Kiteworks

COMPLIANCE BRIEF

Kiteworks Europe AG erhält BSI Cloud Computing Compliance Criteria Catalogue Attestation für regulierte Branchen in Deutschland

Erfüllung der strengsten Sicherheitsanforderungen für Cloud-Betrieb in Finanzwesen, Gesundheitswesen und öffentlichem Sektor

Der BSI Cloud Computing Compliance Criteria Catalogue (C5) definiert empfohlene und branchenspezifisch vorgeschriebene Sicherheitsanforderungen für Cloud Service Provider (CSPs), die in Deutschland tätig sind und deutsche Kunden bedienen – insbesondere in regulierten Sektoren wie Gesundheitswesen, öffentlicher Sektor und Finanzdienstleistungen. Entwickelt vom Bundesamt für Sicherheit in der Informationstechnik (BSI), umfasst C5:2020 insgesamt 121 Kriterien in 17 Bereichen, die kritische Sicherheitsaspekte wie Identitätsmanagement und Incident Response abdecken. Cloud Service Provider weisen ihre Compliance derzeit durch unabhängige Typ-2-Audits nach. Die **aktualisierte Version C5:2025** wird voraussichtlich **2026 finalisiert** und soll ab **2027 verpflichtend** gelten. Wer keinen CSP mit C5-Attestation nutzt, riskiert den Ausschluss von regulierten Ausschreibungen (z. B. Gesundheitswesen, öffentlicher Sektor), Vertrauensverlust bei Kunden, Reputationsschäden sowie indirekte rechtliche und finanzielle Risiken durch zugrundeliegende Vorgaben wie die DSGVO. Die Kiteworks Europe AG hat nun einen bedeutenden Compliance-Meilenstein erreicht: Am 19. Dezember 2025 erhielt sie die BSI C5-Attestation durch unabhängige Prüfung der HKKG GmbH und beweist damit, dass die Plattform eines der anspruchsvollsten Cloud-Sicherheitsframeworks Europas erfüllt.

Grundlegende organisatorische Sicherheit

BSI C5 verlangt von Unternehmen die Einführung umfassender Informationssicherheits-Managementsysteme (ISMS) mit klaren Richtlinien, Personalkontrollen und Asset Management über den gesamten Datenlebenszyklus. Diese grundlegenden Bereiche gewährleisten konsistente Sicherheitspraktiken, das Bewusstsein der Mitarbeitenden für ihre Sicherheitsverantwortung und den systematischen Schutz von Unternehmenswerten von der Erstellung bis zur Löschung. Kiteworks erfüllt diese Anforderungen durch eine umfassende Audit-Protokollierung, die sämtliche Nutzer- und Systemaktivitäten in einem zentralen Log erfasst und so die ISMS-Dokumentation und Richtliniendurchsetzung unterstützt. Die rollenbasierte Zugriffskontrolle mit acht vordefinierten Administratorrollen ermöglicht eine klare Aufgaben- und Verantwortungszuweisung. Das Asset Management erfolgt durch automatisierte Nachverfolgung aller Datenbewegungen, Dateiversionierung und konfigurierbare Aufbewahrungsrichtlinien für die Steuerung von Dateiablauf und -löschung. Das System speichert detaillierte Metadaten für jede Datei und jeden Ordner und bietet vollständige Transparenz über den gesamten Lebenszyklus. Nutzerprofile erzwingen konsistente Sicherheitsrichtlinien im gesamten Unternehmen, während das Risky Settings Dashboard Administratoren auf Abweichungen von sicheren Voreinstellungen hinweist.

Solution Highlights

- **Umfassende Audit-Protokollierung**
- **Gehärtete virtuelle Appliance-Architektur**
- **Unterstützung von Multi-Faktor-Authentifizierung**
- **Doppelte Verschlüsselung mit kundeneigenen Schlüsseln**
- **Automatisiertes Reporting**
- **DevSecOps-Implementierung**

Betriebliche Sicherheitskontrollen zur Unterstützung von Betrieb sowie Identitäts- und Zugriffsmanagement

Die operativen Sicherheitsanforderungen des **BSI C5** verlangen einen ordnungsgemäßen Systembetrieb (u. a. **Schwachstellenmanagement** und **Protokollierung**) sowie ein sicheres **Identitäts- und Zugriffsmanagement (IAM)** mit **starker Authentifizierung** für privilegierte Nutzer. Ziel ist, Systeme durch **Kapazitätsplanung, Malware-Schutz** und **kontrollierten Zugriff** auf sensible Ressourcen dauerhaft abzusichern. Kiteworks setzt diese Anforderungen mit einer gehärteten virtuellen Appliance-Architektur um, die integrierte Netzwerk- und Web Application Firewalls zum Schutz vor unbefugtem Zugriff bietet. Die Plattform gewährleistet umfassendes Schwachstellenmanagement durch kontinuierliche Penetrationstests, automatisierte Sicherheitsupdates und integrierte Intrusion Detection Systeme. Die Identitäts- und Zugriffsverwaltung umfasst Multi-Faktor-Authentifizierung via RADIUS, PIV/CAC-Karten, SMS-basiertem OTP sowie zeitbasiertem OTP mit Unterstützung für Google Authenticator und Microsoft Authenticator. Die Integration mit LDAP, Active Directory, SAML 2.0 und zertifikatsbasierter Authentifizierung ermöglicht zentrales Identitätsmanagement. Das System setzt Least-Privilege-Standards mit granularen Berechtigungen für Ordner und Dateien durch und hält vollständige Audit-Trails aller Authentifizierungsversuche und Zugriffsereignisse vor.

Schutz von Daten und Stärkung der Kundensouveränität über Informationen

Die technischen Schutzmaßnahmen des BSI C5 verlangen robuste Kryptografie für Vertraulichkeit und Integrität, sichere Netzwerkkommunikation für den Schutz von Informationen während der Übertragung sowie Funktionen zur Datenportabilität, einschließlich Datenabruf bei Vertragsende und sicherer Löschung. Diese Bereiche stellen sicher, dass Daten in allen Zuständen geschützt bleiben und Kunden die Kontrolle über ihre Informationen behalten. Kiteworks implementiert doppelte Verschlüsselung für ruhende Daten durch separate Datei- und Festplattenverschlüsselung mit kundeneigenen Schlüsseln. Für die Verschlüsselung während der Übertragung nutzt die Plattform standardmäßig TLS 1.3 und 1.2 mit AES-256. Zu den Kommunikationssicherheitsfunktionen zählen Netzwerksegmentierung für Kundendatenverkehr, DDoS-Schutz und gestufte interne Dienste nach zero trust-Prinzipien. Datenportabilität wird durch umfassende Exportfunktionen via API und Massendownloads gewährleistet. Die Plattform bietet sichere Datenlöschung, die eine Wiederherstellung verhindert, mit konfigurierbaren Aufbewahrungs- und Karenzzeiten für gelöschte Dateien. Die Integration von Hardware Security Modules wie SafeNet Luna und AWS KMS ermöglicht externes Schlüsselmanagement.

Unterstützung von Resilienz und schneller Reaktion auf Störungen

Sichere Entwicklungspraktiken sind erforderlich, einschließlich getrennter Umgebungen, Third-Party-Risikomanagement mit Monitoring, effektives Incident Response Management mit Kundenbenachrichtigung sowie Business Continuity Planning mit definierten Wiederherstellungszielen. Diese Bereiche gewährleisten Resilienz gegenüber Störungen und eine schnelle Reaktion auf Sicherheitsvorfälle. Kiteworks folgt umfassenden DevSecOps-Praktiken unter Einbeziehung von OWASP-Methoden, CWE-Katalogisierung und CVSS v3-Bewertung im gesamten Entwicklungsprozess. Die Plattform trennt Entwicklungs-, Test- und Produktionsumgebungen vollständig, wobei ein dediziertes Sicherheitsteam Releases freigibt. Das Third-Party-Risikomanagement umfasst die automatisierte Nachverfolgung aller Open-Source-Komponenten mit CVE-Dokumentation in den Release Notes. Das Security Incident Management bietet Echtzeit-SIEM-Integration via Syslog und Splunk Universal Forwarder mit sofortigen Alarmmeldungen an Administratoren. Business Continuity umfasst Hochverfügbarkeits-Cluster, automatisierte Failover-Konfigurationen, One-Click-Updates für schnelle Patches und den Node Migration Wizard für das Infrastrukturmanagement. Das System unterstützt konfigurierbare RTO- und RPO-Ziele durch replizierte Datenspeicherung und umfassende Backup-Mechanismen.

Erfüllung regulatorischer Vorgaben und Erhalt des Kundenvertrauens durch Transparenz

Die Compliance-Bereiche des BSI C5 verlangen die Identifikation rechtlicher Anforderungen wie der DSGVO, transparente Bearbeitung von Ermittlungsanfragen staatlicher Stellen mit Kundenbenachrichtigung, sofern zulässig, sowie sichere Produktkonfigurationen mit Schwachstellenscans und verpflichtender Multi-Faktor-Authentifizierung. Diese Kriterien gewährleisten die Einhaltung gesetzlicher Vorgaben und stärken das Kundenvertrauen durch Transparenz. Kiteworks bietet dediziertes Compliance-Reporting für DSGVO, HIPAA und CMMC 2.0 mit automatisierter Kontrollbewertung und Gap-

Analyse. Das Audit-Log der Plattform konsolidiert alle Systemaktivitäten als Nachweis für regulatorische Prüfungen, während spezialisierte Dashboards Compliance-Beauftragten die Überwachung der Einhaltung spezifischer Vorgaben ermöglichen. Die Bearbeitung von Ermittlungsanfragen umfasst detaillierte Protokollierung aller behördlichen Anfragen mit automatischer Kundenbenachrichtigung, sofern gesetzlich nicht untersagt. Zu den Produktsicherheitsfunktionen zählen integrierte AV-Scans, Anbindung an Advanced Threat Protection Systeme, kontinuierliche Schwachstellenscans mittels SAST- und DAST-Methoden sowie verpflichtende MFA für den administrativen Zugriff. Die Plattform unterzieht sich jährlichen externen Penetrationstests, deren Ergebnisse in Sicherheitsverbesserungen einfließen. SafeVIEW- und SafeEDIT-Funktionen gewährleisten sicheren Datenzugriff unter Einhaltung von Anzeige- und Bearbeitungsbeschränkungen.

Die erfolgreiche BSI C5-Attestation von Kiteworks unterstreicht die umfassende Ausrichtung der Plattform an Deutschlands strengen Cloud-Sicherheitsanforderungen für regulierte Branchen. Die Plattform deckt alle 17 BSI-Domänen durch eine integrierte Sicherheitsarchitektur ab, die präventive Kontrollen, kontinuierliches Monitoring und automatisierte Compliance-Funktionen vereint. Mit Defense-in-Depth-Strategien von der gehärteten virtuellen Appliance bis zu anwendungsseitigen Kontrollen ermöglicht Kiteworks Unternehmen, Sicherheit zu gewährleisten und gleichzeitig notwendige Datenzusammenarbeit zu ermöglichen. Die zentrale Audit-Protokollierung, automatisiertes Compliance-Reporting und zentrale Richtlinienverwaltung vereinfachen die komplexe Aufgabe, kontinuierliche Compliance gegenüber Prüfern und Aufsichtsbehörden nachzuweisen. Während Unternehmen sich auf die verschärften Anforderungen von C5:2025 vorbereiten, positionieren die bestehenden Funktionen von Kiteworks in Container-Management, Supply Chain Security und Datensouveränität Kunden optimal, um künftige Standards zu erfüllen, operative Effizienz zu wahren und sensible Daten in der gesamten Datenkommunikationsinfrastruktur zu schützen.