Sicherheit von Adobe Document Cloud

Unternehmen auf der ganzen Welt vertrauen bei der Transformation von Dokumentenprozessen auf Adobe Document Cloud. Herausragende digitale Erlebnisse steigern die Kundenzufriedenheit, beschleunigen Geschäftsprozesse und bringen Wettbewerbsvorteile. Lösungen von Document Cloud lassen sich in bestehende Unternehmenssysteme und Business-Applikationen einbinden. Sie umfassen Adobe Sign und Acrobat DC, Apps und Web-Applikationen, flexible APIs sowie schlüsselfertige Integrationen. Mit Document Cloud können sämtliche Abteilungen Ihrer Organisation operative Abläufe optimieren, das Fehlerrisiko reduzieren und intuitive, vollständig digitale Erlebnisse erstellen.

Bei Adobe ist der Sicherheitsaspekt fester Bestandteil der Unternehmenskultur, Software-Entwicklung und Service-Prozesse. Document Cloud nutzt branchenübliche Sicherheitsverfahren zur Authentifizierung sowie zur Wahrung der Vertraulichkeit von Daten und Integrität von Dokumenten. Ein umfassendes Netzwerk an Technologien, Experten und strategischen Partnerschaften sorgt für den effektiven Schutz Ihrer Daten unter Einhaltung führender Sicherheitsstandards. Erweiterte Workflows, einfache Lizenzverwaltung und eine zuverlässige Cloud-Infrastruktur ermöglichen es Ihrer Organisation, bestehende Prozesse flexibel an neue IT- und Marktanforderungen anzupassen.

Sicherheit an erster Stelle

Adobe nimmt die Sicherheit Ihrer digitalen Inhalte ernst. Alle Produkte, Systeme und Prozesse werden von Adobe kontinuierlich überwacht und laufend optimiert, um den steigenden Ansprüchen und Herausforderungen zum Thema Sicherheit und Datenschutz gerecht zu werden. Die Dienste von Document Cloud, darunter *Adobe Sign* und PDF-Dienste, unterliegen strengen Richtlinien, um die Vertraulichkeit, Integrität und Verfügbarkeit von Dokumenten sicherzustellen. Document Cloud-Daten werden in mehreren geografisch verteilten Rechenzentren gehostet und von Amazon Web Services (AWS) verwaltet, Adobes verlässlichem Partner. In jedem AWS-Rechenzentrum kommen hochmoderne Zugriffskontrollen zur Gewährleistung der physischen Sicherheit und Umgebungssicherung zum Einsatz. Weitere Informationen zu diesem Thema finden Sie unter *https://aws.amazon.com/de/security*.

Im Rahmen des SPLC-Programms (Secure Product Lifecycle) werden zudem zahlreiche Sicherheitsmaßnahmen in den Bereichen Software-Entwicklung, Prozesse und Werkzeuge umgesetzt. SPLC ist in vielen Phasen des Produktlebenszyklus von Document Cloud fest verankert. Für den Schutz auf der physischen Ebene haben wir ein grundlegendes Regelwerk für Sicherheitsprozesse und die Kontrolle unserer Infrastruktur, Applikationen und Dienste implementiert. Weitere Informationen zu den Sicherheitsprozessen und dem Engagement von Adobe innerhalb der Community für IT-Sicherheit sowie dem Adobe Secure Product Lifecycle (SPLC) finden Sie unter *www.adobe.com/de/security.*

Wiederherstellung nach Ausfall

Adobe arbeitet kontinuierlich daran, dass die Prozesse seiner Kunden nicht durch ungeplante Ausfälle beeinträchtigt werden. Sollte es dennoch zu einem Ausfall kommen, hat die schnellstmögliche Wiederherstellung des Zugriffs auf die Dienste von Document Cloud oberste Priorität. Alle Rechenzentren sind so konzipiert, dass System- oder Hardware-Ausfälle für den Kunden lediglich minimale Auswirkungen zur Folge hätten.

Umgebungssicherung

Die Datenzentren von Document Cloud sind mit Sensoren ausgerüstet, die Gefährdungen durch Umwelteinflüsse erkennen, sowie mit Klimaanlagen, mit deren Hilfe die Betriebstemperatur und Luftfeuchtigkeit konstant gehalten werden. Dabei werden die Vorgaben gemäß Sicherheitsstandard SOC 2 Type 2 erfüllt.

Verschlüsselung und Schutz von Daten

Bei der Entwicklung von Adobe-Produkten und -Diensten – einschließlich Document Cloud – steht Datenschutz an erster Stelle. Im Ruhemodus werden Dokumente und Dateien mit dem Standard 256-Bit-AES verschlüsselt, der vom amerikanischen National Institute of Standards and Technology (NIST) festgelegt wurde. Um die sichere Datenübertragung zu gewährleisten, wird HTTP (Hypertext Transfer Protocol) in Verbindung mit TLS-Verschlüsselung (Transport Layer Security) unterstützt.

Der Zugriff auf Kundendaten für bestimmte Geschäfts- und Support-Aktivitäten ist auf bestimmte Document Cloud-Mitarbeiter und autorisierte Partner beschränkt. Adobe bietet keiner Behörde direkten oder systematischen Zugriff auf gespeicherte Kundendaten. Weitere Informationen zu Adobes Richtlinien für Datenschutz finden Sie unter *www.adobe.com/de/privacy*.

Erkennung von Angriffen und Systemüberwachung

Angesichts wachsender und immer komplexerer Bedrohungen verfügt Document Cloud über verschiedene Überwachungssysteme, die das Netzwerk im Hinblick auf Sicherheitsverletzungen, Denial-of-Service-Angriffe, IP-Spoofing, Port-Scanning und andere hochentwickelte Angriffsmethoden analysieren. Die Adobe-Teams für Betriebssicherheit setzen eine Reihe von Überwachungskriterien zur Definition der kritischen Standards für Sicherheit und Verfügbarkeit der Produktionsumgebungen für Adobe-Dienste ein. Zusätzlich kommen Überwachungslösungen von Drittanbietern zum Einsatz, die eine engmaschige Kontrolle von Aktivitätsspitzen oberhalb der definierten Schwellenwerte ermöglichen. Die Teams setzen an kritischen Punkten des Netzwerks IDS-Sensoren (Intrusion Detection System) ein. Diese erkennen nicht autorisierte Zugriffsversuche auf das Netzwerk und alarmieren umgehend das zuständige Sicherheits-Team. Mitarbeiter, die für den laufenden Betrieb von Document Cloud verantwortlich sind, überwachen zudem kontinuierlich Protokolle zu sensiblen Prozessen. Das System wird in regelmäßigen Intervallen überprüft, um sicherzustellen, dass kein unberechtigter Zugriff auf wichtige Komponenten stattgefunden hat.

Adobe strebt durch bestmögliche Automatisierung von Prozessen und die damit verbundene geringere Fehlerquote nach mehr Effizienz, Konsistenz und Wiederholbarkeit. Dieses Konzept wird in zahlreichen Bereichen vorangetrieben, wie bei der Verwaltung von Konfigurationen und Sicherheits-Patches, bei Erstellung und Hardening von Basis-Images sowie bei der Systemüberwachung. Adobe verfolgt einen umfassenden Prozess für Änderungs-Management, durch den Änderungen an Netzwerken oder der Produktionsumgebung von Document Cloud vor einer Übernahme für die Produktion lückenlos dokumentiert, nachverfolgt, getestet, autorisiert und schließlich genehmigt werden.

Wenn ein Sicherheitsproblem auftritt, werden für Cloud-basierte Dienste von Adobe wie Document Cloud wichtige Aspekte wie Fehlerbehebung, Entscheidungsprozesse und externe Überwachung von unserem Security Coordination Center (SCC) zentral gesteuert. Diese Herangehensweise gewährleistet funktionsübergreifende Konsistenz, und Probleme lassen sich schneller lösen.

Interne sowie unabhängige Tests und Beurteilungen

Neue Produktfunktionen werden auf sicherheitsrelevante Fehler hin untersucht. Die dazu erforderlichen Sicherheitsprüfungen sind in den Produktentwicklungszyklus integriert. Zusätzlich wird der Quell-Code auf Schwachstellen getestet sowie statischen und dynamischen Analysen unterzogen. Jede neue Version von Document Cloud wird vor ihrer Veröffentlichung mittels Penetrationstests unabhängiger Drittanbieter getestet, und kritische Fehler werden noch vor dem Release behoben.

Weitere Informationen

Sicherheitsmaßnahmen von Adobe:
www.adobe.com/de/security

Datenschutzrichtlinien von Adobe:
www.adobe.com/de/privacy

Compliance

Document Cloud-Dienste sind mit ISO 27001:2013, PCI DSS* und SOC 2 Type 2 konform und erfüllen viele zusätzliche branchenspezifische Zertifizierungen, Standards und Vorgaben. Adobe Sign zum Beispiel erfüllt die Sicherheitsstandards HIPAA, FERPA, GLBA und 21 CFR Part 11 und ist für SAFE-BioPharma® zertifiziert.

Zugriffskontrolle

Die Infrastruktur von Document Cloud wird in führenden Rechenzentren gehostet und von Amazon Web Services (AWS) verwaltet, unserem bevorzugten Anbieter für Cloud-Dienste. Adobe setzt rollenbasierte Zugriffskontrollen ein, mit denen Zugriffsrechte auf Basis eines Konzepts erteilt werden, das minimale Rechte vorsieht. Die Autorisierung erfordert eine Genehmigung durch den Vorgesetzten, der unmittelbar für die Vertraulichkeit, Integrität und Verfügbarkeit der fraglichen Ressourcen verantwortlich ist.
Nur zugelassene, autorisierte Adobe-Mitarbeiter, Mitarbeiter bei Anbietern von Cloud-Diensten und Vertragspartner mit einem legitimen und anerkannten Unternehmen haben Zugriff auf die gesicherten Standorte in Nordamerika, der Europäischen Union, Australien und Japan.

*Der Dienst „Senden und verfolgen" ist mit dem Standard PCI DSS nicht konform.

Adobe

Adobe Systems GmbH
Georg-Brauchle-Ring 58
D-80992 München
Adobe Systems (Schweiz) GmbH
World Trade Center
Leutschenbachstrasse 95
CH-8050 Zürich
www.adobe.de
www.adobe.at
www.adobe.ch
www.adobe.com

10/17