Penetrationtesting360 – Ihr Weg zu einer belastbaren digitalen Widerstandsfähigkeit

Mit Wirkung zum 17. Januar 2025 tritt der Digital Operational Resilience Act (DORA) in der europäischen Finanzbranche verbindlich in Kraft. Die Verordnung verpflichtet Finanzunternehmen sowie deren IT-Dienstleister dazu, ihre Betriebsstabilität systematisch zu prüfen – insbesondere durch ein risikoorientiertes Testprogramm für Cyberresilienz gemäß den Artikeln 24 bis 27.

Die Planung und Durchführung angemessener Penetrationstests stellt viele Institute vor große Herausforderungen. Die zunehmende Komplexität der IT-Landschaften sowie die strengen regulatorischen Anforderungen erfordern Testverfahren, die sowohl technisch fundiert als auch organisatorisch sauber verankert sind.

Effiziente Risikobewertung

Durch zeitnahe Identifikation und Schließung von Schwachstellen verbessern Sie die Sicherheit Ihres Systems.

Ganzheitliche Compliance

Erfüllen Sie die Anforderungen der Artikel 24 bis 27 der DORA, um regulatorische Compliance sicherzustellen.

Effektives Auditmanagement zur Risikominimierung

Durchführung interner und externer Audits zur Vermeidung von Prüfungsfeststellungen und zur Identifikation anlassbezogener sowie regelmäßiger Auditmaßnahmen.

IT

Ihre Herausforderungen

Sie stehen vor der Aufgabe, einen angemessenen Jahresprüfplan zu erstellen, der sich auf Schutzobjekte im Informationsverbund bezieht. Dieser Plan sollte die technische Überprüfung berücksichtigen und sicherstellen, dass die Objekte den erforderlichen Sicherheitsstandards entsprechen:

- Festlegung einer angemessenen Dauer für den Penetrationstest (Widerstandszeit)
- Festlegung und Definition der Parameter sowie der zugrundeliegenden Szenarien
- Auswertung und sachgerechte Interpretation des Penetrationstestberichts (Schlussbericht)
- Ableiten von angemessenen Maßnahmen zur Schließung bzw. Reduktion der identifizierten Schwachstellen

Unsere Lösungen

Wir erstellen einen Vorschlag für einen Jahresprüfplan, unter Berücksichtigung der Schutzobjekte und deren Kritikalität innerhalb Ihres Informationsverbundes. Dabei berücksichtigen wir Faktoren wie den Geschäftswert, die Auswirkungen auf den Betrieb und die Compliance-Anforderungen.

Auf dieser Grundlage priorisieren wir die Prüfaktivitäten. Gemeinsam mit Ihnen und Ihrem Penetrationsdienstleister erarbeiten wir auf Basis des Schutzobjekts und der jeweiligen aktuellen Bedrohungslage ein detailliertes, risikobasierendes Szenario. Gemeinsam identifizieren und bewerten wir die Risiken, die durch den Penetrationsdienstleister identifiziert wurden. Zudem zeigen wir Ihnen Wege auf, wie Sie gefundene Schwachstellen nachhaltig und praxistauglich schließen können.

Nach Abschluss der Prüfungen erstellen wir ein Management-Reporting. Dieses enthält eine Zusammenfassung der identifizierten Schwachstellen, ihrer Risiken und möglicher Auswirkungen.

Decken Sie mit unserem Expertenteam Sicherheitslücken auf, bevor sie zum Problem werden – setzen Sie auf das richtige Penetrationstest-Setting für maximale IT-Sicherheit!

AWADO GmbH
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft
Wilhelm-Haas-Platz
63263 Neu-Isenburg

Rocco D'Onofrio
Senior Manager

+49 175 6046690
rocco.donofrio@awado-gruppe.de

© AWADO GmbH Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft. Alle Rechte vorbehalten.

PB-231.260224.W01