die bank

05|2023

DORA-RICHTLINIE
SO WERDEN DIGITALE SYSTEME STABIL

Euro 17,00

G 8790

DIGITAL OPERATIONAL RESILIENCE ACT NACHHALTIG UMSETZEN

DORA-Richtlinie: So werden digitale Systeme stabil

Im Fokus steht der Digital Operational Resilience Act, kurz DORA, der am 17. Januar 2023 in Kraft getreten ist. 24 Monate später erfolgt die Anwendung, das heißt, spätestens ab Januar 2025 müssen Finanzinstitute und IKT-Drittanbieter die neuen Anforderungen zur Betriebsstabilität digitaler Systeme erfüllen. Was gilt es zu berücksichtigen? Und vor allem, wie kann man die Vorgaben erfolgreich und pragmatisch im eigenen Unternehmen umsetzen? In diesem Artikel schildert der Autor den Weg zu einer nachhaltigen DORA-Compliance.

Cyber-Gefahren führen bereits mehrere Jahre in Folge die Rangliste der Unternehmensrisiken an. Dabei ist der Finanzsektor für Cyber-Kriminelle besonders attraktiv. Laut einer Studie der Boston Consulting Group aus dem Jahr 2019 wurden Banken 300 mal häufiger angegriffen als Unternehmen anderer Branchen. Außerdem nehmen die Angriffe deutlich zu und werden immer „intelligenter".

Berücksichtigt man zudem, dass laut aktuellem Report des IT-Sicherheitsspezialisten Trend Micro Finanzinstitute am häufigsten Lösegeld an Cyber-Erpresser bezahlen, ergibt sich ein eindeutiges Bild: Die Finanzbranche hat ein besonders hohes Cyber-Risiko – und damit eine besonders hohe Verpflichtung, sich dieser zu stellen, mit guter Vorbereitung, umfassenden Konzepten, intelligenter technischer Unterstützung und schlagkräftigen Teams.

Mit der im Januar in Kraft getretenen DORA-Richtlinie (Digital Operational Resilience Act) schafft die EU länderübergreifende Vorgaben für den Schutz der Finanz-IT-Landschaft und vereinheitlicht das bestehende europäische und nationale Regelwerk.

DORA – worum geht es?

Mit dem Inkrafttreten der DORA-Richtlinie müssen alle Finanzdienstleister nachweisen, dass ihre Organisation ebenen- und bereichsübergreifend unterschiedlichsten IKT-Krisen gewachsen ist und die Betriebsstabilität digitaler Systeme jederzeit sichergestellt ist. Damit rücken die Fähigkeit zur Abwehr von Cyber-Gefahren sowie die Handlungsfähigkeit im Ernstfall in den Fokus.

Abhängig von der Unternehmensgröße und den Risiken aus dem Geschäftsmodell sowie dem Reifegrad der digitalen operationalen Resilienz des jeweiligen Finanzunternehmens wird es erforderlich sein, verschiedene Fähigkeiten im Risikomanagement zu stärken oder evtl. neu zu erwerben, unter Berücksichtigung der Verhältnismäßigkeit. Konkret müssen Organisationen sicherstellen, dass sie:

▷ **Risikomanagement zur Chefsache machen:** Die Richtlinie sieht vor, dass das Management gezielt Verantwortung für die IT-Sicherheit übernimmt. Führungspersonen müssen die Konsequenzen verschiedener Risiken und die an sie gestellten Erwartungen verstehen. Neben gesetzlich vorgeschriebenen Fortbildungen zu IT-Risiken sind sie verpflichtet, eine Risikobewertung nicht nur für das eigene Unternehmen, sondern auch für alle Drittanbieter vorzunehmen. Sie müssen Verantwortliche definieren, Business-Continuity- und Wiederanlaufpläne sowie Audits autorisieren und sich über IKT-Vorfälle sowie die Zusammenarbeit mit Dritten ausreichend informieren. Dazu gehört der Aufbau kurzer Informationswege; idealerweise sind wichtige Informationen stets aktuell und nicht mehr als drei Klicks entfernt. DORA verlangt also, dass Unternehmen IKT-Risikomanagement zur Chefsache machen.

▷ **Risiken gezielt und kontinuierlich erfassen:** Unternehmen müssen ihre Sicherheitsziele kennen und regelmäßig neu justieren. Sie sind verpflichtet, alle Systeme und Schnittstellen 24/7 auf Anomalien zu überwachen, Abweichungen zu erkennen und zu bewerten sowie Risiken zu dokumentieren.

▷ **Reaktionsschnell handeln:** Im Ernstfall müssen Organisationen in der Lage sein, umgehend auf einen Angriff oder eine Anomalie zu reagieren und entsprechende Gegenmaßnahmen einzuleiten. Gleiches gilt für die Implementierung der Notfallvorsorge, das Bewirtschaften von Wiederherstellungsplänen und die Reduktion von Risiken.

▷ **Professionell und strategisch kommunizieren:** Reibungslos, sicher und zielgerichtet – die neue Verordnung stellt zudem hohe Anforderungen an Abläufe und Strukturen für die Kommunikation mit relevanten internen und externen Zielgruppen. Ein wichtiges Ziel ist der schnelle Informationsfluss. Vorfälle müssen daher lückenlos dokumentiert und intern sowie extern kommuniziert werden, um Wissen weitergeben zu können. In schwerwiegenden Fällen besteht nun für den gesamten Finanzsektor – nicht nur für große Institute – eine offizielle Meldepflicht.

1 | Daten redundanzfrei pflegen, alle Fragen aus einer Hand beantworten

Für die Datenbasis im Risikomanagement gilt: Zusammen lassen, was zusammen gehört

1 Discover

- Verschaffen Sie sich einen Überblick über die Datenlage im Unternehmen, auch mit Blick auf Drittanbieter und die globale Gefahrenlage.
- Stellen Sie sicher, dass alle Daten qualitativ hochwertig und hochverfügbar sind.
- Inklusive Vollständigkeit auf allen Ebenen.

2 Map

- Verknüpfen Sie sämtliche relevanten Daten auf intelligente Weise über ein regelbasiertes Repository, um Zusammenhänge und Abhängigkeiten zu ermitteln.
- Digitalisieren Sie die DORA-Richtlinie und verknüpfen Sie einzelne Vorgaben mit Ihrer Business-Architektur, um Schwachstellen und regulatorische Risiken automatisiert zu scannen.

3 Visualize

- Erstellen Sie vielfältige, möglichst individuell zugeschnittene Visualisierungen von Anomalien, Trends, Workflows und Handlungsbedarfen, um schnelle und bessere Entscheidungen zu treffen.

4 Improve

- Bauen Sie ein regelbasiertes und konfigurierbares Analyse-, Berichts- und Meldewesen auf, um mehrere Bewertungen in einem Schritt zu bearbeiten.
- Bilden Sie unterschiedliche Zielgruppen und Themenkreise ab, um Assessments zu optimieren.
- Seien Sie jederzeit nachvollziehbar auskunftsbereit.

Quelle: Eigene Darstellung

▷ **Umfangreich testen und trainieren:** Unternehmen müssen nachweisen, dass ihre Systeme, Daten und Abläufe stets aktuell sind. Dafür ist die Durchführung robuster und umfassender Tests zur digitalen Betriebsstabilität (Operational Resilience Testing) vorgeschrieben. Darüber hinaus sind mindestens alle drei Jahre Threat-Led Penetration-Tests (TLPT) erforderlich, d. h. die Cyber-Resilienz eines Unternehmens muss durch einen simulierten Angriff eines sogenannten ethischen Hackers auf die Probe gestellt werden.

Am Ende laufen alle Anforderungen darauf hinaus, dass die Verantwortlichen in kritischen Situationen schnelle, informierte Entscheidungen treffen können und resilient – das heißt, auf Alternativen vorbereitet – sind. Denn DORA erfordert eine gesamtheitliche Sicht, quasi den Blick auf den Bauplan eines Unternehmens.

Wie sollte man also vorgehen, um die eigene Organisation strategisch aufzustellen und resilient gegen Cyber-Gefahren zu machen?

Datenlage optimieren: Hohe Verfügbarkeit, Aktualität und Qualität sicherstellen

Die wichtigste Grundlage ist eine solide Datenbasis mit hoher Datengüte, Datenverfügbarkeit und Vernetzung. Nur wer weiß, wo er steht, kann den richtigen Weg zum Ziel einschlagen. Was simpel klingt, ist aber in vielen Unternehmen eine immense Herausforderung. Zum einen, weil Daten häufig in Silos vorliegen und für sich genommen wenig aussagekräftig sind. Zum anderen, weil wichtige Daten gar nicht erst erfasst werden oder nicht aktuell vorliegen.

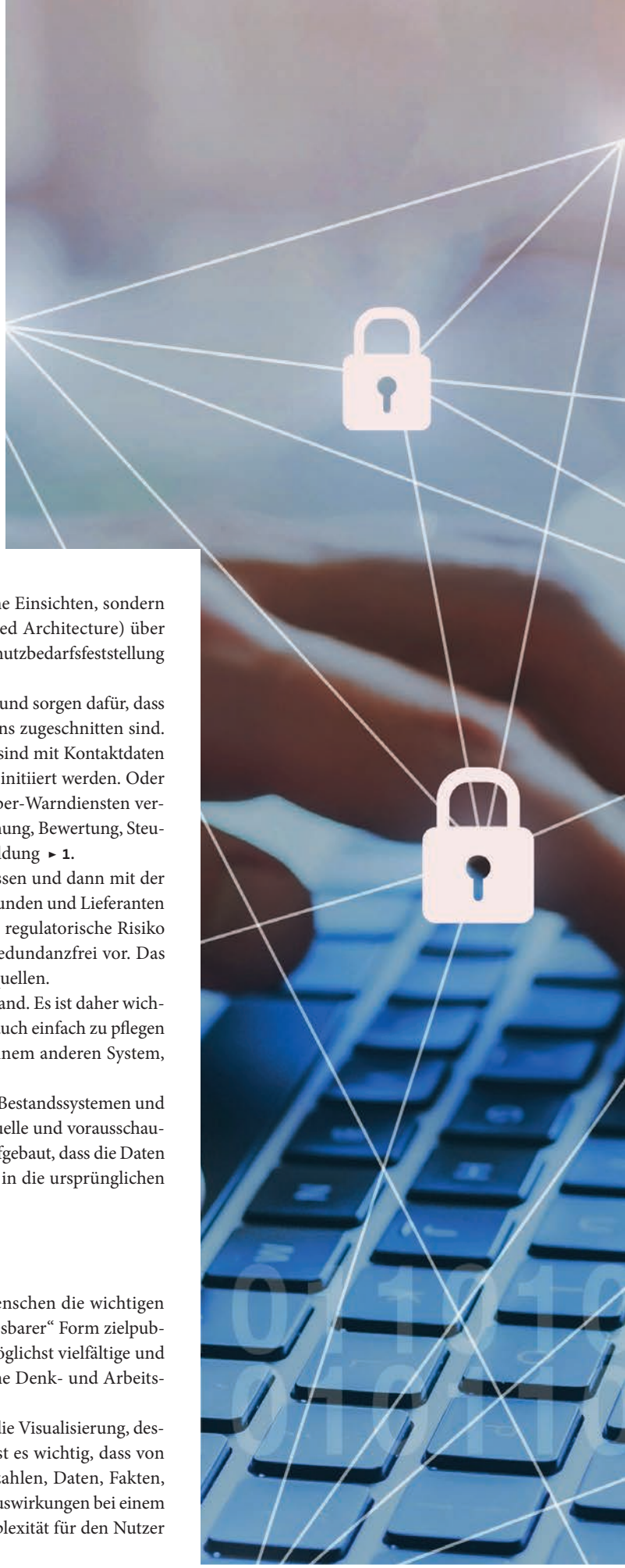
Wichtig für die Umsetzung der DORA-Richtlinie sind zum Beispiel Performance-Daten von IT-Systemen, Daten zur Bedrohungslandschaft und der Kritikalität verschiedener Prozesse und Systeme, aber auch Informationen zu Incident-Response-Plänen mit Eskalationshierarchien und Kommunikationsstrategien.

Ein Kernkriterium ist der Blick über den eigenen Unternehmenshorizont. Können die Verantwortlichen einfach überprüfen, welcher Zulieferer die DORA-Anforderungen erfüllt? Haben sie die globale Gesamtgefahrenlage tagesaktuell im Blick?

Aber auch die vermeintlich simplen Dinge sollten nochmals gründlich geprüft werden. Liegen die vollständigen und tagesaktuellen Kontaktdaten aller relevanten Personen vor, die es bei einem IKT-Notfall zu erreichen gilt? Gibt es den Überblick über wichtige Know-how-Träger im Unternehmen? Im Notfall sind es diese kleinen Dinge, die den Ausschlag geben.

Intelligent dokumentieren: Zusammenhänge erfassen, gezielt handeln

Eine solide Datenbasis ist das nötige Fundament. Ein hilfreiches Arbeitsmittel wird sie aber erst durch eine intelligente Vernetzung der Daten. Zusammenhänge, Abhängigkeiten, Zuordnungen – es gilt, den Datenbestand zu organisieren und zu strukturieren. Das heißt, Prozesse und Abläufe müssen identifiziert, klassifiziert und so dokumentiert werden, dass sie leicht zu aktualisieren und in immer neuen Kombinationen verknüpft werden können.



Wenn Daten intelligent verknüpft sind, liefern sie nicht nur hilfreiche Einsichten, sondern ermöglichen es, Prozesse zu automatisieren – von SOA (Service Oriented Architecture) über Bedrohungsanalyse, Strukturanalyse und Informationsverbund bis zur Schutzbedarfsfeststellung – und entlasten somit die Organisation.

Regelbasierte Daten-Repositories versehen die Daten mit einer Logik und sorgen dafür, dass alle Verknüpfungen individuell auf die Anforderungen des Unternehmens zugeschnitten sind. Liegen zum Beispiel Incident-Response-Pläne in digitaler Form vor und sind mit Kontaktdaten der entsprechenden Teams verknüpft, können automatisierte Workflows initiiert werden. Oder sind Systemdaten der eigenen Systeme mit den Live-Meldungen von Cyber-Warndiensten verknüpft, können automatisierte Alarme ausgelöst oder Regeln zu Überwachung, Bewertung, Steuerung und Kontrolle jeglicher Art angestoßen werden. Vgl. dazu die Abbildung ► **1**.

Besonders hilfreich ist es, die DORA-Richtlinie selbst digital zu erfassen und dann mit der Business-Architektur – von Prozessen und Rollen bis zu Applikationen, Kunden und Lieferanten – zu vernetzen. So können GAPs und Schwachstellen gescannt und das regulatorische Risiko ermittelt werden. Auch liegen in einem solchen Repository die Daten redundanzfrei vor. Das verringert nicht nur den Pflegeaufwand, sondern eliminiert auch Fehlerquellen.

Eine Datenbank ist jedoch immer nur so gut wie ihr aktueller Pflegestand. Es ist daher wichtig, darauf zu achten, dass Daten nicht nur intelligent verknüpft, sondern auch einfach zu pflegen und zu dokumentieren sind. Liegt die Datenquelle außerhalb oder in einem anderen System, wird durch intelligente Anbindung für Konsistenz gesorgt.

Benutzerfreundliche Eingabemasken, umfangreiche Schnittstellen zu Bestandssystemen und ein automatisiertes Abfragen von aktuellen Daten sind essenziell, um aktuelle und vorausschauende Analysen machen zu können. Idealerweise ist die Infrastruktur so aufgebaut, dass die Daten auch umgekehrt fließen können, also von der Gesamtdatenbank zurück in die ursprünglichen Systeme, um auch hier den Pflegeaufwand zu reduzieren.

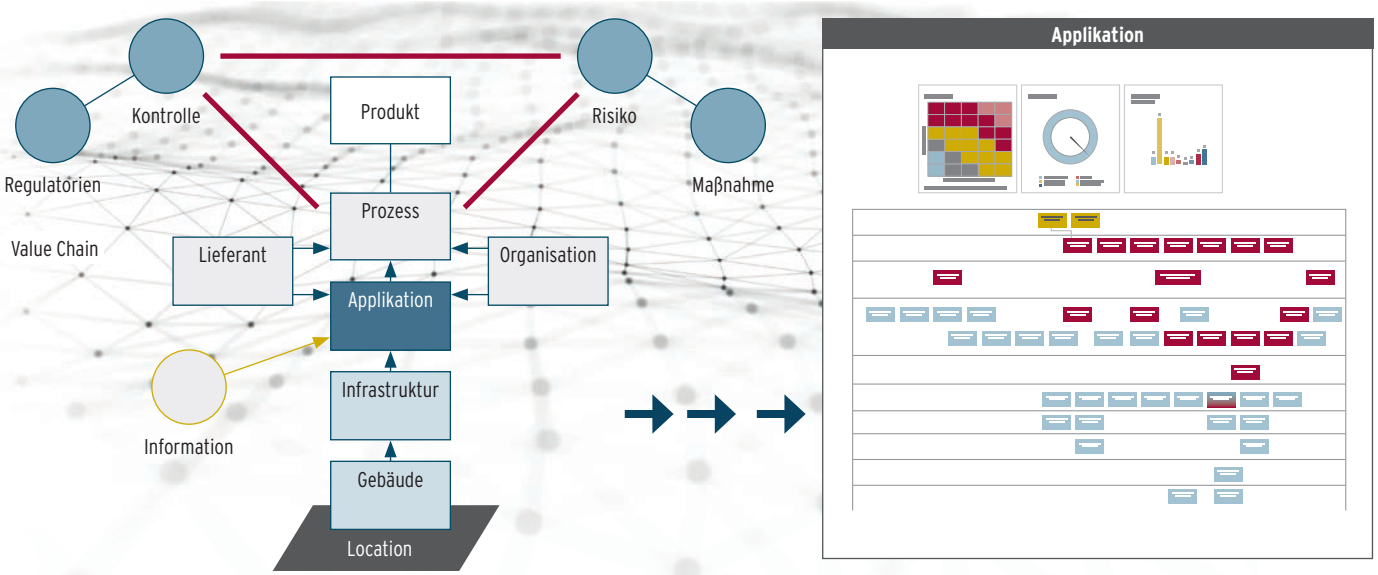
Aussagekräftig visualisieren: ein Lagebild – viele Blickwinkel

Auch wenn sich heute Vieles automatisieren lässt: Am Ende treffen Menschen die wichtigen Entscheidungen. Daten und Informationen sollten daher in „menschenlesbarer“ Form zielpublikumsgerecht vorliegen. Entscheidend ist, dass die Visualisierung auf möglichst vielfältige und individuelle Weise erfolgen kann, damit jeder Entscheider einen für seine Denk- und Arbeitsweise optimierten Input bekommt.

Tabellen, Matrix-Ansichten, Workflows oder Trendcharts – je besser die Visualisierung, desto schneller und gezielter kann gehandelt werden. Aus diesem Grund ist es wichtig, dass von allen Lieferanten und Systemen die wesentlichen Eigenschaften, Kennzahlen, Daten, Fakten, Qualitätsmesswerte, Aggregationen / Konsolidierungen sowie mögliche Auswirkungen bei einem Ausfall vorliegen, sie aber dennoch so präsentiert werden, dass die Komplexität für den Nutzer reduziert wird.

2 | Aktuell pflegen, intelligent verknüpfen, smart visualisieren, gezielt verbessern

Systeme mit leistungsfähigen Daten-Repositories unterstützen bei der nachhaltigen Umsetzung der DORA-Richtlinie



Quelle: Eigene Darstellung

Steuern, bewerten und kontrollieren: mehr Effizienz mit weniger Aufwand

Am Ende steht und fällt die Umsetzung einer Compliance-Vorgabe immer mit der Fähigkeit, die geforderten Nachweise und Prüfungen zu erbringen. Immer häufiger überschneiden sich Anforderungen verschiedener Richtlinien. So finden sich in DORA viele Vorgaben, die aus bestehenden Regularien wie MaRisk/BAIT, bsi 200 1-4 oder den Guidelines der EBA zu Outsourcing Arrangements ICT and Security Risk Management bekannt sind. Ein strukturiertes, vernetztes und intelligentes Kontroll-Assessment ist also auch hier hilfreich.

Ein regelbasiertes und konfigurierbares Analyse- und Berichtswesen kann mehrere Assessments, von DORA bis zur Datenschutz-Grundverordnung GDPR, miteinander vernetzen und mit einer Antwort mehrere Vorgaben bedienen – spontan, periodisch oder permanent, manuell, anlassbezogen, automatisch oder intelligent. Idealerweise bildet ein strukturiertes, nachhaltiges Kontrollmanagement auch unterschiedliche Zielgruppen und Themenkreise eines Unternehmens (IT, Sicherheit, Finanz, Legal etc.) ab. ► 2

FAZIT

Der Aufwand für eine erfolgreiche und nachhaltige Umsetzung der DORA-Richtlinie lässt sich mithilfe intelligenter Datenverknüpfungen deutlich reduzieren. Voraussetzung ist eine hohe Datenverfügbarkeit und -qualität sowie eine intelligente Vernetzung vorhandener Daten mittels Dashboards, Grafiken, Tabellen, Workflows und Alarmen. Dabei gilt für die Verantwortlichen der Hinweis: „Lassen Sie zusammen, was zusammengehört. So müssen Sie den Informationsverbund, also die Vernetzung sämtlicher relevanter Architektur-Assets der IKT, nur einmal pflegen und erhalten eine Unternehmens-DNA, die es erlaubt, alle Fragen aus einer Hand zu beantworten – von Risiko, Kontrolle, Sicherheit und Notfallvorsorge bis hin zu Auslagerung, Wiederanlauf, Rückabwicklung, Test und Simulation Ihrer Systeme."

Autor

Dr. Roland Pulfer, Gründer der Business-DNA Solutions GmbH und GRC-Experte beim Software-as-a-Service-Anbieter F24 AG. Er teilt sein Wissen regelmäßig auch als Speaker, zuletzt beim Kölner OpRisk-Forum zum Thema „DORA – durch Digitalisierung eine Vorgabe intelligent umsetzen".