Krisen bewältigen, Handlungsfähigkeit sichern, Resilienz steigern

Was sagt die DORA zum Umgang mit Krisen?

Vor dem Hintergrund zunehmender Cyber-Bedrohungen, geopolitischer Unsicherheiten und wachsender regulatorischer Anforderungen hat die operationelle Resilienz von Finanzinstituten deutlich an Bedeutung gewonnen. Mit dem Digital Operational Resilience Act (DORA) hat die Europäische Union einen verbindlichen Rahmen geschaffen, der Institute dazu verpflichtet, ihre Fähigkeiten zur Vermeidung, Bewältigung und Nachbereitung von IKT-bezogenen Störungen und Krisen umfassend zu stärken (vgl. Art. 5, 6, 11 DORA).

Während sich in der Vergangenheit viele Maßnahmen auf präventive Kontrollen und klassische Business-Continuity-Management-Ansätze (BCM) konzentrierten, erweitert DORA die Perspektive deutlich. Neben dem Schutz kritischer Systeme wird insbesondere die Fähigkeit in den Fokus gerückt, schwerwiegende Vorfälle effektiv zu managen und die Handlungsfähigkeit auch unter Krisenbedingungen aufrechtzuerhalten (vgl. Art. 17 DORA).

Reicht das bisherige BCM als Maßnahme aus? Was ist darüber hinaus zu beachten?

In zahlreichen Instituten hat sich BCM als essenzieller Bestandteil etabliert und fokussiert sich insbesondere auf die Aufrechterhaltung kritischer Geschäftsprozesse in Notfallsituationen. In der Praxis zeigt sich jedoch, dass Pläne allein nicht ausreichen, wenn sich ein isolierter Notfall zu einer komplexen Krise entwickelt. Situationen dieser Art sind oft durch eine hohe Dynamik, unvollständige Informationslagen, bereichsübergreifende Abhängigkeiten sowie erheblichen Entscheidungs- und Kommunikationsdruck geprägt. DORA bezieht diese Entwicklung ein, indem neben Notfallvorsorge und Wiederanlauf insbesondere auch Incident Management, Krisenkommunikation und Governance-Strukturen stärker in den regulatorischen Fokus rücken (vgl. Art. 5, 11, 13, 17 DORA).

Ein wesentlicher Aspekt ist dabei die eindeutige Festlegung von Rollen, Verantwortlichkeiten und Entscheidungswegen. Leitungsorgane sind explizit dazu angehalten, angemessene Strategien und Lösungsoptionen zu definieren sowie deren Wirksamkeit regelmäßig zu überprüfen (vgl. Art. 5, 6 DORA). Darüber hinaus fordert DORA regelmäßige Tests, Übungen und Reviews, um die tatsächliche Funktionsfähigkeit der etablierten Maßnahmen sicherzustellen (vgl. Art. 24 DORA).

Vor diesem Hintergrund gewinnen integrierte Ansätze an Bedeutung, die technische, organisatorische und personelle Aspekte miteinander verzahnen. Zu den zentralen Handlungsfeldern zählen dabei:

- die Integration von Informationssicherheit, BCM und Krisenmanagement,
- der Aufbau klar strukturierter Krisenstabsorganisationen,
- die Etablierung belastbarer Kommunikations- und Eskalationsprozesse,
- die Durchführung regelmäßiger, realitätsnaher Übungen
- sowie die gezielte Befähigung von Führungskräften zur Entscheidungsfindung unter Unsicherheit.

Kann ein solch komplexer integrierter Ansatz zum Krisenmanagement in der Praxis umgesetzt werden und wenn ja, wie? Welche zentrale Lösung gibt es in der Genossenschaftlichen FinanzGruppe?

Der Ansatz sollte durch die Kombination eines spezialisierten Cybersecurity-Services mit einem strukturierten Krisenmanagementrahmen umgesetzt werden.

Beispiel eines möglichen integrativen Ansatzes in der Praxis

Atruvia hat hierzu infolge einer Beiratsinitiative den Service agree21OpSec-CSIRTaaS erarbeitet. CSIRTaaS (kurz für: Computer Security Incident Response Team as a Service) ist eine spezialisierte Unterstützungsleistung zur strukturierten Bewältigung von Cybervorfällen. Der Service adressiert insbesondere die Anforderungen an Reaktions- und Wiederherstellungsfähigkeit. Im Kern ergänzt der Ansatz präventive Maßnahmen mit operativen Incident-Response-Fähigkeiten durch ein dediziertes Expertenteam. Im Falle eines schwerwiegenden Cyberangriffs übernimmt ein zentrales CSIRT die Koordination verschiedener Maßnahmen. Dazu zählen die initiale Lagebewertung, Eindämmung und forensische Analyse. Zusätzlich wird ein strukturierter „Werkzeugkoffer“ an Notbetriebsmaßnahmen bereitgestellt. Er ermöglicht auch unter Worst-Case-Bedingungen, etwa bei vollständiger Isolation der IT-Systeme, kritische Geschäftsprozesse innerhalb kurzer Zeit wieder aufzunehmen.

Ergänzend zu der beschriebenen operativ-technischen Komponente bietet Atruvia einen ganzheitlichen Beratungsansatz (Produktfamilie: Krisenmanagement 360), der insbesondere die organisatorische und führungsbezogene Ebene adressiert. Ziel ist es, Institute dazu zu befähigen, auch in komplexen und dynamischen Krisensituationen strukturiert, koordiniert und entscheidungssicher zu agieren.

Dieser Ansatz umfasst modulare Leistungsbausteine, die je nach Reifegrad und Zielbild kombiniert werden können. Dazu zählen u.a.:

- **Krisenstabsübungen:** Simulation realistischer Szenarien zur Überprüfung von Entscheidungs-, Eskalations- und Kommunikationsprozessen. Vor Ort in den Instituten gemeinsam mit dem Krisenstab.
- **Notbetriebstests:** Erprobung technischer und organisatorischer Abläufe unter Ausfallbedingungen zur Sicherstellung der Betriebsfähigkeit im Notfall.
- **Assessments:** Strukturierte Analyse des Reifegrads in den Bereichen Informationssicherheit, BCM und Compliance im Kontext regulatorischer Anforderungen anhand eines standardisierten Bewertungsbogens.
- **Krisenstabstrainings:** Individuell zugeschnittene Workshops u. a. zur Stärkung von Rollenverständnis, Führungsverhalten und Kommunikationsfähigkeit in Krisensituationen sowie zur Vertiefung spezifischer Bedarfsfelder.
- **VR-TrainingLab:** Praxisnahe Simulation in einer virtuellen Umgebung zur realitätsgetreuen Abbildung von Stress- und Entscheidungssituationen als innovativer, immersiver Trainingsansatz.

Vorteile eines integrativen Ansatzes beim Krisenmanagement

Generell ist hier eine regelmäßige Durchführung verschiedener Maßnahmen zu empfehlen, um eine kontinuierliche Weiterentwicklung der Resilienz sicherzustellen. Dies unterstützt insbesondere die regulatorische Anforderung nach regelmäßiger Überprüfung und Verbesserung der Maßnahmen (vgl. Art. 24 DORA).

Der Mehrwert eines integrierten Ansatzes liegt vor allem in der Stärkung der Handlungsfähigkeit im Krisenfall. Durch klar definierte Strukturen, trainierte Entscheidungsprozesse und etablierte Kommunikationswege können Reaktionszeiten verkürzt und Fehlentscheidungen

reduziert werden. Gleichzeitig wird die organisationsweite Koordination verbessert, was insbesondere bei bereichsübergreifenden Krisenlagen entscheidend ist.

Zudem ermöglicht ein solcher Ansatz die systematische Identifikation von Schwachstellen in Prozessen, Technologien und Organisationsstrukturen. Dies schafft die Grundlage für eine kontinuierliche Verbesserung und stärkt die langfristige Resilienz des Instituts.

Weiterhin wird durch die Implementierung strukturierter Übungen, umfassender Assessments und sorgfältiger Dokumentationen eine fundierte Grundlage für den Nachweis gegenüber Aufsichtsbehörden geschaffen. Die Anforderungen aus DORA sowie aus nationalen Regelwerken wie MaRisk und KWG können auf diese Weise nachvollziehbar adressiert werden. Im Rahmen der Implementierung von Maßnahmen gewinnt die Nachweisfähigkeit der Wirksamkeit zunehmend an Bedeutung.

Fazit

Zusammenfassend wird deutlich, dass modernes Krisenmanagement weit über die reine technische Absicherung und klassische Notfallkonzepte hinausgeht. Die regulatorischen Anforderungen, insbesondere durch DORA, erfordern eine ganzheitliche Betrachtung der operationellen Resilienz. Integrierte Ansätze, die technische Fähigkeiten mit organisatorischer Vorbereitung und gezielter Befähigung von Entscheidungsträgern verbinden, leisten dabei einen wesentlichen Beitrag zur Sicherstellung der Handlungsfähigkeit in zunehmend komplexen Krisenszenarien. ▬

Jacob Schirner
Consultant Informationssicherheit bei ATRUVIA, Schwerpunkt BCM
E-Mail: jacob.schirner@atruvia.de

Benjamin Wellnitz
Bereichsleiter IKT-Risikokontrolle, Informationssicherheit & Datenschutz,
E-Mail: benjamin.wellnitz@dz-cp.de