Sicherheit der Adobe Creative Cloud für Teams – Überblick

Inhalt

Sicherheit bei Adobe

Adobe nimmt die Sicherheit Ihrer digitalen Inhalte ernst. Von der konsequenten Integration des Sicherheitsaspekts in die Software-Entwicklung bis zur umfassenden Unterstützung des Incident Response Teams setzen wir auf proaktives und flexibles Handeln. Darüber hinaus halten wir uns durch Kooperation mit Partnern, Experten und anderen Unternehmen über die Bedrohungslage und Best Practices auf dem neuesten Stand und übertragen gewonnene Erkenntnisse auf unsere Produkte und Dienste.

In diesem Whitepaper erfahren Sie, wie Adobe für eine sichere Creative Cloud-Umgebung sorgt und Ihre Daten proaktiv schützt.

Die Creative Cloud für Teams

Die Creative Cloud für Teams umfasst sämtliche Desktop-Applikationen der Creative Cloud (darunter Adobe Photoshop CC, Adobe Illustrator CC usw.) sowie Dienste und Verwaltungsfunktionen für Teams. Sie ist auf die Bedürfnisse kleiner bis mittelständischer Unternehmen und Teams abgestimmt. Die Creative Cloud für Teams ist in zwei Lizenzvarianten erhältlich: im Komplett-Abo oder im Einzelprodukt-Abo. Die Lizenzen lassen sich über die intuitive Admin Console auf einfache Weise erwerben, verwalten und bereitstellen.

Speicher und Speicheroptionen der Creative Cloud für Teams

Mit einem Komplett-Abo der Creative Cloud für Teams erhält jeder Anwender bis zu 100 GB Cloud-Speicherplatz (Anwender mit einem Einzelprodukt-Abo erhalten 20 GB). Das Speichern und Abrufen von Daten erfolgt über die zuverlässige Infrastruktur von Amazon S3 (Amazon Simple Storage Service).

Die Nutzung des Cloud-Speichers ist nicht verpflichtend. Es besteht außerdem die Möglichkeit, die Netzwerkverbindung innerhalb des Firmennetzwerks zu blockieren. Weitere Informationen zu den *Speicheroptionen* finden Sie auf der Adobe-Website.

Verwaltungswerkzeuge für die Creative Cloud für Teams

Admin Console

IT-Administratoren können über die intuitive, Web-basierte Admin Console bequem Lizenzen erwerben und verwalten, Anwender hinzufügen und Creative Cloud-Applikationen und -Dienste bereitstellen. Anwender werden per E-Mail gebeten, eine eigene Adobe-ID zu erstellen.

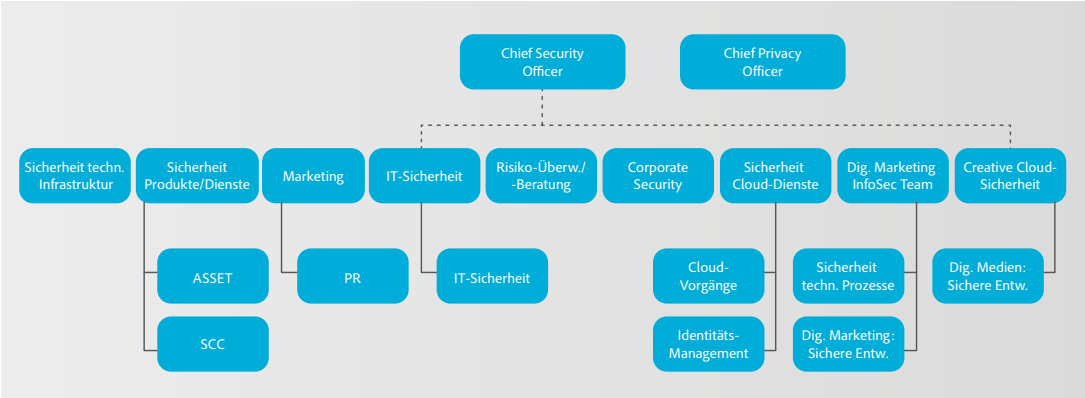
Creative Cloud Packager

Mit dem Creative Cloud Packager, der über die Admin Console der Creative Cloud für Teams verfügbar ist, können IT-Administratoren alle oder ausgewählte Applikationen der Creative Cloud von zentraler Stelle aus implementieren. Creative Cloud Packager stellt sicher, dass alle Anwender mit derselben Software-Version arbeiten und nicht parallel dieselbe Software herunterladen. Dadurch werden Support-Kosten gesenkt und die Netzwerkauslastung reduziert. IT-Administratoren melden sich mit ihrer Adobe-ID bei Creative Cloud Packager an. Diese erstellen sie bei der ersten Registrierung für ein Abo der Creative Cloud für Teams. Weitere Informationen zu *Creative Cloud Packager* und den *Bereitstellungsoptionen* finden Sie auf der Adobe-Website.

Die Adobe-Sicherheitsorganisation

Sämtliche Maßnahmen zur Erhöhung der Sicherheit der Produkte und Dienste von Adobe werden vom Chief Security Officer (CSO) koordiniert. Das Büro des CSO ist für alle Sicherheitsinitiativen für Produkte und Dienste sowie die Implementierung von *Adobe Secure Product Lifecycle (SPLC)* zuständig.

Der CSO leitet auch das Adobe Secure Software Engineering Team (ASSET), ein zentrales Team von Sicherheitsexperten, die den Produkt- und Entwickler-Teams von Adobe, u. a. den Adobe Creative Cloud-Teams, beratend zur Seite stehen. Die ASSET-Experten arbeiten mit verschiedenen Produkt- und Entwickler-Teams von Adobe zusammen, um bei allen Produkten und Diensten das gewünschte Maß an Sicherheit zu erreichen. Sie empfehlen Sicherheitsmaßnahmen mit klar strukturierten und wiederholbaren Prozessen in den Bereichen Entwicklung, Bereitstellung, Betrieb und Fehlerbehebung.



Die Adobe-Sicherheitsorganisation

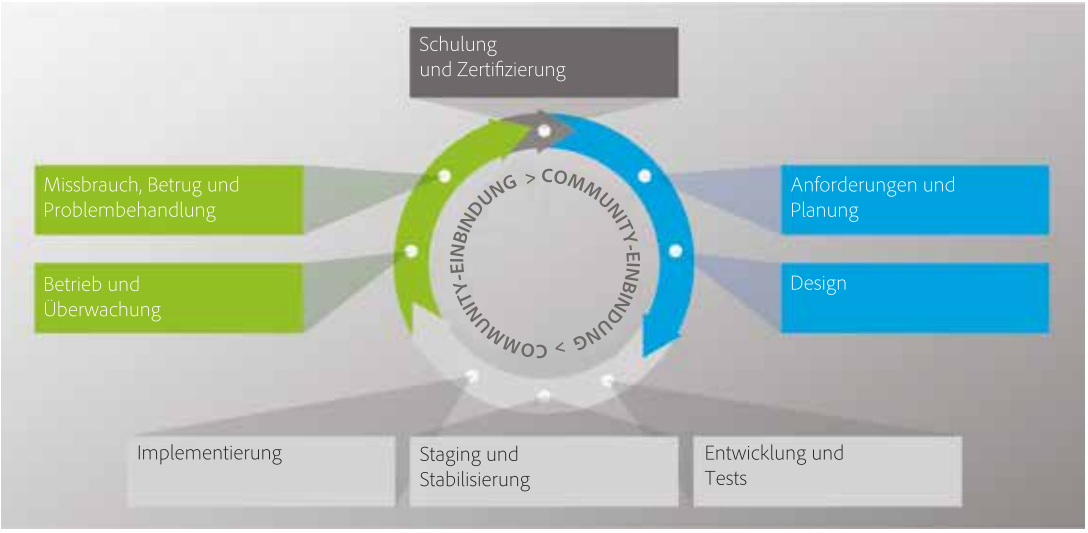
Entwicklung sicherer Adobe-Produkte

Wie bei anderen wichtigen Produkten und Diensten von Adobe wird für die Creative Cloud der SPLC-Prozess (Adobe Secure Product Lifecycle) angewandt. Das SPLC-Programm von Adobe umfasst zahlreiche spezielle, auf größtmögliche Sicherheit ausgerichtete Methoden, Prozesse und Werkzeuge, die während des gesamten Produktzyklus zum Einsatz kommen – von der Entwurfs- und Entwicklungsphase bis hin zur Qualitätssicherung, Testphase und Bereitstellung. Die Sicherheitsexperten des ASSET geben im Rahmen des SPLC-Programms nach Bewertung potenzieller Sicherheitsrisiken Empfehlungen für einzelne Produkte und Dienste. Das SPLC-Programm von Adobe wird u. a. dank der regelmäßigen Einbindung der Community kontinuierlich weiterentwickelt und ist somit in Bezug auf neue Technologien, Sicherheitsmethoden und Bedrohungen stets auf dem neuesten Stand.

Adobe Secure Product Lifecycle

Das Adobe SPLC-Programm umfasst, je nach Creative Cloud-Dienst, einige oder alle der folgenden empfohlenen Verfahren, Prozesse und Werkzeuge:

- Sicherheits-Training und -zertifizierung für die Produkt-Teams
- Analyse der Produktsicherheit, Risiken und aktuellen Bedrohungen
- Richtlinien, Regeln und Analysen für sicheres Coden
- Service-Leitfäden, Sicherheitswerkzeuge und Testmethoden, mit denen das Sicherheits-Team der Creative Cloud die vom Open Web Application Security Project (OWASP) veröffentlichten Top 10 schwerwiegender Sicherheitslücken von Web-Applikationen und die von CWE/SANS veröffentlichten 25 gefährlichsten Software-Fehler leichter erkennen und vermeiden kann
- Prüfungen der Sicherheitsarchitektur und Penetrationstests
- Prüfung des Quell-Codes zur Behebung von Fehlern, die Sicherheitslücken verursachen können
- Validierung anwendergenerierter Inhalte
- Statische und dynamische Code-Analyse
- Scannen von Anwendungen und Netzwerken
- Beurteilung der Produktreife, Notfallpläne, Veröffentlichung von Unterlagen für Entwickler



Adobe Secure Product Lifecycle (SPLC)

Sicherheits-Training für Adobe-Entwickler

Adobe Software Security Certification Program
Im Rahmen des Adobe Secure Product Lifecycle führt Adobe regelmäßig Sicherheitsschulungen für Entwickler-Teams im gesamten Unternehmen durch, um Mitarbeiter auf dem neuesten Stand zu halten. Mitarbeiter, die am Adobe Software Security Certification Program teilnehmen, können durch den Abschluss von Sicherheitsprojekten verschiedene Stufen erreichen.

Das Programm umfasst vier Stufen, die jeweils durch einen farbigen „Gürtel" gekennzeichnet sind: weiß, grün, braun und schwarz. Die weiße und die grüne Stufe werden durch den Abschluss Computer-gestützter Schulungen erreicht. Die braune und schwarze Stufe erfordern die Teilnahme an Sicherheitsprojekten, die sich über mehrere Monate oder ein Jahr erstrecken und in denen praktische Kenntnisse erworben werden. Inhaber des braunen und schwarzen Gürtels werden als Sicherheitsexperten ihres Produkt-Teams ausgezeichnet. Adobe aktualisiert die Schulungen regelmäßig in Bezug auf aktuelle Bedrohungen sowie neue Kontrollmechanismen und Software-Sprachen.

Einige Creative Cloud-Teams nehmen an zusätzlichen Sicherheitsschulungen und -Workshops teil, in denen vermittelt wird, welche Auswirkungen das Thema Sicherheit auf ihre jeweiligen Funktionen innerhalb ihrer Organisation und im gesamten Unternehmen haben.

Adobe Software Security Certification Program

Die Creative Cloud-Architektur

Adobe möchte künftig für alle Komponenten der Creative Cloud für Teams eine einheitliche, gehostete Infrastruktur bereitstellen. Derzeit werden jedoch zwei primäre Infrastrukturen zum Hosten verschiedener Komponenten der Creative Cloud für Teams eingesetzt:

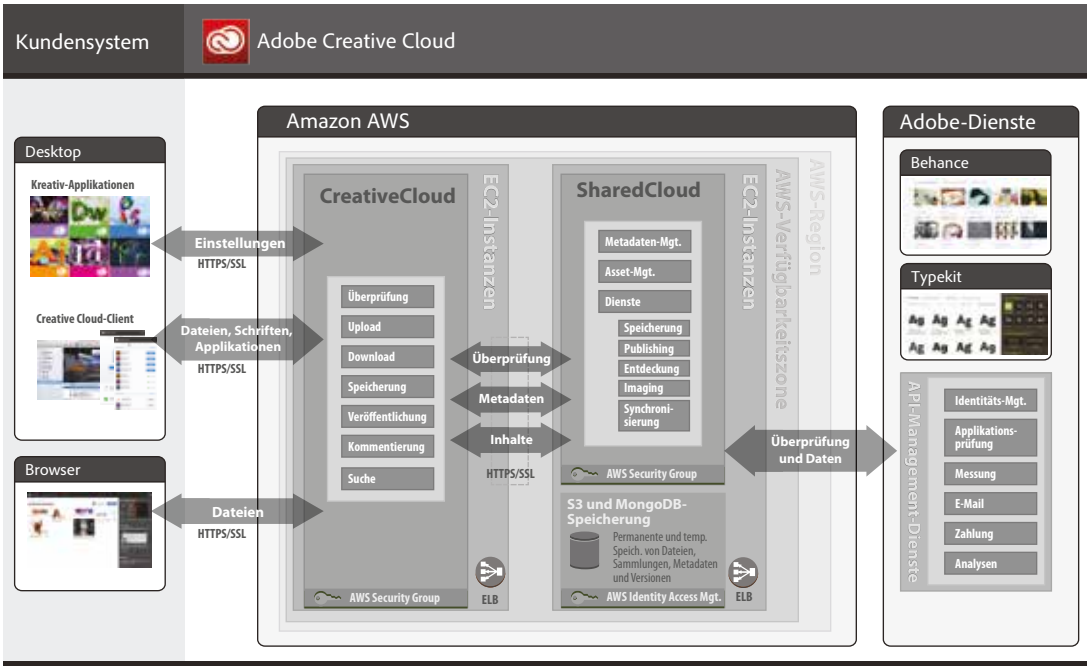
- Amazon Web Services (AWS): Die meisten Komponenten der Creative Cloud für Teams werden auf AWS gehostet, einschließlich Amazon Elastic Compute Cloud (Amazon EC2) und Amazon Simple Storage Service (Amazon S3) in den USA, in Europa und im asiatisch-pazifischen Raum. Amazon EC2 ist ein Web-Dienst, der automatisch skalierbare Rechenkapazität in der Cloud bereitstellt und damit die Web-Skalierung vereinfacht. Amazon S3 ist eine zuverlässige Infrastruktur für die Speicherung und den Abruf jeder beliebigen Datenmenge.

  AWS bietet eine zuverlässige Plattform für Software-Dienste, die von Tausenden von Unternehmen weltweit genutzt wird. Die bereitgestellten Dienste stehen mit bewährten Sicherheitsverfahren im Einklang. AWS wird regelmäßig branchenweit anerkannten Zertifizierungsmethoden und Prüfungen unterzogen. Weitere Informationen finden Sie im Amazon-Whitepaper *Amazon Web Services – Übersicht über Sicherheitsverfahren*.

- Angemietete Rechenzentren: Einige Dienste für die Adobe Creative Cloud, darunter die Adobe-IDs, werden derzeit in sicheren, nicht gekennzeichneten, von Adobe angemieteten Rechenzentren gehostet. Die Infrastruktur und die physischen Sicherheitsmaßnahmen dieser Rechenzentren entsprechen den Branchenstandards.

* Adobe Behance, eine Online-Plattform für den Austausch kreativer Arbeiten, wird in einem sicheren, angemieteten Rechenzentrum des Unternehmens Rackspace gehostet.

* Typekit wird sowohl von *Rackspace* als auch von AWS gehostet. Die Web-Applikation Typekit wird von Rackspace in seinem Rechenzentrum in Chicago gehostet. Die Web-Applikation interagiert mit Quell-Fonts, die auf AWS gespeichert sind, und erstellt anwenderdefinierte „Kits". Die meisten dieser Kits werden auf AWS gehostet. Einige Kunden verfügen jedoch über Kits auf Servern, die von Rackspace gehostet werden.



Die logische Architektur der Creative Cloud für Teams

Die Applikationen der Creative Cloud bauen auf der Adobe Shared Cloud-Plattform von AWS auf. Hochgeladene Dateien werden von einer EC2-Instanz (Amazon Elastic Compute Cloud) verarbeitet und in einem S3-Bucket (Amazon Simple Storage Service) gespeichert, der von IAM-Rollen (Identity and Access Management) innerhalb einer AWS-Region geschützt wird. S3 bietet eine hohe Redundanz: So werden Dateien zu Backup-Zwecken in mehreren AWS-Verfügbarkeitszonen repliziert.

Die Creative Cloud enthält eine Reihe von Diensten, mit denen autorisierte Anwender auf Desktop- und Web-Applikationen zugreifen können.

Der Zugriff auf diese Dienste und Applikationen erfolgt von einem Kundensystem aus über drei Endpunkte:

- Applikationen, z. B. Adobe Photoshop
- Creative Cloud-Client
- Browser.

Welche Dienste verfügbar sind, hängt von der Art des Zugriffs auf die Creative Cloud ab. Die einzelnen Applikationen greifen z. B. auf die Creative Cloud zu, um die Identität des Anwenders zu überprüfen, Einstellungen zu synchronisieren und optional Inhalte auf Adobe Behance zu teilen. Mit dem Creative Cloud-Client können Anwender ihre Desktop-Applikationen herunterladen und aktualisieren, Web-Schriften von Typekit herunterladen und Dateien von ihrem lokalen System in den Creative Cloud-Speicher hoch- bzw. aus dem Creative Cloud-Speicher auf ihr lokales System herunterladen.

Unabhängig vom Endpunkt des Kunden wird jeder Zugriff auf die Creative Cloud mit öffentlichen Diensten überwacht, die auf der Adobe-Website verfügbar sind. Sobald die Identität des Anwenders überprüft wurde, kann dieser jede Aktion durchführen, die vom jeweiligen Endpunkt zulässig ist. Eine Beschreibung der *verfügbaren Werkzeuge und Dienste* finden Sie auf der Adobe-Website.

Verantwortungsbereiche von AWS und Adobe
AWS betreibt, verwaltet und überwacht die Komponenten von der Hypervisor-Virtualisierungsebene bis hin zur physischen Sicherheit der Räumlichkeiten, in denen die Komponenten der Creative Cloud für Teams ausgeführt werden. Adobe ist seinerseits verantwortlich für das Gast-Betriebssystem und deren Verwaltung (einschließlich Updates und Sicherheits-Patches), für Applikationen und für die Konfiguration der von AWS bereitgestellten Firewall für die Sicherheitsgruppe.

AWS betreibt zudem die Cloud-Infrastruktur, die von Adobe genutzt wird, um verschiedene Rechenressourcen z. B. für Datenverarbeitung und -speicherung zur Verfügung zu stellen. Die AWS-Infrastruktur umfasst die Räumlichkeiten, das Netzwerk, die Hardware und die Software (z. B. das Host-Betriebssystem, Virtualisierungs-Software usw.), die die Provisionierung und Verwendung dieser Ressourcen ermöglichen. Amazon wendet in den Bereichen Entwicklung und Verwaltung bewährte Sicherheitsverfahren an und erfüllt zahlreiche Sicherheitsstandards.

Sichere Verwaltung
Adobe verwendet Secure Shell (SSH) und Secure Sockets Layer (SSL) für Verbindungen zur Verwaltung der AWS-Infrastruktur.

Amazon Web Services (AWS)

Geografischer Standort von Kundendaten im AWS-Netzwerk
Für Kundendaten, die in der Cloud in Amazon S3 gespeichert sind, legt Adobe fest, in welcher physischen Region die Daten und Server des jeweiligen Kunden sich befinden sollen. Adobe betreibt die Creative Cloud in drei Regionen: in den USA, in Europa und im asiatisch-pazifischen Raum. Die Datenreplikation für Amazon S3-Datenobjekte erfolgt innerhalb des regionalen Clusters, in dem die Daten gespeichert sind. Es findet keine Replikation in Cluster der Rechenzentren anderer Regionen statt. Inhalte, die von Kunden in der Creative Cloud gespeichert werden, werden nicht in Rechenzentren in anderen Regionen repliziert. So werden standardmäßig alle Inhalte von Kunden aus Europa in die Creative Cloud in Europa hochgeladen.

Isolation von Kundendaten / Abgrenzung von AWS-Kunden
Creative Cloud-Daten, die von Adobe auf AWS gespeichert werden, unterliegen strengen Sicherheits- und Kontrollmechanismen zur Mandantenisolation. AWS ist eine virtualisierte, mehrmandantenfähige Umgebung (Multi-Tenant-Umgebung). Sie hat Sicherheits-Management-Prozesse und andere Sicherheitskontrollfunktionen implementiert, durch die jeder Kunde, z. B. ein Creative Cloud-Kunde, von anderen AWS-Kunden isoliert wird. Mithilfe von Identity and Access Management (IAM) wird der Zugriff auf Rechen- und Speicherinstanzen noch weiter geschützt.

Sichere Übertragung
Adobe sendet eine REST/Query-Anforderung über HTTP/HTTPS oder eine Call-Wrapper-Funktion in einem der AWS SDKs, um eine Verbindung zu einem AWS-Zugriffspunkt herzustellen. HTTPS verwendet Secure Sockets Layer (SSL), ein Verschlüsselungsprotokoll zum Schutz vor dem Abhören, der Manipulation und der Fälschung von Nachrichten. Das Hoch- und Herunterladen von Daten auf bzw. von Amazon S3 durch Adobe erfolgt über SSL-verschlüsselte Endpunkte. Auf die verschlüsselten Endpunkte kann über das Internet und von Amazon EC2 aus zugegriffen werden. So ist eine sichere Datenübertragung innerhalb von AWS sowie von und zu externen Quellen sichergestellt.

Sichere Netzwerkarchitektur
Mithilfe einer Firewall und anderen Mechanismen überwacht und kontrolliert AWS die Kommunikation an der Außengrenze sowie an wichtigen internen Grenzen des Netzwerks. Diese Mechanismen wenden Regelsätze, Access Control Lists (ACLs) und Konfigurationen an, um den Informationsfluss zu speziellen Informationssystem-Diensten zu lenken. ACLs, oder Richtlinien für den Netzwerkfluss, dienen zur gezielten Steuerung des Verkehrsflusses an jeder verwalteten Schnittstelle. Amazon Information Security prüft und genehmigt alle ACL-Richtlinien und weist sie mithilfe des ACL-Manage-Tools von AWS automatisch jeder verwalteten Schnittstelle zu. So ist sichergestellt, dass diese die jeweils aktuellen ACLs anwenden.

Netzwerküberwachung und -schutz
Mit einer Reihe von automatisierten Überwachungssystemen stellt AWS eine hohe Performance und Verfügbarkeit aller Dienste sicher. Überwachungswerkzeuge helfen, an Netzwerkpunkten mit ein- und ausgehender Kommunikation ungewöhnliche oder unzulässige Aktivitäten und Situationen zu erkennen.

Das AWS-Netzwerk bietet zuverlässigen Schutz vor traditionellen Problemen der Netzwerksicherheit:

- DDOS-Angriffe (Distributed Denial Of Service)
- MITM-Angriffe (Man in the Middle)
- IP-Spoofing
- Port-Scanning
- Packet-Sniffing durch andere Instanzen

Weitere Informationen zum Thema Netzwerküberwachung und -schutz finden Sie im Whitepaper *Amazon Web Services – Übersicht über Sicherheitsverfahren* auf der Amazon-Website.

Überwachung der Dienstequalität
AWS überwacht alle elektrischen, technischen und Notfallsysteme und -einrichtungen, damit Probleme jeder Art unmittelbar erkannt werden. Um den unterbrechungsfreien Betrieb aller Geräte sicherzustellen, sorgt AWS für eine kontinuierliche Wartung.

Datenspeicherung und -sicherung
Die Creative Cloud für Teams speichert Daten in Amazon S3, das laut Amazon über eine Speicherinfrastruktur mit einer Beständigkeit von 99,999999999 % und einer Objektverfügbarkeit von 99,99 % in einem Zeitraum von einem Jahr verfügt. Um die Beständigkeit zu erhöhen, speichert Amazon S3 die Kundendaten über PUT- und COPY-Aktionen synchron an mehreren physischen Standorten. Objekte werden redundant auf mehreren Geräten an mehreren physischen Standorten in einer Amazon S3-Region gespeichert. Darüber hinaus berechnet Amazon S3 Prüfsummen für sämtlichen Netzwerkverkehr, um eine eventuelle Beschädigung von Datenpaketen beim Speichern oder Abrufen von Daten zu erkennen.

Änderungs-Management
Routinemäßige und notfallbedingte Änderungen sowie Konfigurationsänderungen an der bestehenden AWS-Infrastruktur werden von AWS entsprechend den Branchenstandards für gleichartige Systeme autorisiert, protokolliert, getestet, genehmigt und dokumentiert. AWS wird von Amazon nach einem festen Zeitplan aktualisiert, um mögliche Auswirkungen für Kunden zu minimieren. AWS informiert die Kunden per E-Mail oder über das *AWS Service Health Dashboard*, falls die Nutzung des Dienstes beeinträchtigt sein sollte. Adobe betreibt zudem ein *Status Health Dashboard* für die Creative Cloud.

Patch-Management
AWS ist verantwortlich für die Installation von Patches auf Systemen, die die Bereitstellung von AWS-Diensten wie dem Hypervisor und Netzwerkdiensten unterstützen. Adobe übernimmt die Installation von Patches für eigene Gast-Betriebssysteme, Software und Applikationen, die in AWS ausgeführt werden. Sind Patches erforderlich, stellt Adobe anstatt des Patches eine neue, sichere Instanz des Betriebssystems bzw. der Applikation zur Verfügung.

Authentifizierung für den Zugriff auf die Creative Cloud für Teams (über Adobe-IDs)

Nachdem ein Anwender eine Einladung zur Zusammenarbeit mit einem Team erhalten hat, erstellt er eine Adobe-ID, die für jeden Zugriff auf die Creative Cloud für Teams benötigt wird. Für die Adobe-ID wird der Hash-Algorithmus SHA 256 in Kombination mit Kennwort-Salts und einer Vielzahl an Hash-Iterationen verwendet. Die Adobe-ID-Accounts werden kontinuierlich auf ungewöhnliche Aktivitäten hin überprüft, um das Sicherheitsrisiko zu minimieren.

Risiko- und Schwachstellen-Management bei Adobe

Penetrationstests
Adobe beauftragt anerkannte Drittanbieter mit der Durchführung von Penetrationstests, um potenzielle Sicherheitslücken aufzudecken und die Sicherheit von Produkten und Diensten von Adobe insgesamt zu verbessern. Bei den Tests werden branchenübliche Best Practices angewandt. Nach Erhalt des Berichts eines Drittanbieters dokumentiert Adobe die Sicherheitslücken, bewertet deren Schweregrad und Priorität und entwirft eine Strategie zur Risikominimierung oder einen Plan zur Problembehebung.

Problembehandlung
Jeden Tag entstehen neue Sicherheitslücken und Bedrohungen. Adobe möchte möglichst umgehend darauf reagieren. Neben branchenspezifischen Schwachstellenlisten, die u. a. von US-CERT, Bugtraq und SANS herausgegeben werden, erhält Adobe regelmäßig die neuesten Sicherheitshinweise führender Anbieter von Sicherheitslösungen.

Hat eine bekannt gegebene Sicherheitslücke Auswirkungen auf die Adobe Creative Cloud, informiert das Adobe Product Security Incident Response Team (PSIRT) die entsprechenden Creative Cloud-Teams, um die erforderlichen Maßnahmen zu koordinieren.

Bei Vorfällen, Sicherheitslücken und Bedrohungen, die Auswirkungen auf das AWS-Rechenzentrum haben, wendet das Amazon Incident Management-Team branchenübliche Diagnoseverfahren an, um eine schnelle Lösung herbeizuführen. Die Mitarbeiter des Teams arbeiten rund um die Uhr an der Erkennung von Vorfällen, der Begrenzung der Auswirkungen und der Problemlösung. Außerdem werden Adobe und andere AWS-Kunden umgehend informiert.

Für Cloud-basierte Dienste von Adobe wie die Adobe Creative Cloud werden 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.

Wenn die Sicherheit eines Adobe-Produkts beeinträchtigt ist, wird das SCC gemeinsam mit den beteiligten Adobe Product Incident Response- und Entwickler-Teams aktiv, um das Problem schnellstmöglich zu identifizieren und zu beheben. Dabei kommt folgende Vorgehensweise zum Einsatz:

- Einstufung der Sicherheitslücke
- Minderung des Risikos im Produktionseinsatz
- Isolierung, Untersuchung und Entfernung manipulierter Knoten (nur Cloud-basierte Dienste)
- Entwicklung einer Lösung
- Implementierung der Lösung
- Überwachung der Aktivitäten und Bestätigung, dass mit der Lösung das angestrebte Ziel erreicht wurde

Forensische Analyse
Bei der Untersuchung eines Vorfalls wendet Adobe branchenübliche Werkzeuge und Methoden an. Der forensische Analyseprozess umfasst eine vollständige Bilderfassung oder einen Speicherauszug, eine sichere Aufbewahrung von Beweisen und eine lückenlose Dokumentation der Überwachungskette. Adobe arbeitet im Bedarfsfall mit Strafverfolgungsbehörden oder unabhängigen Forensiklabors zusammen.

Physische Sicherheit und Umgebungssicherung in AWS-Rechenzentren

Die Maßnahmen zur Erhöhung der physischen Sicherheit und zur Umgebungssicherung bei AWS werden im SOC 1-Bericht (Service Organization Controls), Typ 2, beschrieben. Im folgenden Abschnitt sind einige Sicherheitsmaßnahmen und Kontrollmechanismen aufgeführt, die in allen AWS-Rechenzentren weltweit angewandt werden. Weitere Informationen zu AWS und den *Sicherheitsmaßnahmen bei Amazon* finden Sie auf der Amazon-Website zum Thema Sicherheit.

Physische Sicherheit
Die AWS-Rechenzentren zeichnen sich durch innovative Architektur und modernste Technik aus. Amazon verfügt über langjährige Erfahrungen in der Planung, in der Konstruktion und im Betrieb großer Rechenzentren. Diese Erfahrung wurde auf die AWS-Plattform und -Infrastruktur angewandt. AWS-Rechenzentren sind in unauffälligen Gebäuden untergebracht. Der physische Zugang wird durch professionelles Sicherheitspersonal, Videokameras, Einbruchmeldeanlagen und andere elektronische Geräte streng kontrolliert. Das gesamte Gelände und alle Gebäudeeingänge werden überwacht. Autorisierte Mitarbeiter müssen mindestens zwei Mal eine Zwei-Faktor-Authentifizierung durchlaufen, bevor Sie die einzelnen Etagen des Rechenzentrums betreten dürfen. Alle Besucher und Dienstleister müssen sich ausweisen und registrieren. Sie werden während der gesamten Besuchszeit von autorisierten Mitarbeitern begleitet.

Der Zugang zum Rechenzentrum und zu Informationen wird ausschließlich Mitarbeitern und Dienstleistern gestattet, die einen legitimen geschäftlichen Grund haben. Besteht dieser geschäftliche Grund nicht mehr, wird die Zutrittsberechtigung sofort aufgehoben, auch wenn die jeweilige Person weiterhin als Mitarbeiter von Amazon oder Amazon Web Services tätig ist. Der Zutritt zu den Rechenzentren durch Mitarbeiter von AWS wird protokolliert und regelmäßig überprüft.

Brandbekämpfung
AWS hat Anlagen zur automatischen Branderkennung und -bekämpfung eingerichtet. Die Brandmeldeanlage setzt sich aus folgenden Komponenten zusammen: Rauchmelder, die in allen Räumlichkeiten des Rechenzentrums installiert sind, Räume für die mechanische und elektrische Infrastruktur, Kühlräume und Räume für die Generatoranlage. Diese Bereiche werden entweder durch Nasssprinkleranlagen, doppelt gesicherte vorgesteuerte Sprinkleranlagen oder Trockensprinkleranlagen geschützt.

Raumklima und -temperatur
Mit einer Klimaanlage sorgt AWS für eine konstante Betriebstemperatur der Server und anderer Hardware-Geräte. So wird eine Überhitzung verhindert und die Gefahr von Ausfällen verringert. In den Rechenzentren von AWS werden die atmosphärischen Bedingungen auf einem optimalen Niveau gehalten. Temperatur und Luftfeuchtigkeit werden vom AWS-Personal und den technischen Systemen entsprechend überwacht und geregelt.

Kontinuierliche Stromversorgung
Die Stromversorgungssysteme der Rechenzentren von AWS sind vollständig redundant und können rund um die Uhr instandgesetzt werden, ohne Betriebsabläufe zu beeinträchtigen. Durch eine unterbrechungsfreie Stromversorgung (USV) ist während eines Stromausfalls die Stromversorgung von kritischen und wichtigen Geräten sichergestellt. In den Rechenzentren ermöglichen Generatoren eine Notstromversorgung in der gesamten Anlage.

Videoüberwachung
Der physische zum Betriebsgelände und zu den Gebäuden der AWS-Rechenzentren wird durch Überwachungskameras, Einbruchmeldeanlagen und andere elektronische Geräte streng kontrolliert.

Wiederherstellung nach Ausfall
AWS-Rechenzentren zeichnen sich durch eine hohe Verfügbarkeit aus und sind so konzipiert, dass System- oder Hardware-Ausfälle nur minimale Auswirkungen auf die Kunden haben. Die Rechenzentren sind in Gruppen auf mehrere Regionen weltweit verteilt. Alle Rechenzentren sind rund um die Uhr online und für die Kunden verfügbar. Bei einem Funktionsausfall wird der Datenverkehr automatisch umgeleitet. Für wichtige Anwendungen gilt die N+1-Konfiguration. Kommt es in einem Rechenzentrum zu einem Funktionsausfall, stehen genügend Kapazitäten zur Verfügung, damit der Datenverkehr auf die anderen Standorte verteilt werden kann. Weitere Informationen zu *Wiederherstellung nach Ausfall von AWS* finden Sie auf der Amazon-Website zum Thema Sicherheit.

Adobe-Standorte

Adobe verfügt über Büros auf der ganzen Welt. Die folgenden Prozesse und Vorgehensweisen werden zum Schutz vor Sicherheitsbedrohungen unternehmensweit angewandt:

Physische Sicherheit
An jedem Unternehmensstandort von Adobe sind rund um die Uhr Sicherheitskräfte im Einsatz. Adobe-Mitarbeiter tragen eine Schlüsselkarte mit ID für den Zugang zum Gebäude mit sich. Besucher betreten das Gebäude nur über den Haupteingang, melden sich an der Rezeption an und ab, zeigen einen temporären Besucherausweis vor und werden während der gesamten Besuchszeit von einem Mitarbeiter begleitet. Alle Server-Komponenten, Entwicklungsrechner, Telefonsysteme, Datei- und Mailserver sowie andere sensible Systeme sind zu jeder Zeit in kontrollierten Server-Räumen eingeschlossen, die nur von entsprechend autorisiertem Personal betreten werden dürfen.

Virenschutz
Adobe scannt alle eingehenden und ausgehenden geschäftlichen E-Mails auf bekannte Malware.

Adobe-Mitarbeiter

Mitarbeiterzugriff auf Kundendaten
Für die Creative Cloud verwendet Adobe segmentierte Entwicklungs- und Produktionsumgebungen, bei denen der Zugriff auf Live-Produktionssysteme auf Netzwerk- und Anwendungsebene durch technische Kontrollen begrenzt wird. Nur mit speziellen Berechtigungen können Mitarbeiter auf die Entwicklungs- und Produktionssysteme zugreifen.

Zuverlässigkeitsprüfung
Adobe führt vor jeder Neueinstellung eine Zuverlässigkeitsprüfung durch. Inhalt und Umfang des Berichts, den Adobe in der Regel einfordert, umfassen Fragen zum Bildungshintergrund, den beruflichen Werdegang, Gerichtsakten einschließlich etwaiger Vorstrafen sowie berufliche und private Referenzen – jeweils im Rahmen des geltenden Rechts. Die Zuverlässigkeitsprüfung entspricht der regulären Vorgehensweise in den USA zur Einstellung neuer Mitarbeiter. Hierzu gehören u. a. Bewerber, die Systeme verwalten oder Zugriff auf Kundendaten haben werden. Neue Mitarbeiter in Zeitarbeit unterliegen in den USA der Zuverlässigkeitsprüfung durch die jeweilige Zeitarbeitsfirma. Diese muss den Richtlinien zur Zuverlässigkeitsprüfung von Adobe entsprechen. Außerhalb der USA führt Adobe bei bestimmten neuen Mitarbeitern Zuverlässigkeitsprüfungen gemäß den Richtlinien von Adobe und dem im jeweiligen Land geltenden Recht durch.

Kündigung von Mitarbeitern
Wenn ein Mitarbeiter bei Adobe kündigt, reicht sein Vorgesetzter ein Kündigungsformular ein. Nach der Genehmigung informiert Adobe People Resources alle Beteiligten per E-Mail über spezielle Maßnahmen, die bis zum letzten Tag des Mitarbeiters zu ergreifen sind. Kündigt Adobe einem Mitarbeiter, sendet Adobe People Resources eine ähnliche E-Mail-Benachrichtigung an alle Beteiligten, in der auch Datum und Uhrzeit der Kündigung angegeben sind.

Adobe Corporate Security stellt anhand der folgenden Maßnahmen sicher, dass der Mitarbeiter nach dem letzten Beschäftigungstag keinen Zugang mehr zu vertraulichen Dateien oder Büros von Adobe hat:

- Löschung des E-Mail-Zugriffs
- Löschung des Remote-VPN-Zugriffs
- Entwertung der Zugangskarte für das Büro und das Rechenzentrum
- Beendigung des Netzwerkzugriffs

Auf Anfrage können Vorgesetzte den Sicherheitsdienst bitten, den gekündigten Mitarbeiter aus dem Büro oder Gebäude von Adobe zu begleiten.

Vertraulichkeit von Kundendaten

Adobe behandelt Kundendaten zu jeder Zeit vertraulich. Die Nutzung oder Weitergabe der im Auftrag eines Kunden erfassten Daten durch Adobe erfolgt ausschließlich im Rahmen des mit diesem Kunden abgeschlossenen Vertrags und entsprechend den *Nutzungsbedingungen* und den *Richtlinien für den Datenschutz* von Adobe.

Safe Harbor
Adobe Systems Incorporated (Adobe USA) befolgt die *zwischen den USA und der EU vereinbarte Safe-Harbor-Regelung*.

Einhaltung von Sicherheitsvorschriften

Amazon Web Services (AWS) und Rackspace weisen mit der ISO27001-Zertifizierung, dem SOC2-Bericht und anderen branchenüblichen Security Frameworks die Einhaltung von Sicherheitsstandards für Daten nach.

Adobe arbeitet derzeit an der Entwicklung, Implementierung und Optimierung der Sicherheitsprozesse und -Kontrollmechanismen für Creative Cloud-Vorgänge, um den im SOC2-Bericht bewerteten Trust Services Principles und dem Sicherheitsstandard ISO 27001 gerecht zu werden.

Fazit

Das proaktive Sicherheitskonzept und die strikten Verfahren, die in diesem Whitepaper beschrieben wurden, dienen dem Schutz Ihrer Creative Cloud-Daten. Adobe nimmt die Sicherheit Ihrer digitalen Inhalte ernst.

Weitere Informationen finden Sie unter *http://www.adobe.com/de/security*

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

3/14