Kiteworks

COMPLIANCE-INFORMATION

Kiteworks ermöglicht robuste regulatorische Compliance gemäß FINMA-Rundschreiben 2023/1 “Betriebliche Risiken und Resilienz – Banken”

Vereinheitlichter Schutz kritischer Daten und integrierte Kontrollen erleichtern die Erfüllung der Erwartungen der Schweizer Finanzaufsicht

Die FINMA ist die Schweizer Behörde, die Finanzinstitute in der Schweiz überwacht und reguliert. Ihr vollständiger Name lautet “Eidgenössische Finanzmarktaufsicht”. Banken, Wertpapierhändler, Finanzgruppen und Großkonzerne müssen die vollständige Einhaltung des “Rundschreiben 2023/1 Betriebliche Risiken und Resilienz – Banken” der FINMA sicherstellen, um erhebliche regulatorische, finanzielle und reputative Auswirkungen zu vermeiden. Die Nichteinhaltung der Vorschriften birgt erhebliche aufsichtsrechtliche Risiken, die die Stabilität und den Fortbestand eines Finanzinstituts bedrohen könnten. Verstöße können zu Zwangsmaßnahmen, Einschränkungen der Aktivitäten, Geldstrafen und sogar zum Verlust der Betriebslizenz führen. Angesichts komplexer Verflechtungen können Probleme bei einem Finanzinstitut schnell auf andere übergreifen und die Finanzmärkte stören. Daher räumen die Aufsichtsbehörden Schutzmaßnahmen wie den im Rundschreiben beschriebenen Maßnahmen zur betrieblichen Resilienz und Kontinuität Priorität ein. Während für kleinere Unternehmen einige proportionale Ausnahmen gelten, gibt es für betriebliche Risiken keine Größenbeschränkungen. Alle Banken und Wertpapierhändler müssen die Grundsätze anwenden, während globale/systemrelevante Finanzinstitute und Bankengruppen absolute Konformität und strenge Tests erwarten sollten. Für Banken die Privat- und Geschäftskredite vergeben, steht mehr auf dem Spiel, da operationelle Ausfälle unmittelbare Auswirkungen auf Kunden und Gegenparteien haben könnten. Die Reichweite dieses Rundschreibens erstreckt sich jedoch auf den gesamten Banken-, Handels- und Versicherungssektor und darüber hinaus. Kiteworks bietet folgendermaßen Unterstützung bei der Einhaltung der Vorgaben dieses Rundschreibens:

Operatives Risikomanagement mit mehrstufiger Sicherheit

Banken sind verpflichtet, operationelle Risiken zu kategorisieren, inhärente und verbleibende Risiken zu bewerten, zentrale Kontrollen und risikomindernde Maßnahmen zu implementieren, regelmäßige Risiko- und Kontrollbewertungen durchzuführen, Verluste und Indikatoren in Bezug auf die vom Vorstand festgelegte Risikotoleranz zu überwachen und der obersten Führungsebene Risikoberichte vorzulegen. Die gehärtete virtuelle Appliance und das aus mehreren Schichten bestehende Sicherheitsmodell von Kiteworks minimieren Angriffsflächen, um Betriebsunterbrechungen zu vermeiden. Die Zero-Trust-Architektur geht von einem Sicherheitsverstoß aus, isoliert Komponenten und die doppelte Verschlüsselung von Daten schützt unstrukturierte Daten. Umfassende Aktivitätsprotokolle verfolgen administrative Aktionen, Eindringversuche,

Highlights der Lösung

- **Granulare Zugriffskontrollen**
- **Detaillierte Aktivitätsprotokolle**
- **Zero-Trust-Architektur**
- **Konfigurierbare Geo-/IP-Beschränkungen**
- **Integration externer Parteien**

Anomalien und Benutzeraktivitäten für jede Datei und Systemkomponente. Die Protokolle werden in SIEM-Systeme eingespeist, um schnelle Compliance-Audits, Sicherheitsforensik und die Bekämpfung laufender Bedrohungen zu ermöglichen. Granulare Richtlinien steuern den IP- und Datenzugriff. Authentifizierungsoptionen umfassen MFA und SSO zur Zugriffskontrolle und sind auf die niedrigsten Berechtigungen ausgelegt. Diese Funktionen helfen Schweizer Finanzinstituten bei der Umsetzung der wichtigsten FINMA-Anforderungen in Bezug auf Resilienz, Geschäftskontinuität, Sicherheit und Compliance von Bankensystemen und -prozessen.

Implementierung und Durchsetzung des IKT-Risikomanagements

Institutionen müssen IT-Governance-Verfahren und Change-Management-Prozesse implementieren, Bestandslisten und Kontinuitätspläne für IKT-Assets (Informations- & Kommunikationstechnologie) und -Betrieb pflegen, Entwicklungs-/Testumgebungen einschränken, Systemanforderungen validieren und Fähigkeiten zur Reaktion auf größere IT-Ausfälle oder Cyber-Vorfälle etablieren. Kiteworks protokolliert alle System- und Benutzeraktivitäten für Sicherheitsüberwachung, die Reaktion auf Vorfälle (Incident Response) und Audits. Die gehärtete virtuelle Appliance minimiert Angriffsflächen durch eingebettete Firewalls, Web-App-Firewalls und Intrusion Detection. Automatisierte Penetrationstests und Bug Bountys stellen sicher, dass Schwachstellen schnell gefunden und behoben werden. Ein-Klick-Cluster-Updates sorgen für schlüsselfertige Patches. Diese Vorgehensweisen erfüllen die Erwartungen der FINMA im Hinblick auf die IKT-Governance und die operative Resilienz innerhalb des Finanzsektors.

Schnelle Berichterstattung für das Cyber-Risikomanagement

Banken benötigen Bedrohungsanalysen, Daten- und Systemschutz sowie Erkennungs- und Reaktionsfähigkeit gemäß internationalen Cybersecurity-Standards. Sie müssen wesentliche Angriffe innerhalb von 72 Stunden an die FINMA melden, regelmäßig Schwachstellentests und Szenarioübungen durchführen und die durch Tests aufgedeckten Lücken analysieren und beheben. Kiteworks ist durch Schichten wie eingebettete Firewalls, Web-App-Firewalls, IP-Blocking und ein Intrusion-Detection-System gehärtet. Sandboxing isoliert Softwarekomponenten, während Verschlüsselung und Zugriffskontrollen den Zugriff auf Daten und Systeme einschränken. Konfigurierbare Cyber-Bedrohungsdaten können in das SIEM-Monitoring integriert werden. Zusammen unterstützen diese Funktionen die Umsetzung der Anforderungen der FINMA bezüglich Identifikation, Schutz, Erkennung, Reaktion und Management von Cyber-Risiken in Schweizer Finanzinstituten.

Konsistenter Schutz für das Risikomanagement kritischer Daten

Finanzinstitute müssen einen Rahmen schaffen, um sensible Daten nach ihrer Kritikalität zu klassifizieren, den Zugriff durch Autorisierungs- und Überwachungssysteme einzuschränken, vertrauenswürdige Dienstleister auszuwählen, erhöhte Sicherheitsmaßnahmen für Verfügbarkeit/Integrität/Vertraulichkeit für ausgelagerte und übertragene Datensätze basierend auf Datensensibilität und Standortrisiken zu implementieren und Vorfälle zu melden, die die Integrität kritischer Daten verletzen. Die Enterprise-Connect-Integration von Kiteworks vereint unstrukturierte Daten unter einer zentralen Datenverwaltung. Richtlinien klassifizieren die Sensibilität, Verschlüsselung sichert Daten und granulare Berechtigungen steuern den Zugriff über integrierte Repositorys wie SharePoint und Dropbox. Die Nachverfolgung protokolliert Benutzeraktivitäten in diesem vereinheitlichten Ökosystem, um konsolidierte Audit-Trails zur Nachweisführung der Compliance zu erstellen. Die Plattform ermöglicht einen konsistenten Schutz kritischer Daten und eine einheitliche Übersicht über die Systeme der jeweiligen Schweizer Bank und reduziert gleichzeitig Risiken, die sich aus fragmentierten Sicherheitsmodellen ergeben. Rollenbeschränkungen, die Erkennung von Anomalien und Zugriffskontrollen über die Systeme externer Parteien hinweg, tragen dazu bei, die FINMA-Anforderungen zum Schutz sensibler Finanzdaten und zur Erkennung von unberechtigten Zugriffsversuchen zu erfüllen.

Zentralisiertes Risikomanagement über Grenzen hinweg

Die Finanzinstitute müssen die Risiken bei grenzüberschreitenden Geschäften gründlich bewerten, die notwendige Maßnahmen zur Bewältigung ausländischer rechtlicher/regulatorischer Risiken ergreifen, länderspezifisches Fachwissen gewährleisten und bei der Beauftragung externer Parteien, die Offshore-Dienstleistungen erbringen, Sorgfalt walten lassen. Kiteworks ermöglicht eine zentralisierte Verwaltung von schweizerischen Bankdaten, die im Ausland genutzt werden. Konfigurierbare IP- sowie länderspezifische und geografische Zugriffsbeschränkungen kontrollieren den grenzüberschreitenden Datenfluss auf Grundlage der Benutzerrolle und der Sensibilität des Inhalts. Rechtliche Schutzmechanismen verschlüsseln die Daten in On-Premises und Cloud-Repositorys sowie während der Übertragung. Detaillierte Aktivitätsprotokolle bieten Audit-Trails, die sich über integrierte globale Systeme erstrecken, um die Compliance nachzuweisen. Zusammen unterstützen diese grenzüberschreitenden Kontrollen die Anforderungen der FINMA, um die Risiken von Offshore-Diensten zu bewerten, die Schweizer Vertraulichkeitsbestimmungen außerhalb des Territoriums durchzusetzen, die Einhaltung der gesetzlichen Bestimmungen nachzuweisen und das Risiko ausländischer rechtlicher und regulatorischer Regelungen zu begrenzen.

Kiteworks bietet integrierte Sicherheit für unstrukturierte Daten, Governance und Kontrolle, die für die Einhaltung der gesetzlichen Anforderungen der FINMA unerlässlich sind. Die auf Resilienz ausgerichtete Architektur, Verschlüsselung, Zugriffskontrollen und Aktivitätsverfolgung setzen die Erwartungen in Bezug auf operative Risiken, IKT-, Cyber- und Datensicherheit um. Die Plattform überbrückt unterschiedliche Umgebungen, um zentralisierte Richtlinien, integrierte Audits/Forensik und schnelle, schlüsselfertige Patches zu ermöglichen. Konfigurierbare IP-, Länder- und Systemzugriffsbeschränkungen unterstützen die Anwendung der Schweizer Vertraulichkeitsregeln im Ausland. Zusammen reduzieren diese vereinheitlichten Funktionen die Compliance-Kosten für Finanzinstitute, indem sie die Sicherheit konsolidieren, fragmentierte Tools und Kontrollen eliminieren und gleichzeitig die Stabilität der Banken und die Datenhoheit der Verbraucher stärken.