controlware

DORA in der Praxis –
Von regulatorischen Anforderungen zur technischen Realität

DORA in der Praxis – Von regulatorischen Anforderungen zur technischen Realität

Mit dem Inkrafttreten der DORA-Verordnung beginnt für viele Finanzunternehmen, Versicherungen, Wertpapierfirmen und Zahlungsdienstleister eine neue Phase des IKT-Risikomanagements. Doch was bedeutet das konkret für die technische Umsetzung? Das Whitepaper zeigt, wie aus regulatorischen Vorgaben funktionierende IT-Lösungen werden und sich diese sinnvoll in bestehende Systemlandschaften integrieren lassen, ohne die Betriebsfähigkeit oder Innovationskraft zu gefährden. Anhand praxiserprobter Methodik und klarer Umsetzungsarchitektur wird ein Weg aufgezeigt, DORA nicht nur regelkonform, sondern zukunftsfähig zu gestalten.

Die DORA-Realität: Wenn Compliance auf IT-Infrastruktur trifft

Seit dem 17. Januar 2025 sind Finanzinstitute und deren IKT-Dienstleister zur Anwendung der Digital Operational Resilience Act (DORA) verpflichtet. Die EU-Verordnung 2022/2554 stellt Unternehmen der Finanzbranche vor die zentrale Herausforderung, komplexe IT-Infrastrukturen mit strikten Compliance-Anforderungen in Einklang zu bringen. Dabei überfordert insbesondere die Interpretation identifizierter Gaps und deren Übersetzung in konkrete technische Maßnahmen viele Projektteams. Das Kernproblem liegt hauptsächlich darin, regulatorische Vorgaben in Realität und Praxis umzusetzen. Zudem verschärfen personelle Ressourcenengpässe bei gleichzeitig hohem Spezialisierungsgrad die Balance zwischen Compliance, Betreibbarkeit, Flexibilität und zukunftsfähiger Skalierbarkeit.

Regulatorischer Rahmen und Implementierungsrealität

DORA markiert einen bedeutsamen Paradigmenwechsel im IKT-Risikomanagement des Finanzsektors. Die Verordnung löst nationale IT-Aufsichtsanforderungen wie BAIT, ZAIT, KAIT und VAIT ab. Die verbundenen Rundschreiben werden durch die BaFin sukzessive aufgehoben, um Doppelregulierung zu vermeiden. Im Gegensatz zu bisherigen fragmentierten Ansätzen strukturiert DORA das IKT-Risikomanagement entlang des NIST Cybersecurity Framework und ermöglicht die zusammenhängende Betrachtung verschiedener Domänen.

Erstmals unterliegen kritische IKT-Dienstleister direkter EU-Regulierung durch Aufsichtsmechanismen. Die europäischen Aufsichtsbehörden (EBA, ESMA, EIOPA) fungieren hier als federführende Überwachungsbehörden mit zwangsgeldbewährten Informations-, Kontroll- und Prüfrechten. Diese können umfassende Untersuchungen durchführen, Inspektionen anordnen und bei Nichtkonformität sogar die Aussetzung der Dienstleisternutzung veranlassen.

Die Konkretisierung vager DORA-Anforderungen erfolgte erst 2024 durch technische Regulierungsstandards (RTS und Implementierungsstandards (ITS). Diese schaffen zwar mehr Klarheit, lassen aber weiterhin Interpretationsspielräume bei der praktischen Umsetzung zu. Die tatsächliche Wirksamkeit und Nachweisbarkeit implementierter Maßnahmen werden spannend zu beobachten sein, insbesondere im Kontext der Angriffserkennung und damit verbundener SOC- und SIEM-Implementierungen. Anstehende Prüfungen werden Best Practices formen und Licht in die notwendige Nachweisführung bringen, auf die regulierte Unternehmen und Institute reaktionsfähig sein müssen.

IKT-Risikomanagement als technologischer Kern

Basierend auf der strukturierten Regulierungslandkarte ergeben sich *vier zentrale Säulen des IKT-Risikomanagements*, die ineinandergreifen:

Schutz und Prävention
Art. 9 DORA

Zero-Trust-Architekturen (und damit verbundene Wirkprinzipien wie Mikrosegmentierung) stellen in mehr als einer Hinsicht eine wichtige Weichenstellung dar: Sie verbessern die technische Resilienz, schaffen die Grundlagen für risikobasierte Modelle zur Gewährleistung der Verfügbarkeit, Authentizität und Integrität, unterstützen bei der Vermittlung benötigter Fähigkeiten und ermöglichen die Umsetzung geforderter Konzepte, etwa mit Blick auf automatisierte Mechanismen zur Isolierung von Systemen oder „Least Privilege". Identity & Access Management (IAM) sowie Privileged Access Management (PAM) bilden dabei das Fundament, um die Identität als „den neuen Perimeter" bestmöglich abzusichern.

Herausforderungen im jeweiligen Betriebskontext der Organisation und generelle DORA-Anforderungen an das Schwachstellen-, Exposure- und Patch-Management erfordern zunehmend den Einsatz von Automatisierung, um eine effektive und systematische Umsetzung zu gewährleisten – ergänzt durch kryptografische Maßnahmen, die das Sicherheitsniveau erhöhen und grundlegende Anforderungen an die Vertraulichkeit adressieren.

Erkennung
Art. 10 DORA

Die geforderte, unmittelbare Erkennung von Anomalien und Bedrohungen wird durch (Managed) XDR-Plattformen realisiert, die eine korrelierte Bedrohungserkennung ermöglichen. Aktuelle SIEM- und technologische SOC-Implementierungen müssen über traditionelle Ansätze hinausgehen und moderne, integrierte Lösungsansätze verfolgen, um die DORA-Anforderungen an Betreibbarkeit und Wirksamkeit zu erfüllen.

Reaktion
Art. 11 DORA

Um im Rahmen IKT-bezogener Vorfälle schnell und angemessen reagieren und mögliche Schäden begrenzen zu können, sind automatisierte Playbooks sowie die Integration von SOAR für effektive Eindämmungsstrategien und -maßnahmen erforderlich. Um die Fortführung der kritischen Funktionen der Organisation sicherzustellen bzw. Einschränkungen so gering wie möglich zu halten, müssen den beschriebenen IKT-Reaktionsplänen vor allem Wiederherstellungs- und Geschäftsfortführungspläne folgen.

Zudem ist es ratsam, definierte Verantwortlichkeiten und Eskalationswege in automatisierte Workflows zu integrieren. Die Einbettung in bestehende Krisenmanagement-Prozesse sowie kontinu-

Managed Detection & Response – modular und mehrfach ausgezeichnet!

Controlware Managed SOC Services basiert auf marktführenden EDR/XDR-Lösungen, welche zur Risikoerkennung an Endpoint (Client/Server) eingesetzt werden in Verbindung mit SOC-Leistungen wie Incident Analyse und Threat Hunting. Ziel des Managed SOC Services auf Basis EDR/XDR ist es, Bedrohungen früh zu erkennen, zu bewerten und entsprechende Gegenmaßnahmen einzuleiten bzw. Handlungsempfehlungen auszusprechen. Unser Managed SOC-Service auf XDR-Basis entspricht den Empfehlungen des BSI zur Protokollierung und Detektion von Cyber-Angriffen.

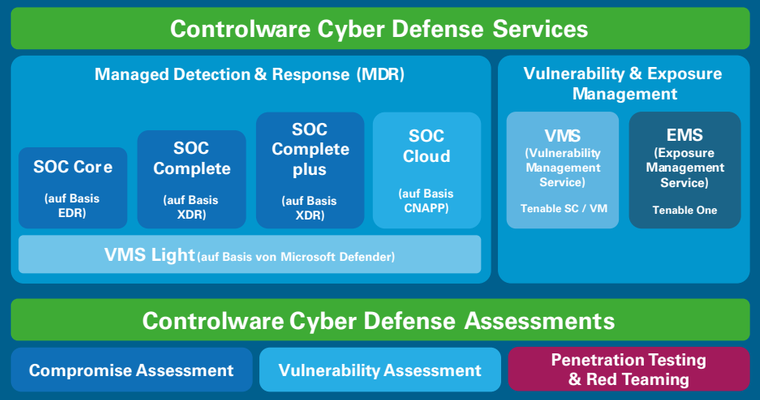

Abbildung oben: Mehrfach ausgezeichnet – die Cyber Defense Services der Controlware

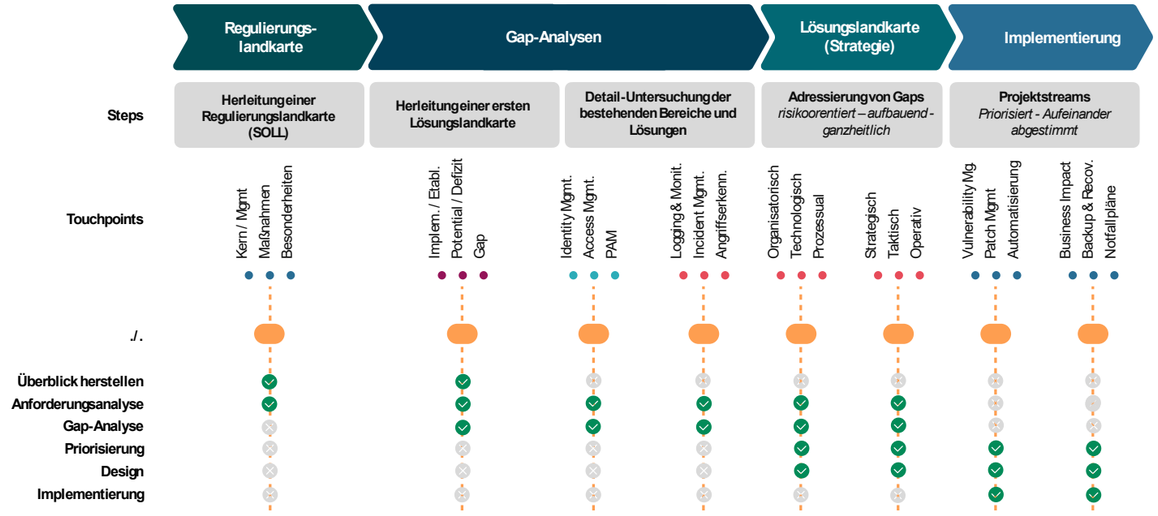

Abbildung: Die ”IT- und Lösungslandkarte” – Integration von IT-Compliance

ierliche Wirksamkeitskontrollen (wie zum Beispiel Tabletop-Übungen und realitätsnahe Notfallübungen oder -simulationen) sind dabei essenziell. Solche realistischen Testszenarien erfordern eine solide Grundlage aus Sicht des Business Continuity Managements (BCM) – mit klaren Zielen sowie ineinandergreifenden Mechanismen und Prozessen, die auch Services von IKT-Drittdienstleistern einbeziehen.

IKT-Geschäftsfortführung und Recovery
Art. 11-12 DORA

IKT-Services und jegliche technische sowie organisatorische Maßnahmen – unter anderem in den Bereichen Reaktion, Wiederherstellung und Fortführung kritischer Funktionen – müssen auf den Vorgaben der IKT-Geschäftsfortführungsleitlinie sowie auf Analysen und Ableitungen zur Geschäftskritikalität (BIA) basieren und entsprechend konzipiert werden. Es ist unerlässlich, dass Fortführungs-, Backup- und Recovery-Strategien in bestimmten Fällen für kritische und wichtige Funktionen die Switch-Over-Fähigkeit zu Backup-Rechenzentren sicherstellen. Automatisierte Wiederherstellungs- und Disaster-Recovery-Tests vervollständigen die Fähigkeiten in diesem Bereich.

Implementierungsmethodik: Von der Regulierungslandkarte zur Lösungsarchitektur

Für eine erfolgreiche Umsetzung von DORA auf technologischer Ebene hat sich in unserer Praxis ein systematisches, phasenorientiertes Vorgehen bewährt. Dieses verbindet technische Exzellenz mit regulatorischen Anforderungen und fördert zugleich das Überwinden organisatorischer Silos. Dadurch wird eine nachhaltige und ganzheitliche Implementierung ermöglicht, die sowohl Compliance als auch Innovation unterstützt.

PHASE 1: Identify and Analyse (Regulierungslandkarte, Governance und Compliance)

Die Grundlage des Vorgehens bildet die Entwicklung einer strukturierten Regulierungslandkarte, die DORA-Anforderungen gegen relevante Bestands-Regularien oder -Standards mappt und strukturierte Anforderungskataloge ableitet. Dabei werden Inputs aus durchgeführten Schutzbedarfs-, Business Impact- und Risikoanalysen berücksichtigt.

Die systematische Bestandsaufnahme erfolgt Workshop-basiert gemäß einer bewährten Methodik, die den aktuellen Zustand (Design, Komponenten, Funktionalitäten, Prozesse und Workflows) erfasst. Besondere Bedeutung kommt der Identifikation von Schwachstellen, Defiziten und Potentialen auf technischer und organisatorischer Ebene zu.

Die Besonderheit dieser Methodik liegt im Aufbrechen von Silos durch zusammenhängende Betrachtung der entsprechenden Bereiche, beispielsweise:

- Log Management, Angriffserkennung und Incident Management / Response
- Identity Management, Access Management und Privileged Access Management
- Vulnerability Management, Patch Management, Automatisierung und Exposure Management

Ebenso werden vorhandene Betriebsansätze wie Plan-Build-Run oder DevSecOps in die Analyse einbezogen.

PHASE 2: Strategische Lösungsarchitektur (Lösungslandkarte)

Die Entwicklung der angestrebten SOLL-Landkarte erfolgt entlang von drei Dimensionen: organisatorisch, technisch und prozessual. Dabei werden verschiedene Ebenen und Zeithorizonte betrachtet – strategisch, taktisch und operativ – unter Berücksichtigung der Grundsätze: risikoorientiert, aufbauend und ganzheitlich.

Make-or-Buy-Entscheidungen gewinnen besondere Relevanz bei der Auslagerung technischer Expertise und Betriebstätigkeiten, insbesondere bei Managed Services zum Thema Angriffserkennung (Managed Detection- & Response (MDR)- / SOC).

Eine Lösungslandkarte berücksichtigt zudem die Prägung eines notwendigen Mindsets und integriert nicht nur die menschliche Komponente, sondern auch das zukünftige gemeinsame Arbeiten. Zentrale Konzepte umfassen Zero-Trust-Architekturen, Plattformansätze, integrierte Ansätze sowie das Management von Schnittstellen und das Aufbrechen bzw. Verbinden von Silos aus Prozess- und Workflow-Sicht.

PHASE 3: Technische Konzeption der vier Säulen

Die ***Protection-Implementierung*** beinhaltet die Integration von Vulnerability Management , Patch Management und Automatisierung. Mikrosegmentierung mit automatischer Isolation kompromittierter Systeme wird zum Standard. Die Identität als neuer Perimeter erfordert Risk-based Authentication und Privileged Access Management sowie den Umgang mit den Herausforderungen rund um Entra ID.

Die ***Detection-Realisierung*** erfolgt durch XDR-Plattformen für korrelierte Bedrohungserkennung, Threat Intelligence Integration und Penetration Tests. Software-defined Security für dynamische Infrastrukturen und Exposure Management als Erweiterung des klassischen Schwachstellenmanagements erhöhen die Erkennungsqualität.

Die ***Response-Orchestrierung*** implementiert Incident Response Automation mit definierten Playbooks (SOAR), Integration in bestehende Krisenmanagement-Prozesse sowie kontinuierliche Wirksamkeitskontrollen und regelmäßige organisatorische und technische Wirksamkeitstests, einschließlich Notfallübungen und Table-Tops.

Die ***Recovery-Optimierung*** stellt abgestimmte Prozesse und angemessene Reaktions- und Wiederherstellfähigkeiten sicher und behandelt die Integration der organisatorischen Ebene aus dem BCM und IT-Notfallmanagement, den Anforderungen aus den Business Impact und Schutzbedarfseinschätzungen, sowie tatsächliche technische Fähigkeiten und etablierte Notfallpläne. Automatisierte Tests bestimmter Use-Cases und Komponenten gewährleisten eine kontinuierliche Validierung.

PHASE 4: Abgestimmte Projektstreams zur Umsetzung

Die Umsetzung von Projektstreams erfolgt priorisiert und aufeinander abgestimmt. Dokumentationsautomatisierung für Audit-Readiness und kontinuierliche Anpassung an die evolvierende Compliance-Landschaft gewährleisten nachhaltige Compliance.

Regelmäßige Überprüfungen und Aktualisierungen der Automatisierungstools und -prozesse ermöglichen die regelmäßige Anpassung an

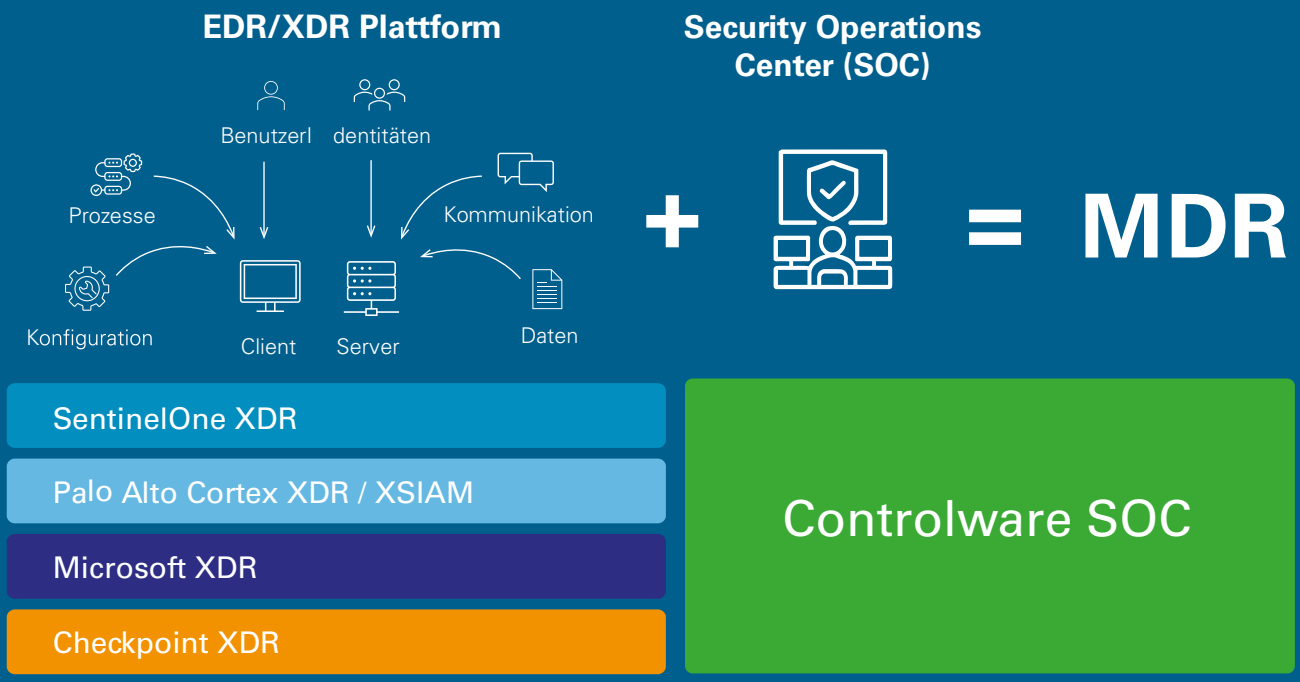

Abbildung: Controlware Managed Detection & Response (MDR)

vorhandene und neue Bedrohungen sowie an regulatorische Änderungen.

Von der Compliance zur nachhaltigen Cyber-Resilienz

DORA stellt weit mehr als eine weitere Compliance-Anforderung dar – DORA ist ein Katalysator für IT-Modernisierung, der bei strategischer Herangehensweise als Wettbewerbsvorteil positioniert werden kann. Der Erfolg liegt in den strukturierten maßnahmen, die technische Exzellenz mit regulatorischen Anforderungen verbinden und Automatisierung als Schlüssel für operative Effizienz einsetzen.

Mehrwert von Controlware: Technologischer Praxispartner

Als erfahrener Vermittler zwischen Consulting-Strategien und IT-Realität unterstützt Controlware Finanzinstitute in allen Phasen der technischen DORA-Umsetzung. Der ganzheitliche Ansatz schafft die notwendige Balance zwischen Compliance, Betreibbarkeit und Innovation, während bewährte Methodiken eine strukturierte Herangehensweise für nachhaltige Cyber-Resilienz gewährleisten.

Die technische Umsetzung der DORA-Anforderungen erfordert tiefe Eingriffe in komplexe Infrastrukturen, mit denen Projektteams häufig überfordert sind – sei es aufgrund fehlender personeller Ressourcen oder mangelndem technischen Know-how. Controlware schließt diese Lücke als Praktiker, der die Herausforderungen beim „Interpretieren" und „Übersetzen" identifizierter Gaps versteht und konkrete technische Lösungen aus regulatorischen Anforderungen herleitet. ■

Unsere Standorte

Deutschland

Zentrale
Controlware GmbH
Waldstraße 92
63128 Dietzenbach

Tel. +49 6074 858-00
Fax +49 6074 858-108
info@controlware.de
www.controlware.de
blog.controlware.de

Besuchen Sie uns auf:

Berlin
Tel. +49 30 67097-0
info-ber@controlware.de

Düsseldorf
Tel. +49 2159 9696-0
info-due@controlware.de

Frankfurt/Main
Tel. +49 6074 858-206
info-ffm@controlware.de

Hagen
Tel. +49 2331 8095-0
info@networkers.de

Hamburg
Tel. +49 40 251746-0
info-ham@controlware.de

Hannover
Tel. +49 511 726092-0
info-han@controlware.de

Ingolstadt
Tel. +49 841 23222-0
info-ing@controlware.de

Kassel
Tel. +49 561 47576-0
info-kas@controlware.de

Leipzig
Tel. +49 341 98387-30
info-lei@controlware.de

München
Tel. +49 89 666367-0
info-muc@controlware.de

Stuttgart
Tel. +49 711 770568-0
info-stu@controlware.de

Wolfsburg
Tel.: +49 5362 9993413
info-wey@controlware.de

Österreich

Innsbruck
Tel. +43 512 345200
info@controlware.at

Wien
Tel. +43 1 890 0724-0
info@controlware.at

Schweiz

Tel. +41 55 4156476
info@controlware.ch