HYCU®

Schritt für Schritt zur DORA-Konformität

Ihr Leitfaden zur Erfüllung der Anforderungen der EU-Verordnung in Bezug auf Geschäftskontinuität und die Widerstandsfähigkeit Ihres Unternehmens.

CHECKLISTE

01

Bevor wir beginnen...

DORA deckt ein breites Spektrum ab, von der Reaktion auf Zwischenfälle bis hin zur Abwehr von Bedrohungen. Was den Datenschutz anbelangt, so sind viele Unternehmen nicht darauf vorbereitet, die Anforderungen an die Geschäftskontinuität und Ausfallsicherheit zu erfüllen. Tatsächlich sind sich viele Unternehmen nicht einmal bewusst, dass sie für die Einhaltung der Vorschriften und den Datenschutz ihrer SaaS-Anwendungen selbst verantwortlich sind!

Um aber Ihre Verantwortung in Bezug auf SaaS- und Cloud-Daten besser zu verstehen, lesen Sie **das Modell der ‚Shared Responsability'**, indem Sie den QR-Code unten scannen.

Entdecken Sie das Model der 'Shared Responsibility' und vermeiden Sie kritische Fehler

Checkliste

Erfüllen Sie die DORA-Anforderungen für Backup, Disaster Recovery und digitale Ausfallsicherheit

Geschäftskontinuität, Datensicherung und Tests sind wichtige Anforderungen, die Sie mit DORA erfüllen müssen.

Wie viele Kästchen können Sie für Ihr Unternehmen heute abhaken?

Starten Sie! Risikobewertung

- [ ] Erstellen Sie einen Rahmen, um alle ICT-Services zu identifizieren und abzubilden (z. B. Atlassian Cloud, AWS, Salesforce, usw.)
- [ ] Nutzen oder erstellen Sie Audit-Vorlagen, um jede IT Technologie in Zusammenhang mit Sicherheit, Erkennung, Reaktion und Geschäftskontinuität zu bewerten.
- [ ] Bestimmen Sie Verantwortliche für den Datenschutz bei allen verwendeten SaaS-Anwendungen.
- [ ] Nutzen Sie Tools für die kontinuierliche Überwachung von verwendeten Technologien und dokumentieren Sie regelmäßig Änderungen in Ihrem Tech-Stack - über alle Abteilungen hinweg

Backup-Anforderungen

- [ ] Planen von täglichen Backups für jede Instanz und Anwendung in Ihrer Umgebung.
- [ ] Sicherstellen, dass Sicherungskopien im Falle eines Ausfalls oder einer Cyber-Bedrohung zugänglich sind.
- [ ] Festlegen einer Mindesthäufigkeit für die Backups pro Anwendung.
- [ ] Sicherstellen, dass das Sicherungssystem außerhalb der primären SaaS-Anwendungen läuft und von diesen getrennt ist.
- [ ] Speichern von Backups außerhalb des Unternehmens in einem S3-kompatiblen Speicher, unabhängig von den primären SaaS-Anwendungen.
- [ ] Aktivierung der Unveränderbarkeit des Backup-Speicherziels im Falle eines Cyber-Ereignisses.
- [ ] Der Standort des Backup-Speichers muss die Anforderungen des entsprechenden Landes erfüllen (falls es solche gibt).
- [ ] Implementierung und Aufrechterhaltung von Multi-Faktor-Authentifizierung, Verschlüsselung und Netzwerksegmentierung zum Schutz der Integrität und Vertraulichkeit von Backups.

Reaktion auf Vorfälle und Wiederherstellung

- [ ] Festlegen von Wiederherstellungs-SLAs, die der Bedeutung der jeweiligen Anwendung angemessen sind.
- [ ] Entwicklung und regelmäßige Aktualisierung von Notfallwiederherstellungsplänen, die Vorlagen für verschiedene Vorfallszenarien enthalten. Sicherstellen, dass diese Pläne umfassend und auf die Bedürfnisse des Unternehmens zugeschnitten sind.
- [ ] Durchführung regelmäßiger Schulungen und Simulationen, um die Effektivität der Mitarbeiter im „Incident Response“ Fall zu optimieren. Der Schwerpunkt liegt dabei auf klar definierten Rollen, Verantwortlichkeiten und Maßnahmen für ein effektives Störungsmanagement.

Nachvollziehbare Wiederherstellung und Berichterstattung

- [ ] Dokumentation und Aufzeichnung aller Prozesse, um die Einhaltung der DORA-Anforderungen nachzuweisen und sich für Audits und Inspektionen zu wappnen.
- [ ] Nutzen von fortschrittlichen Tools für die kontinuierliche Überwachung und Echtzeit-Berichterstattung von Sicherungs- und Wiederherstellungsaktivitäten, um die Entscheidungsfindung und die Reaktionsmöglichkeiten auf Vorfälle zu verbessern.

HYCU®

Übernehmen Sie die Kontrolle über Ihre Daten

Entdecken Sie Lücken in der DORA-Konformität und aktivieren Sie den Datenschutz mit diesem kostenlosen SaaS-Erkennungstool