HADRIAN

Checkliste zur DORA-Einhaltung

Bei der Navigation durch die dynamische Landschaft des Finanzsektors ist der Digital Operational Resilience Act (DORA) ein wichtiger Wegweiser, der den Weg zur operativen Resilienz von Unternehmen prägt. Um Ihre Organisation bei der Erreichung und Aufrechterhaltung der DORA-Konformität zu unterstützen, wurde diese umfassende Checkliste erstellt, die als strategischer Fahrplan dient.

Jedes Element ist so konzipiert, dass es Ihre Organisation durch die nuancierte Landschaft von DORA führt und nicht nur die Einhaltung der Vorschriften, sondern auch die Schaffung eines robusten und anpassungsfähigen Rahmens für die operative Widerstandsfähigkeit fördert.

Verständnis und Einhaltung der DORA-Vorschriften

- [ ] **Bestimmung der DORA-Zuständigkeit:** Stellen Sie fest, ob Ihre Organisation in den Geltungsbereich der DORA-Zuständigkeit fällt, und ermitteln Sie die spezifischen Anforderungen.
- [ ] **Entwicklung einer Resilienzstrategie:** Formulierung einer Strategie für die digitale betriebliche Widerstandsfähigkeit im Einklang mit den DORA-Vorschriften.
- [ ] **Regelmäßige Überprüfung der Anforderungen:** Halten Sie sich über die DORA-Anforderungen auf dem Laufenden und stellen Sie sicher, dass Sie diese stets verstehen und einhalten.

Risikobewertung und -management

- [ ] **Stärkung der Informationssicherheit:** Verstärkung der Maßnahmen zur Informationssicherheit, die Zugangskontrollen, Verschlüsselung, sichere Kodierung und Datenschutz umfassen.
- [ ] **Durchführen einer Risikobewertung:** Bewerten Sie potenzielle Risiken und Schwachstellen in Ihren IKT-Systemen und berücksichtigen Sie dabei interne und externe Bedrohungen.
- [ ] **Verwaltung des Risikos von Drittanbietern:** Bewertung von Drittanbietern hinsichtlich ihrer Belastbarkeit und Sicherheit in Übereinstimmung mit den DORA-Anforderungen.
- [ ] **Identifizierung und Sicherung von IKT-Vermögenswerten:** Umsetzung von Maßnahmen zur Identifizierung und Sicherung von IKT-Vermögenswerten gemäß den DORA-Vorschriften.
- [ ] **Nutzen Sie automatisierte Lösungen:** Einsatz automatisierter Lösungen und Erkennung von Bedrohungen für eine effiziente Risikoerkennung.
- [ ] **Setzen Sie Prioritäten bei den Abhilfemaßnahmen:** Konzentrieren Sie sich auf Abhilfemaßnahmen und bereiten Sie Nachweise für die Einhaltung der Vorschriften vor.
- [ ] **Externe Risiken überwachen:** Überwachen Sie externe Quellen auf potenzielle Risiken und tauschen Sie Informationen aus, um die Widerstandsfähigkeit zu erhöhen.
- [ ] **Schaffung eines IKT-Risikomanagement-Rahmens:** Schaffung eines IKT-Risikomanagement-Rahmens und Durchführung von Tests zur digitalen operativen Belastbarkeit.

Kultur und Führung

- [ ] **Förderung einer positiven Organisationskultur:** Sorgen Sie für eine positive Organisationskultur, die die Zusammenarbeit und die Widerstandsfähigkeit fördert
- [ ] **Priorisieren Sie die Sicherheitskultur:** Kultivieren Sie eine sicherheitsorientierte Unternehmenskultur durch Mitarbeiterschulung und -einbindung.
- [ ] **Befähigung von Führungskräften:** Befähigung der Führungskräfte durch entsprechende Schulungen zur effektiven Einhaltung der Vorschriften.
- [ ] **Ganzheitlicher Ansatz zur Einhaltung von Vorschriften:** Beziehen Sie mehrere Teams in die Zusammenarbeit ein, um einen ganzheitlichen Ansatz zur Einhaltung der Vorschriften zu erreichen.
- [ ] **Schulung und Sensibilisierung der Mitarbeiter:** Bieten Sie umfassende Schulungsprogramme an, um die Mitarbeiter über bewährte Praktiken im Bereich der Cybersicherheit und die Meldung von Vorfällen aufzuklären.

Prozess und Automatisierung

- [ ] **Implementierung von CI/CD und automatisierten Tests:** Wenden Sie Continuous Integration (CI), Continuous Deployment (CD) und automatisierte Tests für optimierte Prozesse an.
- [ ] **Plan zur Reaktion auf Zwischenfälle:** Entwickeln Sie einen detaillierten Reaktionsplan für die Erkennung von, die Reaktion auf und die Wiederherstellung nach Sicherheitsvorfällen.
- [ ] **Dokumentation und Aufzeichnungen:** Führen Sie detaillierte Aufzeichnungen über Risikobewertungen, Reaktionspläne auf Vorfälle und Maßnahmen zur Einhaltung der Vorschriften.
- [ ] **Penetrationstests:** Führen Sie regelmäßig Penetrationstests durch und nutzen Sie dabei Frameworks wie TIBER-EU.
- [ ] **Automatisieren Sie die Erkennung von Bedrohungen:** Automatisieren Sie die Erkennung von Bedrohungen mit Tools wie EDRs, XDRs, Scannern und SIEMs.

Architektur, Design und Verwaltung durch Dritte

- [ ] **Entwurf für Skalierbarkeit und Widerstandsfähigkeit:** Entwerfen Sie Systeme für Skalierbarkeit, Belastbarkeit und Wartungsfreundlichkeit.
- [ ] **Microservices-Architektur:** Implementieren Sie eine Microservices-Architektur und Containerisierung für einen effizienten Betrieb.
- [ ] **Überlegungen zu Drittanbietern:** Überprüfen Sie die Richtlinien zu IKT-Drittanbietern (CTPS) und berücksichtigen Sie die Vorschriften bei der Beauftragung von Drittanbietern.
- [ ] **Nutzen Sie Trainingsprogramme:** Nutzen Sie Tools wie das Schulungsprogramm von CybeReady, um Entwickler in die Lage zu versetzen, sichere Anwendungen zu entwickeln.

Überwachung, Messung und kontinuierliche Verbesserung

- [ ] **Festlegung von KPIs und Echtzeit-Überwachung:** Legen Sie wichtige Leistungsindikatoren (KPIs) fest und führen Sie eine Echtzeit-Überwachung ein.
- [ ] **Regelmäßige Überprüfung von Resilienzstrategien:** Regelmäßige Überprüfung und Aktualisierung der Resilienzstrategien und -politiken.

- [ ] **Analysieren Sie vergangene Vorfälle:** Analysieren Sie vergangene Vorfälle, berücksichtigen Sie die daraus gezogenen Lehren und wenden Sie Verbesserungen an.
- [ ] **Kontinuierliche Überwachung und Bewertung:** Implementieren Sie kontinuierliche Überwachungsprozesse, um aufkommende Risiken und Schwachstellen zu erkennen und umgehend darauf zu reagieren.
- [ ] **Interne Audits und Beurteilungen:** Führen Sie regelmäßig interne Audits und Bewertungen durch, um verbesserungswürdige Bereiche zu ermitteln und Lücken bei der Einhaltung der Vorschriften zu schließen.

Sicherheit und Rechtskonformität

- [ ] **Integrieren Sie Sicherheitspraktiken:** Integrieren Sie Sicherheitspraktiken in den Entwicklungslebenszyklus mit einem DevSecOps-Ansatz.
- [ ] **Durchführung von Sicherheitsprüfungen:** Führen Sie regelmäßig Sicherheitsaudits und Schwachstellenbewertungen durch, um den Datenschutz zu gewährleisten.
- [ ] **ISMS einführen:** Einrichtung eines Informationssicherheitsmanagementsystems (ISMS), das sich an internationalen Normen wie ISO 27001 orientiert.
- [ ] **Einhaltung rechtlicher Standards:** Gewährleisten Sie die Einhaltung von gesetzlichen, regulatorischen und branchenüblichen Standards, einschließlich GDPR.
- [ ] **Mit Regulierungsbehörden zusammenarbeiten:** Bleiben Sie auf dem Laufenden über Aktualisierungen der Vorschriften und führen Sie einen offenen Dialog mit den zuständigen Behörden, um die Einhaltung der Vorschriften zu verstehen.

Wie Hadrian helfen kann

Kontinuierlich

Hadrians Continuous Automated Red Teaming (CART) simuliert permanente, automatisierte Angriffe auf Ihr System, um Schwachstellen sofort zu erkennen und neue Bedrohungen schnell aufzuspüren.

Selbstständig

Hadrians KI-gesteuerte Sicherheitsplattform bewertet Ihre gesamte Angriffsfläche, deckt Schwachstellen von Dritten auf, bewertet Ausnutzungsrisiken, gibt Behebungsempfehlungen und sorgt für kontinuierliche Sicherheit.

Vollständig

Herkömmliche Compliance-Berichte liefern keine Echtzeit-Updates, wodurch Probleme oft zu spät erkannt werden. Hadrian bietet präzise Berichte, die den DORA-Anforderungen entsprechen und leicht weitergegeben werden können, sodass alle über die Einhaltung informiert bleiben.

Lesen Sie den Leitfaden zur Vorbereitung auf die Vorschriften zur digitalen Ausfallsicherheit.

Datenblatt herunterladen

Oder scannen Sie den QR-Code