Sicherheit von Adobe Creative Cloud – Häufig gestellte Fragen für IT-Mitarbeiter

Die meisten Fragen, die Adobe zu Creative Cloud erreichen, betreffen Sicherheit, Datenschutz und Compliance-Richtlinien. Unternehmen, die Creative Cloud verwenden, erwarten eine sichere Speicherung und einen zuverlässigen Zugriff auf ihre Daten. Dieses Dokument versucht, viele der häufig gestellten Fragen von IT-Sicherheitsmitarbeitern zu diesen Themen im Zusammenhang mit Creative Cloud zu beantworten.

1 Wo wird Creative Cloud gehostet?

Creative Cloud wird auf Amazon Web Services (AWS), einschließlich Amazon Elastic Compute Cloud (Amazon EC2) und Amazon Simple Storage Service (Amazon S3), in den Vereinigten Staaten, Europa und in der Region Asien-Pazifik gehostet. AWS bietet eine zuverlässige Plattform für Softwaredienste, die von Tausenden von Unternehmen weltweit genutzt wird. AWS stellt Dienste in Übereinstimmung mit definierten Best Practices für die Sicherheit bereit und führt regelmäßig branchenübliche und anerkannte Zertifizierungen und Prüfungen durch (aws.amazon.com/security/). Somit profitieren auch Creative Cloud-Mitglieder von den fortwährenden Bestrebungen durch Amazon, verlässliche Sicherheitsverfahren für gespeicherte Assets sicherzustellen.

2 Wo befinden sich die Kundendaten?

Die Kundendaten werden in Amazon S3 gespeichert. Adobe legt fest, in welcher physischen Region die Daten und Server einzelner Kunden gespeichert werden. Für Datenobjekte von Amazon S3 findet eine Datenreplikation innerhalb des regionalen Clusters statt, in dem die Daten gespeichert sind. Es erfolgt keine Replikation in Cluster und Datenzentren der anderen Regionen. Adobe betreibt Creative Cloud in 3 Regionen: Vereinigte Staaten, Europa und Asien-Pazifik.

Beispiel: Standardmäßig werden alle Cloud-Daten von Creative Cloud-Kunden in Europa im AWS-Datenzentrum für Europa gespeichert und nicht an Datenzentren außerhalb Europas übertragen.

3 Wer übt die Kontrolle über die Creative Cloud-Datenzentren aus?

Bei allen Teilen der Creative Cloud, die in AWS bereitgestellt werden, unterliegen die physischen Komponenten der Kontrolle durch Amazon. Um Kunden ein besseres Verständnis der Kontrollfunktionen in AWS zu vermitteln und eine Einschätzung der Effizienz zu ermöglichen, veröffentlicht AWS einen SOC 1-Bericht (Service Organization Controls), Typ 2 (aws.amazon.com/security/), mit den Kontrollfunktionen, die für Amazon EC2, Amazon S3 und Virtual Private Cloud (VPC) definiert sind, sowie detaillierten physischen Sicherheits- und Umweltkontrollfunktionen. Die sehr spezifische Definition dieser Kontrollfunktionen sollte die Anforderungen der meisten Kunden erfüllen.

4 Gestattet Amazon Kundenbesichtigungen der AWS-Datenzentren?

Nein. In den AWS-Datenzentren werden Daten mehrerer Kunden gehostet. Aus diesem Grund gestattet AWS keine Besichtigungen der Datenzentren durch Kunden, da sonst die Daten einer Vielzahl von Kunden physisch für Dritte zugänglich wären. Um dieser Kundenanforderung gerecht zu werden, prüft ein unabhängiger und qualifizierter Prüfer im Rahmen eines SOC 1-Berichts, Typ 2, das Vorliegen und den Betrieb der entsprechenden Kontrollfunktionen. Durch diese allgemein anerkannte Überprüfung durch eine dritte Partei erhalten Kunden eine unabhängige Perspektive auf die Effizienz der vorhandenen Kontrollfunktionen. Adobe hat eine Vertraulichkeitsvereinbarung mit AWS unterzeichnet und ist berechtigt, eine Kopie des SOC 1-Berichts, Typ 2, zu erhalten (aws.amazon.com/security/). Unabhängige Prüfungen der physischen Sicherheit der Datenzentren sind außerdem Bestandteil der ISO 27001-Zertifizierung von AWS, der PCI-Prüfung und des ITAR-Prüfverfahrens.

5 Erhalten Dritte Zugang zu den AWS-Datenzentren?

Der Zugang zu den Datenzentren wird durch AWS streng kontrolliert, selbst für interne Mitarbeiter. Dritte erhalten keinen Zugang zu AWS-Datenzentren, sofern nicht eine explizite Genehmigung des zuständigen Managers für das AWS-Datenzentrum gemäß der AWS Access Policy erteilt wurde. Im SOC 1-Bericht, Typ 2 (aws.amazon.com/security/), finden Sie weitere Informationen zu spezifischen Kontrollfunktionen, die den physischen Zugang und die Zugangsautorisierung für Datenzentren regeln, sowie zu weiteren verwandten Kontrollfunktionen.

6 Wer ist verantwortlich für die Installation von Patches?

Adobe ist verantwortlich für die Installation von Patches in unseren Gastbetriebssystemen, unserer Software und den Anwendungen, die in AWS ausgeführt werden. AWS ist verantwortlich für das Patchen von Systemen, die AWS-Dienste bereitstellen, wie z. B. Hypervisor- und Netzwerkdienste. Diese Patches erfolgen gemäß den AWS-Richtlinien und in Übereinstimmung mit ISO 27001-, NIST- und PCI-Anforderungen.

7 Werden privilegierte Aktionen überwacht und kontrolliert?
Der Zugriff auf Systeme und Daten wird durch die vorhandenen Kontrollfunktionen beschränkt oder die Daten selbst sind zugriffsbeschränkt und werden überwacht. Zusätzlich sind Kundendaten und Server standardmäßig von anderen Kunden logisch isoliert. Die Zugriffskontrolle für privilegierte Benutzer der AWS-Infrastruktur wird im Rahmen der AWS-Prüfungen und Zertifizierungen gemäß SOC 1, ISO 27001, PCI, ITAR und FISMA durch einen unabhängigen Prüfer kontrolliert.

8 Hat der Cloud-Anbieter Maßnahmen implementiert, um einer Gefährdung durch unberechtigte Zugriffe von internen Mitarbeitern auf Kundendaten und Anwendungen vorzubeugen?
AWS implementiert entsprechende Maßnahmen gemäß SOC 1, die im SOC 1-Bericht, Typ 2, beschrieben werden (aws.amazon.com/security/). Zusätzlich führt Adobe regelmäßig Risikobewertungen bezüglich der Kontrolle und Überwachung von internen Zugriffen durch.

9 Wie isoliert Creative Cloud Kundendaten?
Alle Daten, die von Adobe im Auftrag der Kunden gespeichert werden, unterliegen umfassenden Sicherheits- und Kontrollfunktionen zur Isolation der einzelnen Mandanten. Für Creative Cloud-Speicher wird Amazon S3 verwendet, das erweiterte Datenzugriffskontrollfunktionen bereitstellt.

10 Ist die Implementierung der Kundentrennung sicher?
Bei der AWS-Umgebung handelt es sich um eine virtualisierte Mehrmandantenumgebung. AWS hat Sicherheitsmanagementprozesse, PCI- sowie weitere Sicherheitskontrollfunktionen implementiert, durch die jeder Kunde von anderen Kunden isoliert wird. Die Systeme von AWS wurden so entworfen, dass Zugriffe von Kunden auf physische Hosts oder diesen Kunden nicht zugewiesene Instanzen vermieden werden, indem alle Zugriffe durch die Virtualisierungssoftware gefiltert werden. Diese Architektur wurde von einem unabhängigen PCI Qualified Security Assessor (QSA) validiert und erfüllt alle Anforderungen gemäß PCI DSS 2.0 (aws.amazon.com/security/pci-dss-level-1-compliance-faqs/).

11 Verfolgt AWS Strategien, um bekannten Sicherheitslücken im Hypervisor zu begegnen?
Amazon EC2 verwendet derzeit eine hochgradig angepasste Version des Xen-Hypervisors. Die Sicherheit des Xen-Hypervisors von AWS wird im Rahmen von Analysen und Prüfungen regelmäßig durch unabhängige Prüfer bewertet. Im Whitepaper zur AWS-Sicherheit (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) finden Sie weitere Informationen zum Xen-Hypervisor und zur Isolation von Instanzen.

12 Unterstützen die bereitgestellten Dienste eine Verschlüsselung?
Creative Cloud verschlüsselt Daten während der Übertragung mit SSL.

13 Welche Rechte an den Kundendaten erhält der Cloud-Anbieter?
Creative Cloud-Kunden behalten das Eigentum und alle Rechte an ihren Daten. Ausführliche Informationen hierzu finden Sie in den Nutzungsbedingungen von Adobe (www.adobe.com/go/gffooter_terms_of_use_de) und in den Datenschutzrichtlinien (www.adobe.com/privacy/policy.html).

14 Veröffentlicht AWS die physischen und Umweltkontrollfunktionen?
Ja. Die physischen und Umweltkontrollfunktionen werden in einem SOC 1-Bericht, Typ 2, gezielt erläutert (aws.amazon.com/security/). Zusätzlich verfügt AWS über Zertifizierungen nach ISO 27001 und FISMA, die ebenfalls spezifische Best Practices für die vorhandenen physischen und Umweltkontrollfunktionen erfordern.

15 Können Kunden den Zugriff auf Creative Cloud durch Clients wie PCs und Mobilgeräte sichern und verwalten?
Ja. Mit Creative Cloud können Kunden den Zugriff durch Clients und Mobilgeräte entsprechend ihren eigenen Anforderungen verwalten.

16 Gestattet AWS den Kunden eine Absicherung ihrer virtuellen Server?
Ja. Adobe hat eine eigene Sicherheitsarchitektur implementiert, die auf AWS aufsetzt und auf verschiedenen anerkannten Best Practices basiert (einschließlich SANS Top 20 Controls for Internet Security, Consensus Audit Guidelines, NIST Guidelines und Internet Standards).

17 Bietet AWS auch Funktionen für Identity and Access Management (IAM)?
AWS stellt eine Suite mit verschiedenen IAM-Angeboten bereit, über die Adobe Benutzeridentitäten verwalten, Sicherheitsanmeldeinformationen zuweisen, Benutzer in Gruppen organisieren und Benutzerberechtigungen zentral verwalten kann.

18 Wird Adobe einzelne Creative Cloud-Systeme zu Wartungszwecken offline schalten?
Creative Cloud wurde so implementiert, dass Ausfallzeiten quasi eliminiert werden. Die Dienste bleiben während neuer Bereitstellungen weiterhin verfügbar und erreichbar, da durch die Verwendung von A/B-Umgebungen und weiteren Mechanismen Live-Übergänge ohne extern sichtbare Ausfallzeiten realisiert werden.

19 Wie schützt sich AWS gegen DDoS-Attacken (Distributed Denial of Service)?
Das AWS-Netzwerk bietet einen sehr viel weiter reichenden Schutz im Vergleich zur herkömmlichen Netzwerksicherheit. Im Whitepaper zur AWS-Sicherheit (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) finden Sie weitere Informationen zu diesem Thema, einschließlich einer Diskussion über DDoS.

20 Verfügt Adobe über einen Plan für das Betriebskontinuitätsmanagement für Creative Cloud?
AWS bietet ein Programm für das Betriebskontinuitätsmanagement an (media.amazonwebservices.com/AWS_Disaster_Recovery.pdf) und Creative Cloud wurde für die Ausführung in mehreren Regionen und mehreren Verfügbarkeitszonen bzw. Datenzentren entwickelt. Adobe hat Creative Cloud so entworfen, konzipiert und implementiert, dass Datenredundanzreplikation und Bereitstellungsarchitekturen mit mehreren Regionen/Verfügbarkeitszonen zum Einsatz kommen.

21 Macht AWS Angaben zur Dauerhaftigkeit der Daten?
Creative Cloud speichert Daten in Amazon S3, das eine zuverlässige und dauerhafte Speicherinfrastruktur bereitstellt. Objekte werden redundant auf mehreren Geräten und an mehreren Standorten in einer Amazon S3-Region gespeichert. Sobald Daten gespeichert wurden, realisiert Amazon S3 die Dauerhaftigkeit von Objekten durch die schnelle Erkennung und Reparatur aller eventuellen Redundanzverluste. Amazon S3 überprüft außerdem regelmäßig die Integrität gespeicherter Daten durch die Verwendung von Prüfsummen. Wenn Fehler entdeckt werden, werden diese unter Einsatz der redundanten Daten behoben.

22 Plant Adobe eine Konformitätsprüfung gemäß FISMA (Federal Information Security Management Act)?
Adobe plant derzeit keine Konformitätsprüfung gemäß FISMA (Federal Information Security Management Act) für Creative Cloud.

23 Ist Creative Cloud HIPAA-konform?
Adobe beabsichtigt keine Zertifizierung der Creative Cloud gemäß HIPAA (Health Insurance Portability and Accountability Act von 1996), da Creative Cloud nicht für die Verarbeitung von Gesundheitsdatensätzen vorgesehen ist.

Referenzen

Whitepaper „AWS: Sicherheitsprozesse im Überblick", März 2013 (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

Whitepaper „AWS: Risiko und Compliance", Januar 2013 (media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf)

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com