklus der Datenbestände und IKT-Systeme abdecken, von der Entwicklung und Einführung bis hin zur Wartung und Außerbetriebnahme. Es wird erwartet, dass Finanzunternehmen ihre Strategien zum Risikomanagement regelmäßig überprüfen und aktualisieren und diese an neue und aufkommende Bedrohungen anpassen.

Das bedeutet, dass Sie:

- Ein klares Verständnis für Ihre Daten und deren Sensibilität sowie Ihre Ressourcen und die potenziellen Auswirkungen eines Vorfalls auf diese haben müssen.
- Die Transparenz innerhalb Ihres Netzwerks durch kontinuierliche Überwachung der Benutzeraktivität erhöhen müssen.
- Anhand detaillierter Auditprotokolle und Berichte Aktivitätsmuster der Benutzer analysieren und Risiken bewerten müssen.
- Anomalien im Benutzerverhalten erkennen und potenzielle Sicherheitsrisiken identifizieren müssen.
- Benutzerdefinierte Warnregeln in Übereinstimmung mit bestehenden Sicherheitsrichtlinien festlegen und den Erhalt von Echtzeitbenachrichtigungen einrichten müssen.

Commvault-Lösungen können diese Anforderungen durch die Erkennung, Klassifizierung und den Schutz vertraulicher Daten erfüllen, eine standardisierte Cyber-Recovery-Plattform aufbauen, frühzeitig vor Bedrohungen warnen, Angriffe mithilfe moderner Deception-Technologien umlenken und Anomalie-Erkennung für Incident-Response-Maßnahmen einsetzen.

Im Folgenden finden Sie einige spezifische Anforderungen der DORA-Verordnung sowie Informationen, wie Commvault-Lösungen Sie bei der Erfüllung unterstützen können.

Provision	Commvault Solution
Artikel 8 verpflichtet Unternehmen dazu, alle IKT-Funktionen zu ermitteln, zu klassifizieren und zu dokumentieren, kritische Systeme und Daten zu erfassen und Drittanbieter zu benennen.	Mit Commvault Cloud Risk Analysis bietet Commvault einzigartige Möglichkeiten zur Ermittlung und Klassifizierung von Daten. So verfügen IKT-Unternehmen über einen automatisierten Prozess, um die Dokumentation sensibler und kritischer Daten auf dem neuesten Stand zu halten und schnell handeln zu können. Threatwise ermöglicht die Asset-Erkennung sowie die Risikoverfolgung auf TTP-Ebene, wenn der Köder benutzt wird.
Artikel 9 sieht vor, dass Unternehmen IKT-Systeme angemessen schützen müssen, um sicherzustellen, dass diese sicher sind und nicht beschädigt werden können oder die Gefahr eines Datenverlusts besteht. Sie müssen Datenkopien isolieren, um zu verhindern, dass die Daten bei einem Cyberangriff verschlüsselt werden.	Commvault ermöglicht Unternehmen den Aufbau einer sicheren Zero Trust-Plattform zur Cyber-Recovery mit einem Sicherheitsstatus-Dashboard, MFA, MPA, PAM und RBAC mit granularen Sicherheitsfunktionen. Diese zentrale, integrierte Plattform bietet sichere, verschlüsselte und unveränderliche Backup-Kopien auf Basis marktführender Verschlüsselungsstandards.
Artikel 10 schreibt vor, dass Unternehmen in der Lage sein müssen, anomale Aktivitäten schn ell zu erkennen.	Commvault Cloud® Threat Scan und Threatwise ermöglichen es Unternehmen, Anomalien in ihrer Umgebung proaktiv zu erkennen, einschließlich bösartiger oder beschädigter Dateien, umfangreicher Datenänderungen oder Verhaltensweisen, die auf das Auskundschaften durch Angreifer hindeuten könnten. Warnmeldungen zu diesen Anomalien werden über die Commvault-Plattform oder durch Integration in vorhandene Sicherheits- und Reporting-Tools wie SIEM, SOAR sowie Ticketing-Systeme bereitgestellt.
Artikel 11 gibt Organisationen vor, über dokumentierte IKT-BC-Richtlinien einschließlich eines Response- und Recoveryprozesses zu verfügen, der auch getestet werden muss.	Commvault Cloud bietet flexible und automatisierte Wiederherstellungsprozesse, einschließlich der Möglichkeit zur Wiederherstellung in einem Cleanroom mithilfe einer Air-Gap-Kopie. Der automatisierte Cleanroom vereinfacht Recovery-Tests, die unkompliziert und kostengünstig durchgeführt werden können.
In Artikel 12 werden die Backup-Strategien und -Verfahren sowie Maßnahmen zur Business Continuity beschrieben. **Unternehmen sollten Ziele für die Wiederherstellungszeit in Übereinstimmung mit den Geschäftsanforderungen und der Wichtigkeit der betroffenen Systeme erstellen. Unternehmen müssen die Daten an einem anderen Ort wiederherstellen können. Und was Cyber-Recovery betrifft, müssen Unternehmen in der Lage sein, Daten in einem Cleanroom wiederherzustellen.**	Commvault bietet die Möglichkeit zur flexiblen Richtlinienverwaltung und unterstützt mehrere Speicherorte in Rechenzentren sowie bei privaten/öffentlichen Cloud-Anbietern. Verwaltet wird das Ganze über eine zentrale Plattform. Commvault Threat Scan überwacht Malware und sorgt für eine saubere Wiederherstellung. Zusätzlich stellt Commvault Cleanroom Recovery-Funktionen zur Verfügung, sodass Wiederherstellungstests automatisiert durchgeführt werden können.

Commvault®

02 Meldung von Vorfällen

Eines der zentralen Elemente von DORA ist die Verpflichtung für Finanzunternehmen, wichtige Cybervorfälle unverzüglich ihren jeweiligen Regulierungsbehörden zu melden. In Kapitel III (Artikel 17-23) heißt es, dass die betreffenden Unternehmen über die Mittel verfügen müssen, um IKT-bezogene Vorfälle schnell zu erkennen, zu verfolgen, zu klassifizieren und zu melden sowie Verantwortlichkeiten und Abhilfepläne für verschiedene Vorfallszenarien festzulegen.

Diese Bestimmung gewährleistet einen zeitnahen Informationsfluss zwischen Finanzinstituten und Finanzaufsichtsbehörden, was für die Bewältigung von Systemrisiken und die generelle Stärkung der Widerstandsfähigkeit im Finanzsektor von entscheidender Bedeutung ist. Die Richtlinie legt die Vorfallsarten, die gemeldet werden müssen, sowie die Meldefristen und die Details, die in den Berichten enthalten sein sollten, fest.

Unternehmen müssen:

- IKT-bezogene Vorfälle auf Basis frühzeitiger Warnungen bei verdächtigem Benutzerverhalten, unbefugtem Zugriff und Anomalien umgehend erkennen.
- Die Reaktion auf Vorfälle durch automatisierte Gegenmaßnahmen, wie z. B. das Blockieren von Benutzern und die Deaktivierung von Prozessen, beschleunigen.
- Für eine umfassende Protokollierung sorgen, um die Ursache, die Auswirkungen und den Umfang des Vorfalls zu untersuchen und ähnliche Fälle in Zukunft zu verhindern.
- Die Benutzeraktivitäten in einem manipulationssicheren Dateiformat aufzeichnen, um für forensische Untersuchungen solide Beweise für den Vorfall vorlegen zu können.
- Über Sicherheitsvorfälle informieren und die Einhaltung der Sicherheitsvorschriften gegenüber den zuständigen Behörden durch Vorlage gut strukturierter und informativer Berichte nachweisen.

Commvault unterstützt Unternehmen bei der Einhaltung von Vorschriften durch Frühwarnindikatoren mit Deception-Technologie, einen Cleanroom für forensische Analysen, Anomalie-Erkennung und Bedrohungs-Scans zur Unterstützung des Vorfallsmanagements sowie standardisiertes Reporting mit SIEM/SOAR-Integration.

Im Folgenden finden Sie einige spezifische Anforderungen der DORA-Verordnung sowie Informationen, wie Commvault-Lösungen Sie bei der Erfüllung unterstützen können.

Provision	Commvault Solution
In den Artikeln 17 - 23 werden die Anforderungen an ein IKT-Vorfallsmanagement sowie an die Harmonisierungs- und Reporting-Fähigkeiten eines Unternehmens beschrieben.	Commvault Cloud streamlines Incident Response and Threat Intelligence processes through extensive ecosystem integration capabilities. Integrations with SIEMs, XSOAR, and third-party vendors facilitate efficient correlation analysis and mitigations.
Die Artikel 17 - 23 schreiben vor, dass Unternehmen den Response-Prozess auf Vorfälle durch die Automatisierung von Gegenmaßnahmen beschleunigen müssen.	Commvault Cloud unterstützt Sicherheits-Teams durch die Bereitstellung von Frühwarnindikatoren und hilft dabei, die Anforderung zu erfüllen, innerhalb eines bestimmten Zeitrahmens auf wichtige Vorfälle zu reagieren, indem Cyber-Deception und Anomalie-Erkennung zum Einsatz kommen.
Gemäß den Artikeln 17 - 23 müssen Unternehmen die Behörden über Sicherheitsvorfälle informieren und die Einhaltung der Cybersecurity-Anforderungen nachweisen, indem sie übersichtliche und informative Berichte vorlegen.	Commvault Cloud liefert Berichte, die auf der Konfiguration und den von der Plattform gesammelten Daten basieren. Sie umfassen den Sicherheitsstatus der Plattform, Audit-Trails, den Workload-Schutz, die angewandten Richtlinien, die geschätzte Wiederherstellungszeit und andere Komponenten. Darüber hinaus können diese Daten verwendet werden, um externe Tools und Portale zu befüllen.

03 Testen der digitalen operationalen Resilienz

In Kapitel IV (Artikel 24-27) von DORA wird dargelegt, dass Finanzunternehmen ihre Bereitschaft zur Bewältigung von IKT-bezogenen Vorfällen mindestens einmal jährlich bewerten und testen müssen, um Lücken in der betrieblichen Resilienz zu erkennen und zu beseitigen. Dies umfasst eine Reihe von Testaktivitäten, wie z. B. Schwachstellen-bewertungen, Penetrationstests und szenariobasierte Tests. Diese Tests sollen nicht nur Schwachstellen in IKT-Systemen und -Prozessen identifizieren, sondern in erster Linie die Wirksamkeit der Präventions-, Erkennungs-, Reaktions- und Wiederherstellungs-maßnahmen des Unternehmens bewerten.

Finanzunternehmen müssen:

- Für IKT-Unternehmen geeignete Business Continuity-Pläne erstellen, pflegen und regelmäßig testen, insbesondere in Bezug auf kritische oder wichtige Funktionen, die ausgelagert oder durch vertragliche Vereinbarungen an IKT-Drittdienstleister vergeben werden.
- Die IKT-Business-Continuity-Pläne sowie die Response- und Recovery-Pläne bei IKT-Systemen, die alle Funktionen unterstützen, mindestens einmal jährlich testen.
- IKT-Systeme auf der Grundlage des DORA-Test-Frameworks regelmäßig testen, um die Widerstandsfähigkeit gegenüber Ausfällen zu bewerten.

Commvault kann Unternehmen dabei unterstützen, diese Bestimmungen mithilfe von Cleanroom Recovery zu erfüllen. Sie ermöglicht Recovery-Tests mit reduzierten TCO, verfügt über forensische Testkapazitäten und stellt dank der Reporting-Funktionen prüfbare Aufzeichnungen sowie Erfolgsnachweise bereit.

Im Folgenden finden Sie einige spezifische Anforderungen der DORA-Verordnung sowie Informationen, wie Commvault-Lösungen Sie bei der Erfüllung unterstützen können.

Provision	Commvault Solution
Die Artikel 24 - 27 enthalten Anforderungen für regelmäßige Überprüfungen der operationalen Resilienz, einschließlich Performance, Kompatibilität und Business Continuity.	Commvault Cloud bietet die einzigartige Möglichkeit, Cyber-Recovery-Tests mit einem Cleanroom in der Public Cloud oder On Premise zu orchestrieren. Dies umfasst eine Air-Gap-gesicherte Kopie der Daten und eine Recovery-Orchestrierung in einem sauberen Tenant. Cyber-Recovery-Tests können auch in einem Rechenzentrum mit einer isolierten Wiederherstellungsumgebung durchgeführt werden.

04 Management des Drittparteienrisikos

In Anbetracht der zunehmenden Abhängigkeit von IKT-Drittdienstleistern sind in Kapitel V (Artikel 28-44) von DORA die Regeln und Anforderungen aufgeführt, die Finanzunternehmen einhalten müssen, um die Sicherheit bei der Zusammenarbeit mit IKT-Dienstleistern zu gewährleisten und mit Drittparteirisiken angemessen umgehen zu können. Finanzunternehmen müssen sorgfältige Due Diligence-Prüfungen durchführen, bevor sie Vereinbarungen mit Dienstleistern abschließen.

Diese Unternehmen müssen

- Die Aktivitäten von Drittanbietern an den Endgeräten ihres Unternehmens überwachen, um die Einhaltung der festgelegten Richtlinien und Standards sicherzustellen.
- Granulare Zugriffsberechtigungen für Drittanbieter definieren, damit diese nur Zugriff auf die Ressourcen und Daten haben, die sie benötigen.
- Die Sicherheit von RDP-Verbindungen verbessern und unberechtigten Zugriff auf vertrauliche Daten oder andere potenziell schädliche Aktivitäten rasch erkennen.
- Benutzerdefinierte Live-Warnungen und Benachrichtigungen zu verdächtigem Verhalten und Sicherheitsverletzungen von Drittanbietern konfigurieren.
- Die Aktivitäten von Drittanbietern in Ihrer IT-Infrastruktur mithilfe detaillierter Protokolle zur Benutzeraktivität überwachen.
- Mit Drittparteienrisiken umgehen können und nicht überwiegend auf Drittdienstleister vertrauen.
- Gegebenenfalls technische Ausstiegsstrategien bereitstellen.

Commvault kann Unternehmen durch Workload-, Cloud- und Hypervisor-übergreifende Datenportabilität bei der Einhaltung dieser Vorschriften unterstützen.

Im Folgenden finden Sie spezifische Anforderungen der DORA-Verordnung sowie Informationen, wie Commvault-Lösungen Sie bei der Erfüllung unterstützen können.

Provision	Commvault Solution
In Artikel 28.8 wird dargelegt, wie Unternehmen mit Drittparteienrisiken umgehen sollen und wie einer übermäßigen Abhängigkeit von Drittdienstleistern entgegenzuwirken ist. Unternehmen müssen überdies geeignete Ausstiegsstrategien einrichten.	Die Any-to-Any-Portabilität von Commvault ermöglicht eine nahtlose Daten- und Anwendungsmigration zu und von Drittdienstleistern und kann als Ausstiegsstrategie oder Datenmigrationslösung genutzt werden.

05 Informationsaustausch

Kapitel VI (Artikel 45) von DORA ermutigt Finanzinstitute, Informationen und Erkenntnisse über Cyberbedrohungen untereinander auszutauschen, um die digitale operationale Resilienz der gesamten Branche zu erhöhen.

Diese Institute sollten:

- Detaillierte Aufzeichnungen über Benutzeraktivitäten führen und Sicherheitsvorfälle dokumentieren, um sie bei der Meldung von und Zusammenarbeit bei Vorfällen an Aufsichtsbehörden und andere Finanzunternehmen weitergeben zu können.
- Umfassende Protokolle und Berichte erstellen, um die Einhaltung gesetzlicher Vorschriften zur Cybersicherheit zu demonstrieren.
- Beim Übermitteln von Cybersicherheitsnachweisen die Daten in einem geschützten Dateiformat exportieren.

Commvault kann Ihnen mit den folgenden Funktionen bei diesen Bemühungen helfen:

- Bidirektionaler Austausch von Threat Intelligence/IOCs mithilfe nativer REST- APIs und Sicherheitsintegrationen von Drittanbietern führen zu einer Informationsanreicherung, die hilft, Vorfälle besser klassifizieren/aktualisieren zu können.
- Verschlüsselte und mit zertifikatbasierten Signaturen versehene Kommunikation über Syslog-/Webhook-/API-Aufrufe ermöglicht das Streamen von Sicherheitsprotokollen zur zentralisierten Sammlung und Archivierung von Beweisen.
- Vom Menschen und Maschinen veranlasste Aktionen/Rekonfigurationen werden vollständig über eingebettete Prüfprotokolle erfasst und ermöglichen das Sichern von Beweisen.

Im Folgenden finden Sie einige spezifische Anforderungen der DORA-Verordnung sowie Informationen, wie Commvault-Lösungen Sie bei der Erfüllung unterstützen können.

Provision	Commvault Solution
Gemäß Artikel 45 müssen Finanzinstitute detaillierte Aufzeichnungen über Nutzeraktivitäten anlegen und Sicherheitsvorfälle dokumentieren. Sie müssen umfassende Protokolle und Berichte erstellen, um die Einhaltung gesetzlicher Vorschriften zur Cybersicherheit nachzuweisen	Commvault-Lösungen ermöglichen es Unternehmen, sensible Daten, unsichere oder nicht aktivierte sichere Konfigurationen zu identifizieren und diese in gemeinsam genutzten Dokumentationssätzen zu erfassen. Alle Benutzeraktivitäten, einschließlich API-Dienstkonten an der CV-Schnittstelle, werden erfasst. Darüber hinaus kann Threatwise Sicherheitsgemeinschaften
Artikel 45 schreibt außerdem vor, dass Unternehmen beim Weitergeben von Cybersicherheitsnachweisen Daten in einem geschützten Dateiformat exportieren müssen.	Commvault-Lösungen verfügen über mehrere Formate für Bedrohungsinformationen und ermöglichen die gemeinsame Nutzung von Protokollen über mehrere verschlüsselte und authentifizierte Kanäle wie Syslog/Webhook/RestAPIs. So können alle risikobezogenen Attribute über die zentralisierten Tools der Kunden zentral erfasst und gesichert werden.

Strafen für Nichteinhaltung

Die Nichteinhaltung von DORA kann zu erheblichen Strafen führen, die für die Aufrechterhaltung der Integrität und Wirksamkeit der Richtlinie von entscheidender.

Bedeutung sind. Diese können je nach Schwere und Art des Verstoßes variieren. Sie sollen abschreckend wirken und stehen in einem angemessenen Verhältnis zur Finanzkraft und Größe des Unternehmens sowie zum Ausmaß des durch die Nichteinhaltung verursachten Schadens.

Bei geringfügigen Verstößen können Finanzunternehmen Warnungen oder Verweise erhalten. Bei schwerwiegenderen Verstößen können jedoch strafrechtliche und/oder verwaltungsrechtliche Sanktionen verhängt werden. Bei wiederholten oder besonders eklatanten Verstößen sind die Regulierungsbehörden befugt, zusätzliche Sanktionen zu verhängen. Dazu gehören der Entzug von Zulassungen, vorübergehende Verbote bestimmter Geschäftsaktivitäten oder andere Einschränkungen, die zum Schutz des Finanzsystems erforderlich sind.

Kontaktieren Sie unser Team, wenn Sie mehr darüber erfahren möchten, wie Commvault-Lösungen Ihr Unternehmen bei der Einhaltung der DORA-Bestimmungen unterstützen können.

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®