Kiteworks

COMPLIANCE-INFORMATION

Cyberrisiken reduzieren mit Kiteworks und der NIS 2-Richtlinie

Für Grundversorger und Online-Marktplätze: Sichere Inhalte und NIS 2-Compliance

Die Europäische Union (EU) hat die NIS 2-Richtlinie vorgeschlagen, ein EU-weites Regelwerk für den Umgang mit Risiken der Informations- und Kommunikationstechnologie (IKT) sowie Cyberbedrohungen im Bereich der Grundversorgung und Online-Marktplätze. Durch die Bereitstellung einer einzigen Plattform für den Schutz und die Verwaltung von Kommunikationsinhalten reduziert Kiteworks die Komplexität und bietet gleichzeitig Transparenz, damit Unternehmen die Einhaltung der NIS 2-Richtlinie nachweisen können.

Die vorgeschlagene Verordnung würde Finanzunternehmen dazu verpflichten, die Sicherheit ihrer IKT-Systeme und -Netzwerke zu gewährleisten und größere Zwischenfälle den zuständigen Behörden zu melden. Außerdem soll ein koordinierter EU-weiter Ansatz für die Cybersicherheit und die Reaktion auf Sicherheitsvorfälle eingeführt werden, wobei die zuständigen nationalen Behörden für die Überwachung und Durchsetzung verantwortlich sind. NIS 2 wird für EU-Unternehmen mit mehr als 50 Mitarbeitern und einem Jahresumsatz von mehr als 10 Millionen US-Dollar sowie für alle Unternehmen gelten, die bereits unter die bestehende NIS-Richtlinie fallen. Kiteworks und ein von Kiteworks unterstütztes Private Content Network, das vor Ort, in der Cloud oder als hybride Lösung eingesetzt werden kann, unterstützen Sie direkt dabei, Ihre sensiblen Datei- und E-Mail-Daten, die Sie intern und extern kommunizieren, gesetzeskonform zu schützen. So funktioniert's:

Durchsetzung der Einhaltung von Richtlinien zur Sicherheit von Informationssystemen

Kiteworks ermöglicht seinen Kunden die Standardisierung von Sicherheitsrichtlinien unter anderem für E-Mail, File-Sharing, mobile Geräte, MFT und SFTP mit der Möglichkeit, granulare Richtlinienkontrollen zum Schutz der Daten anzuwenden. Administratoren können rollenbasierte Berechtigungen für externe Anwender definieren und so die Einhaltung von NIS 2 über alle Kommunikationskanäle hinweg durchsetzen.

Effizientes Management von Sicherheitsvorfällen

Die Erkennung von Anomalien ermöglicht einen sofortigen Überblick über nicht autorisierte Zugriffe. Die KI-Technologie erkennt verdächtige Ereignisse, z. B. eine mögliche Exfiltration, und sendet eine Warnung per E-Mail und Audit-Protokolle. Durch die unveränderlichen Audit-Protokolle der Plattform können Unternehmen darauf vertrauen, dass Angriffe früher erkannt werden und die korrekte Beweiskette für forensische Untersuchungen erhalten bleibt. Dies ermöglicht eine effiziente und fristgerechte Meldung von Datenschutzverletzungen an das Computer Security Incident Response Team (CSIRT) oder, falls erforderlich, an die Europäische Agentur für Cybersicherheit (ENISA) gemäß der Richtlinie.

Unterstützung der Geschäftskontinuität mit integriertem Disaster Recovery von Kiteworks

Durch die genaue Protokollierung aller Aktivitäten und technischen Daten mit benutzerfreundlichen Tracking-Anzeigen erfüllen Audit-Protokolle einen doppelten Zweck: Sie ermöglichen einem Unternehmen, Datenschutzverletzungen zu untersuchen und sie dienen bei Audits als Nachweis der Compliance. Im Falle einer Datenschutzverletzung kann das Unternehmen genau sehen, was exfiltriert wurde, so dass es sofort mit der Wiederherstellung der Daten beginnen und das Tagesgeschäft fortsetzen kann, ohne die Compliance zu gefährden.

Schwachstellenmanagement in Entwicklung und Instandhaltung

Kiteworks wendet einen strikten Lifecycle für sichere Softwareentwicklung an, einschließlich umfangreicher Security Code Reviews, regelmäßiger Penetrationstests und eines Bounty-Programms zum Schutz Ihrer Daten. Eine eingebettete Netzwerk-Firewall und WAF, Zero-Trust-Zugriff und eine minimierte Angriffsfläche reduzieren das Sicherheitsrisiko erheblich. Kiteworks bietet seinen Kunden auch One-Click-Updates an, die auf Kompatibilität mit anderen Systemkomponenten getestet wurden, was zeitnahe Patches für das Betriebssystem, Datenbanken und Open-Source-Bibliotheken ermöglicht.

Definition und Umsetzung grundlegender Cyberhygieneverfahren

Kiterworks wurde von der ISO validiert, um Ihre sensiblen Inhalte effektiv vor Cyberrisiken zu schützen (ISO 27001), auch wenn sie als Cloud-Service bereitgestellt werden (ISO 27017), und um Ihr Unternehmen vor dem Verlust personenbezogener Daten zu schützen (ISO 27018). Darüber hinaus verfügt Kiteworks über eine Reihe von Compliance-Zertifizierungen, darunter die SOC-2-Compliance und SOC-2-Zertifizierung. Diese Zertifizierungen, zusammen mit der Single-Tenant-Architektur und der Multi-Layer-Sicherheit, bestätigen, dass Kiteworks mit seinem Content Management System in der Lage ist, Ihr Content-Risiko zu minimieren und Ihre grundlegenden Verfahren zur Cyberhygiene NIS 2-konform zu machen.

Schutz von Inhalten durch Verschlüsselung

Stellen Sie die Verschlüsselung aller Inhalte auf Volume- und Dateiebene im ruhenden Zustand (mit AES-256-Verschlüsselung) und die TLS-Verschlüsselung bei der Übertragung sicher, um Inhalte vor unbefugtem Zugriff, Datenkorruption und Malware zu schützen. Die flexible Verschlüsselung ermöglicht es Ihnen, die Ende-zu-Ende-Verschlüsselung von Kiteworks zu nutzen und eine Brücke zu Partnern mit verschiedenen Standards wie OpenPGP, S/MIME und TLS zu schlagen. Die E-Mail-Sicherheit von Kiteworks bietet Verschlüsselung und einheitliche Sicherheitskontrollen mit einem E-Mail Protection Gateway, das sicherstellt, dass nur authentifizierte Anwender Nachrichten lesen können.

Festlegen von Richtlinien für Zugangskontrolle und Asset Management

Kiteworks-Administratoren richten granulare Kontrollen zum Schutz sensibler Inhalte und zur Durchsetzung von Compliance-Richtlinien ein und ermöglichen Unternehmensinhabern die einfache Verwaltung von Inhalten, Ordnern, Einladungen und Zugriffskontrollen, um die NIS 2-Konformität aller Inhalte sicherzustellen. Die richtlinienkonforme Zugriffskontrolle kann zusätzlich mit Geofencing, App-Aktivierung, Dateityp-Filterung und der Kontrolle der E-Mail-Weiterleitung erweitert werden.

Verifizierung der Benutzer mit Hilfe einer Multi-Faktor-Authentifizierung

Anwendung granularer MFA- und SSO-Richtlinien für Rollen und Standorte unter Verwendung von RADIUS, SAML 2.0, Kerberos, Authentifizierungsanwendungen, PIV/CAC, SMS und dergleichen.

März 2023

www.kiteworks.com