# Adobe Analytics und Sicherheit – 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 Services.

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

## Adobe Analytics

Adobe Analytics ist eine Lösung zur Durchführung von Echtzeitanalysen und detaillierten Segmentierungen für alle Marketing-Kanäle. Sie ist Teil von Adobe Marketing Cloud und ermöglicht es Ihnen, durch die Sammlung und Analyse von Kundendaten Ihre Kunden gezielter anzusprechen und Ihr Marketing effektiver zu machen.

Adobe Analytics ist in drei Hauptversionen mit unterschiedlichem Funktionsumfang verfügbar:

**Adobe Analytics** vereint die Funktionen verschiedener Werkzeuge für Web-Analysen, die bislang von Adobe angeboten wurden: Reporting und Analysen (vorher in SiteCatalyst), Ad-hoc-Analysen (Discover), Report Builder (Plug-in für Microsoft Excel) und Data Warehouse (Daten-Repository). Alle diese Funktionen stehen Ihnen jetzt zentral und nahtlos in Adobe Analytics über Adobe Marketing Cloud zur Verfügung.

**Adobe Analytics – Mobile Apps** kombiniert alle Funktionen aus Adobe Analytics mit erweiterten Analysen und Interaktionsfunktionen für Apps, mit denen Sie die Anzahl der App-Downloads erhöhen, integrierte, kanalübergreifende Daten gewinnen und Ihre Anwender durch mobile Kampagnen und intelligentes Standort-Marketing an sich binden.

**Adobe Analytics Premium Complete** umfasst alle Funktionen aus Adobe Analytics und Adobe Analytics – Mobile Apps, ergänzt durch Kundenanalysen, Multi-Channel-Funktionen und statistische/prädiktive Modelle (primär mithilfe der Data Workbench), die Ihnen ein umfassenderes Bild Ihrer Kunden und deren Bedeutung für Ihr Unternehmen vermitteln. Die Adobe Analytics Premium-Bundles Predictive Intelligence, Customer 360 und Cross-Channel Attribution enthalten einen Teilbereich der Funktionalität aus Adobe Analytics Premium Complete und sind zudem für spezifische Kundenanforderungen verfügbar.

## Anwendungsarchitektur von Adobe Analytics

- **Adobe Analytics-Benutzeroberfläche** – Hier definieren die Kunden die Regeln zur Erfassung der Besucherinformationen, die gemessen und analysiert werden sollen.
- **Adobe Analytics Application Measurement** – Software, die das Verhalten und die Aktionen der Endanwender auf den Websites von Adobe Analytics-Kunden misst und sammelt.
- **RDC-Server (Regional Data Collection)** – Server, auf dem die gemessenen Verhaltens- und Aktionsdaten der Endanwender erfasst werden.
- **RDP-Server (Regional Data Processing)** – Server, auf dem die Anwenderdaten gemäß den Regeln, die der Kunde auf der Benutzeroberfläche von Adobe Analytics festgelegt hat, verarbeitet werden.

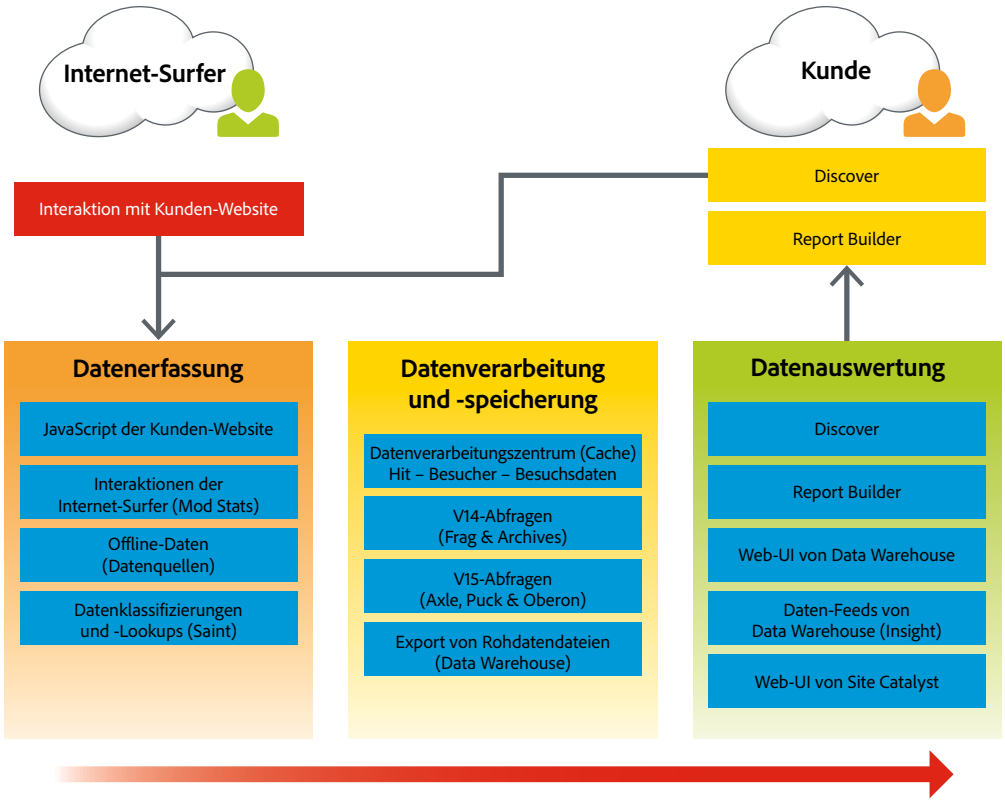



Abb. 1: Produktarchitektur und Datenfluss von Adobe Analytics

Alle Komponenten von Adobe Analytics werden in Adobe-eigenen oder von Adobe gemieteten Rechenzentren gehostet. Einzige Ausnahme ist die Software Adobe Analytics Application Measurement, die sich auf dem Webserver des Kunden befindet.

## Anwendungssicherheit und Netzwerkarchitektur von Adobe Analytics

Wenn ein Endanwender eine Website öffnet, auf der Adobe Analytics Application Measurement ausgeführt wird, sendet Adobe Analytics die gemäß Kundenanweisung erfassten Verhaltensdaten des Anwenders an die Adobe Analytics Application Measurement-Software zurück. Für die gesamte Kommunikation zwischen der Adobe Analytics Application Measurement-Software und den zugehörigen Cookies gelten dieselben Sicherheitsregeln wie für die Website des Kunden. Hat der Kunde HTTPS implementiert, wird bei der Kommunikation zwischen der Mess-Software und den Endanwender-Cookies auch HTTPS verwendet.

Bei Beendigung der Web-Sitzung sendet die Adobe App Management-Software die Verhaltensdaten des Anwenders per HTTPS an einen der weltweiten RDC-Server von Adobe.

Der RDC-Server verarbeitet die empfangenen Daten zunächst mit der Adobe Analytics-Regel-Engine für die Vorabverarbeitung. Die Engine wendet alle Regeln an, die der Kunde auf der Benutzeroberfläche definiert hat. Anschließend sendet der RDC-Server die Daten an einen der RDP-Server von Adobe. Befindet sich am Standort des RDC-Servers auch ein RDP-Server, werden die Daten dorthin gesendet. Ist dies nicht der Fall, werden die Daten an den nächstgelegenen RDP-Server gesendet und mittels HTTPS gesichert. Der RDP-Server speichert die Datenbank im Adobe Analytics-Data Warehouse auf diesem Server.

An diesem Punkt hat der Kunde verschiedene Möglichkeiten, um die mit Adobe Analytics erfassten Daten darzustellen:

- Erstellung und Anzeige formatierter Berichte mit der Adobe Analytics-Web-Applikation – alle Interaktionen mit der Adobe Analytics-Web-Applikation werden per HTTPS gesichert.
- Implementierung eines Data Warehouse-Berichtswerkzeugs, um Daten direkt aus dem Data Warehouse per HTTPS oder Secure FTP abzurufen
- Verwendung eines Rohdaten-Feeds, der in einem Cloud-basierten Data Warehouse gespeichert oder zur Visualisierung mit anderen Daten-Feeds oder -quellen zusammengeführt werden kann

## Datenfluss mit Adobe Analytics

Adobe Analytics bietet zwei primäre Verfahren für die Sammlung von Daten, mit denen die Online-Präsenzen des Kunden abgebildet werden können:

- **Direkt auf der Kunden-Website** – Mit einer Kombination aus eingebettetem JavaScript-Code auf den Web-Seiten des Kunden, angepassten URLs und HTTP-Headern sowie beständigen Cookies sammeln die Adobe Analytics-Server Informationen über die Handlungen und das Verhalten des Anwenders bei der Interaktion auf der Kunden-Website. Diese Informationen werden an die Datenerfassungs-Server von Adobe Analytics mit der geringsten Entfernung zum Standort der Aktivität übergeben. Die Server übertragen diese Daten dann an das Adobe Analytics Data Processing Center (DPC), wo mit ihrer Aufbereitung begonnen wird. Die Standorte dieser Server werden später in diesem Dokument erläutert.
- **Aus anderen Kanälen als Websites** – Adobe Analytics unterstützt die Datenerfassung und -analyse über SFTP-Schnittstellen (Secure File Transfer Protocol). Die Kunden stellen diese Daten in einem vorgegebenen Dateiformat mit den erforderlichen Klassifikationen bereit und laden sie sicher über diese Schnittstelle hoch.

Sobald die Daten an Adobe gesendet wurden, werden sie im Adobe-Data Warehouse für das Reporting analysiert und zusammengestellt. Für den Zugriff auf die im Data Warehouse aufbereiteten und gespeicherten Daten stehen folgende Optionen zur Auswahl:

- **Web-Schnittstelle zur Marketing Cloud** – Diese Oberfläche ermöglicht die Erstellung von Berichten, Ad-hoc-Abfragen und anderen Analysen der im Adobe-Data Warehouse gespeicherten Daten. Dies ist die gängigste Form des Zugriffs auf Daten in Adobe Analytics.
- **Web-Oberfläche direkt im Data Warehouse** – Hier können Kunden die Rohdaten direkt bearbeiten und komplexere Berichte und Feeds als über die Marketing Cloud-Schnittstelle generieren.
- **Adobe Analytics-Desktoptool für Ad-hoc-Analysen** – Mit diesem Tool können Kunden schnell erweiterte Analysen der Aktivitätsdaten ihrer Websites durchführen, u. a. durch die gleichzeitige Anzeige mehrerer Berichte, die Segmentierung nach Dimensionen (Kampagnen, Produkte, Seiten usw.) sowie die Darstellung aus der Mikro- und Makroperspektive, um Effekte auf die Zielkennzahlen zu evaluieren. Kunden erhalten mit diesen Funktionen aussagekräftige Werte zu Traffic, Grafiken, Umsatz und Produktbewegung.
- **Excel-Plug-in** – Das Plug-in ermöglicht die Bearbeitung und Auswertung von Daten mit den Funktionen in Microsoft Excel.
- **Download von Rohdaten aus dem Data Warehouse** – Kunden können ihre eigenen erweiterten Analyse- und Berichts-Suiten für die Verarbeitung der Analytics-Daten nutzen.

### Datenfluss mit Adobe Analytics Premium

Adobe Analytics Premium bietet mit der Data Workbench ein zusätzliches Desktoptool, mit dem die gesammelten Daten und die Applikations-Services noch intensiver genutzt werden können. Der Datenfluss und die Zugriffsoptionen bei Verwendung der Data Workbench unterscheiden sich teilweise von Adobe Analytics.

- **Daten-Feeds** – Die meisten Quellprotokolldaten stammen von Daten-Feeds aus Adobe Analytics. Die Adobe Analytics-Daten werden in den Datenverarbeitungszentren für Analytics erfasst und gespeichert. Die Daten-Feeds können für eine Einspeisung in die Data Workbench-Cluster eingerichtet werden und werden dann intern mittels Secure FTP von den Analytics-Servern direkt an die Data Workbench gesendet.
- **Sensor** – Beim Einsatz von Sensoren erfolgt die Datenerfassung direkt in der Data Workbench. Die Sensoren können auf den Web-Servern beim Kunden gehostet und direkt an die gehostete Adobe-FSU (File Server Unit) gesendet werden. Alternativ können sie auch als dedizierte Server von Adobe gehostet werden. In beiden Fällen werden die Sensordaten im NAS (Network Attached Storage) gespeichert.
- **Offline-Daten** – Kunden können Daten aus verschiedenen Quellen hochladen. Meist werden jedoch Flat Files verwendet. Die Daten können über FTP oder sFTP an die gemeinsame FTP-Infrastruktur für Produkte gesendet werden. Skripte auf DWB-Servern (Data Workbench) rufen die Daten dann vom FTP-Server in die DWB-Umgebung ab. Darüber hinaus können die Kunden bestimmte Dateien über die DWB Client-Oberfläche hochladen, wie z. B. Lookup-Dateien.
- **Konfigurationsdaten** – Kunden können Regeln einrichten, die das Lesen, Filtern und Verarbeiten der Daten definieren. Diese Regeln werden als Konfigurationsdateien auf der FSU gespeichert. Die Konfigurationsdaten auf den Produktions-Servern werden extern gesichert und gespeichert. Kunden können neue Regeln hochladen und ein Neuverarbeitungsereignis auslösen, das die Quellprotokolldaten entsprechend den Regeln abruft. Das resultierende Daten-Set wird in mindestens einer DPU (Data Processing Unit) gespeichert und kann dann vom Kunden abgerufen/verwendet werden.
- **Daten-Set** – Diese Daten befinden sich auf den DPUs. Die Daten verwenden ein proprietäres Datenbankformat der Data Workbench. Sie können über die Client-Software der DWB-Workstations, über eine API oder über einen Berichts-Server, der gespeicherte Abfragen ausführt und Berichte per E-Mail verteilt, abgerufen werden.
- **Datenexport** – Kunden können die Daten aus einem DWB-Daten-Set exportieren und an externe Systeme senden. Das kann über Secure FTP direkt aus einem Server in einem DWB-Cluster oder über die gemeinsame FTP-Infrastruktur für Produkte erfolgen.

## Authentifizierung über Adobe Marketing Cloud

Für den Zugriff auf Adobe Analytics ist eine Authentifizierung mit Benutzernamen und Kennwort erforderlich. Bei der Anmeldung mit einer Adobe-ID verwendet Adobe den Hash-Algorithmus SHA 256 in Kombination mit Kennwort-Salts und einer Vielzahl an Hash-Iterationen. Unsere Entwickler-Teams implementieren kontinuierlich neue Schutzmechanismen, um auf der Basis neuester Authentifizierungsstandards die höchstmögliche Sicherheit bieten zu können.

Anwender können über eine von drei anwendergebundenen Lizenzen auf Adobe Analytics zugreifen:

Die **Adobe ID** ist ein von Adobe gehosteter und von Einzelanwendern erstellter und verwalteter Account.

Die **Enterprise ID** ist ein von Adobe gehosteter und vom IT-Administrator des Abonnenten erstellter und verwalteter Account. Die Organisation ist Eigentümer der Anwender-Accounts und aller zugehörigen Inhalte, während Adobe die Enterprise ID hostet und die Authentifizierung durchführt. Administratoren können die Zugriffsberechtigung für Adobe Analytics aufheben, indem sie den Account übernehmen oder die Enterprise ID löschen und so den Zugriff auf die zugehörigen Daten dauerhaft sperren.

Die **Federated ID** ist ein vom Unternehmen verwalteter Account, bei dem alle Identitätsprofile und zugehörigen Inhalte vom internen Identitäts-Management-System über Single Sign-on (SSO) bereitgestellt werden. Sämtliche Accounts werden von der IT erstellt und verwaltet. Adobe unterstützt die meisten Anbieter für SAML 2.0-Authentifizierung.

Die Berechtigungen für den Zugriff auf Applikationen und Services werden über das Adobe Enterprise Dashboard erteilt. Informationen zum Dashboard erhalten Sie unter *https://helpx.adobe.com/de/enterprise/help/aedash.html*.

Weitere Informationen über spezielle Zugriffsverfahren für Adobe Analytics-Daten und -Berichte über genehmigte Applikationen finden Sie in der Produktdokumentation unter *https://marketing.adobe.com/resources/help/de_DE/sc/user/home.html*.

## Hosting-Rechenzentren für Adobe Analytics

Adobe Analytics wird auf Adobe-eigenen Servern gehostet und verwaltet. Einige Standorte verfügen über Zentren für Datenerfassung und Datenverarbeitung. Die fünf Standorte mit beiden Arten von Zentren werden in der folgenden Karte als **Core und Edge**-Standorte aufgeführt.

Die sechs Standorte, die lediglich ein Datenerfassungszentrum mit einem oder mehreren Datenerfassungs-Servern aufweisen, werden in der folgenden Karte als **Edge**-Standorte aufgeführt.

Jedes vom Kunden definierte Datenerfassungssegment (Report Suite) wird einem bestimmten Datenverarbeitungszentrum zugewiesen, das der Kunde bei der Implementierung ausgewählt hat. Daher kann es vorkommen, dass Hits, die in einem Datenerfassungszentrum in Singapur erfasst wurden, zur Verarbeitung in die USA gesendet werden, obwohl es ein Datenverarbeitungszentrum vor Ort gibt.


Abb. 2: Adobe-Netzwerk für regionale Datenerfassung

### Prozess zur Erfassung regionaler Daten

Die Datenerfassung von Adobe beinhaltet folgende Schritte:

1. Zuerst muss der Adobe Analytics-Kunde seinen Adobe-Erfassungscode ändern (s_code.js oder AppMeasurement.js, AppMeasurement-Bibliotheken, mobile SDK-Konfiguration usw.), um die RDC-Domäne omtrdc.net zu verwenden.
2. Dann ordnet Adobe mittels erweiterter DNS-Technologie (Domain Name Service) die RDC-Domäne dem nächstgelegenen Datenerfassungszentrum des Besuchers zu.
3. Wenn ein Hit gesendet wird, wird die Adobe-Bildanforderung automatisch an das RDC weitergeleitet, dass dem Besucher am nächsten liegt.
4. Das RDC-Zentrum leitet die Daten über einen sicheren Datenkanal an das regionale Datenverarbeitungszentrum weiter, wo sie verarbeitet und für Adobe Analytics und andere Produkte von Adobe Marketing Cloud (je nach Kundenwunsch) bereitgestellt werden.
5. Die RDC-Domäne leitet auch Anforderungen der Dateneinfüge-API über das nächste Datenerfassungszentrum weiter. Zwischen dem Browser und dem Datenerfassungszentrum werden nur HTTPS-Hits verschlüsselt. Alle Daten, die von RDC-Standorten an DPC-Standorte gesendet werden, werden ebenfalls per HTTPS verschlüsselt.

Sollte die Kommunikation zwischen Datenerfassungszentrum und Datenverarbeitungszentrum (DPC) unterbrochen werden, versucht die RDC-Infrastruktur von Adobe, die Daten über ein anderes Datenerfassungszentrum an das DPC zu senden. Die Daten werden lokal gespeichert und an das DPC weitergeleitet, wenn die Kommunikation wiederhergestellt wurde. Aufgrund des begrenzten Speicherplatzes steht diese Option nur für kurzzeitige Unterbrechungen zur Verfügung.

Bei längeren Ausfällen konfiguriert das Adobe Network Operations-Team das vom RDC verwendete globale DNS-System um, damit die Daten über ein anderes Datenerfassungszentrum weitergeleitet werden.

## Adobe Analytics-Netzwerk-Management

Da über das Adobe Analytics-Netzwerk Daten gesammelt, bereitgestellt und für Auswertungen aufbereitet werden, hat seine Sicherheit hohe Priorität. In der Netzwerkarchitektur sind daher Best Practices der Branche für Sicherheits-Design implementiert, darunter die Segmentierung der Entwicklungs- und Produktionsumgebungen, DMZ-Segmente, gehärtete Bastion Hosts und eindeutige Authentifizierung.

### Trennung der Client-Daten

Die Daten werden in separaten Datenbanken (Report Suites) abgelegt, wobei die Berichte der einzelnen Client-Adressen auf einem oder mehreren Servern gruppiert werden. In einigen Fällen können mehrere Clients einen Server gemeinsam verwenden. Die Daten werden jedoch stets in separaten Datenbanken gehalten. Die einzige Zugriffsmöglichkeit auf diese Server und Datenbanken besteht über die Analytics-Anwendung per Secure Access. Sonstige Zugriffe auf die Anwendungs- und Daten-Server erfolgen ausschließlich durch autorisierte Adobe-Mitarbeiter über verschlüsselte Kanäle in geschützten Management-Verbindungen. Durch die Trennung von Test- und Produktionsumgebungen wird außerdem verhindert, dass Kundendaten in Testumgebungen verwendet werden.

### Sicheres Management

Adobe unterhält dedizierte Netzwerkverbindungen zwischen den Niederlassungen und Rechenzentren, um eine sichere Verwaltung der Adobe Analytics-Server zu gewährleisten. Alle Management-Zugriffe auf die Server erfolgen über verschlüsselte SSH- (Secure Shell), SSL- (Secure Sockets Layer) oder VPN-Verbindungen (Virtual Private Networks). Bei einem Fernzugriff ist immer eine Zwei-Faktor-Authentifizierung erforderlich. Adobe gewährt keinen Management-Zugriff für Verbindungen aus dem Internet, es sei denn, die Verbindung erfolgt von einer vertrauenswürdigen IP-Adresse.

### Firewalls und Load-Balancer

Die im Netzwerk aktiven Firewalls für Adobe Analytics blockieren alle Internet-Verbindungen, die andere Ports verwenden als die hierfür freigegebenen Ports 80 für HTTP und 443 für HTTPS. Zusätzlich führen sie NAT-Services (Network Address Translation) aus. Mit NAT wird die echte IP-Adresse eines Servers vor dem Client, der die Verbindung aufbauen möchte, verborgen. Die Load-Balancer fungieren als Proxy-Server für eingehende HTTP-/HTTPS-Verbindungen und verteilen Anfragen weiter, sodass das Netzwerk auch temporäre Lastspitzen ohne Performance-Einbußen bewältigen kann. Firewalls und Load-Balancer sind vollständig redundant implementiert. So ist die Gefahr geringer, dass durch den Ausfall einer einzelnen Komponente der gesamte Datenverkehr lahmgelegt wird.

### Nicht Routing-fähige private Adressen

Die Kundendaten von Adobe Analytics werden auf Servern mit nicht Routing-fähigen IP-Adressen (RFC 1918) verwaltet. Diese privaten Adressen in Kombination mit den Firewalls und der NAT-Funktionalität von Adobe Analytics schützen die einzelnen Server im Netzwerk vor direkten Anfragen aus dem Internet und verringern so die Gefahr von Angriffen.

### Intrusion Detection

Adobe setzt an kritischen Punkten des Adobe Analytics-Netzwerks IDS-Sensoren (Intrusion Detection System) ein. Diese erkennen nicht autorisierte Zugriffsversuche auf das Netzwerk und alarmieren umgehend das Sicherheits-Team. Dieses Team geht allen Angriffsmeldungen nach, indem der Alarm überprüft und die betroffene Plattform auf Anzeichen einer Gefährdung untersucht wird. Die Sensoren des Systems werden überwacht und in regelmäßigen Abständen auf den neuesten Stand gebracht.

### Service-Monitoring

Alle Server, Router, Switches, Load-Balancer und andere wichtige Komponenten des Adobe Analytics-Netzwerks werden rund um die Uhr überwacht. Die Meldungen der verschiedenen Überwachungssysteme gehen beim Adobe Network Operations Center (NOC) ein, das mögliche Probleme umgehend behebt oder an die verantwortlichen Adobe-Mitarbeiter weiterleitet. Die Überwachung wird durch zahlreiche externe Partner zusätzlich verstärkt.

### Backups

Adobe sichert täglich Snapshots der Kundendaten für Adobe Analytics. Jeder Snapshot wird bis zu sieben Tage gespeichert. Die Kombination verschiedener Backup-Verfahren ermöglicht schnelle Wiederherstellungen von Kurzzeit-Backups sowie eine externe Sicherung der Daten.

### Change Management

Alle Eingriffe werden mithilfe eines Werkzeugs für die Änderungsverwaltung geplant, um die Kommunikation zwischen Teams, die gemeinsame Ressourcen verwenden, zu verbessern. Betroffene Parteien erhalten Benachrichtigungen über anstehende Änderungen. Das Tool findet auch bei geplanten Wartungsarbeiten Anwendung, z. B., um Totalabschaltungen nicht in Zeiten mit hohem Netzwerkverkehr zu legen.

### Patch-Management

Adobe setzt interne Repositorys und ein branchenübliches Konfigurations-Management-System für Patches und Pakete ein, um die Verteilung von Patches an Host-Computer innerhalb der Analytics-Organisation zu automatisieren. Je nach Funktion des Hosts und der Wichtigkeit anstehender Patches werden die Patches zum Zeitpunkt ihrer Veröffentlichung und nach einem festgelegten Zeitplan an die Hosts verteilt. Im Bedarfsfall erfolgt die Verteilung sicherheitsrelevanter Patches auch kurzfristig.

### Zugriffssteuerung

Nur autorisierte Anwender innerhalb des Adobe-Intranet und externe Anwender, die über einen mehrstufigen Authentifizierungsprozess eine VPN-Verbindung aufgebaut haben, haben Zugriff auf die Administrationswerkzeuge. Für Audits protokolliert Adobe darüber hinaus alle Verbindungen zum Produktions-Server von Adobe Analytics.

### Protokolle

Schutz vor nicht autorisierten Zugriffen und Änderungen bieten Netzwerk- und OS-bezogene Protokolle sowie Intrusion Detection-Systeme. Der für die Protokolle notwendige Speicherplatz wird festgelegt, regelmäßig überprüft und gegebenenfalls erweitert, um eine zuverlässige Speicherung der Log-Dateien sicherzustellen. Die vom System generierten Protokolle werden speziell gesichert, und der Zugriff auf die Protokolle und die Protokollierungs-Software ist auf autorisierte Mitarbeiter des Adobe Digital Marketing Information Security-Teams beschränkt. Adobe bewahrt die Originalprotokolle ein Jahr lang auf.

## Adobe Analytics-Sicherheitsfunktionen für Administratoren

Adobe Analytics bietet Administratoren umfassende Funktionen zur Steuerung des Zugriffs auf Berichtsdaten, wie z. B. sichere Kennwörter, befristete Gültigkeit von Kennwörtern sowie Einschränkungen für IP-Anmeldungen und E-Mail-Domänen. Weitere Informationen erhalten Sie unter *https://marketing.adobe.com/resources/help/de_DE/reference/security_manager.html*.

## Physische Sicherheit und Umgebungssicherung in Adobe-Rechenzentren

Die im Folgenden beschriebenen physischen und umgebungsbedingten Zugriffskontrollen gelten für alle Rechenzentren von Adobe. Einige Standorte setzen darüber hinaus weitere Kontrollmechanismen ein, die hier nicht behandelt werden.

### Physische Sicherheit

Die gesamte Hardware in Adobe-eigenen und von Adobe gemieteten Räumlichkeiten ist physisch gegen unbefugte Zugriffe abgesichert. An allen Standorten mit Produktions-Servern für Adobe Analytics ist rund um die Uhr Sicherheitspersonal im Einsatz, das stets über aktuelle Zugangsberechtigungen verfügen muss. Diese bestehen aus einer PIN, einer Zugangskarte oder einer Kombination aus beiden, ohne die kein Zugang zum jeweiligen Rechenzentrum gewährt wird. Alle Zugangsberechtigten sind auf einer genehmigten Liste autorisierter Personen verzeichnet. Einige Standorte verfügen zudem über Sicherheitsschleusen, die verhindern, dass eine nicht autorisierte Person gemeinsam mit einer berechtigten Person ein Gebäude betritt.

### Brandbekämpfung

Alle Rechenzentren müssen mit einer Rauchmeldeanlage ausgestattet sein, die die Luft permanent analysiert und bei Brandgefahr sofort Alarm auslöst. Darüber hinaus muss eine doppelt gesicherte vorgesteuerte Trockensprinkleranlage installiert sein, mit der gewährleistet ist, dass kein Wasser in einen Server-Bereich abgegeben wird, ohne dass zuvor ein Feueralarm ausgelöst und eine Hitzeentwicklung festgestellt wurde.

### Raumklima und -temperatur

Alle Rechenzentren müssen über Klimaanlagen mit Luftfeuchtigkeitsregelung und Flüssigkeitsdetektoren verfügen, die das Raumklima und die Temperatur überwachen. Ein vollständig redundantes HLK-System (Heizung, Lüftung, Klima) wird rund um die Uhr von Fachpersonal betreut, das im Fall von Störungen umgehend eingreift. Falls sich die Umgebungsparameter außerhalb eines von Adobe definierten Toleranzbereichs bewegen, werden sowohl Adobe als auch das zuständige Network Operations Center (NOC) alarmiert.

### Videoüberwachung

An Standorten, an denen Produkt-Server für Adobe Analytics betrieben werden, muss zumindest an Ein- und Ausgängen Videoüberwachung eingesetzt werden. Für Rechenzentren fordert Adobe zudem, dass der manuelle Zugriff auf die Geräte überwacht wird, um bei Problemen oder Verdacht auf Verletzung von Zugriffsbeschränkungen die Videoprotokolle ggf. zu überprüfen.

### Permanente Stromversorgung

Durch mehrere Versorgungsleitungen aus voneinander unabhängigen Stromversorgungszentren wird sichergestellt, dass in allen von Adobe betriebenen Rechenzentren eine permanente Stromversorgung gewährleistet ist. In Notfällen sorgen Notstromanlagen automatisch für eine unterbrechungsfreie Stromzufuhr. Adobe schreibt für alle Rechenzentren den Betrieb redundanter Komponenten auf allen Ebenen vor, einschließlich Generatoren und Liefervereinbarungen für Dieseltreibstoff. Die Generatoren müssen an allen Standorten regelmäßig unter Volllast getestet werden, um ihre einwandfreie Funktionsweise sicherzustellen.

### Disaster Recovery

Wenn aufgrund einer Störung eine der Datenerfassungsumgebungen nicht verfügbar sein sollte, z. B. bei einem Standortproblem oder einem lokalen bzw. regionalen Störfall, stellt Adobe mit dem hier beschriebenen Prozess sicher, dass die Datenerfassung fortgeführt und Daten effizient und vollständig wiederhergestellt werden.

**Failover-Prozess**

Im Fall von Ereignissen, die zu einer längeren Unterbrechung der Datenerfassung führen können, konfiguriert Adobe das DNS neu, damit die Erfassungsanforderungen an einen anderen, nicht betroffenen Standort gesendet werden. Adobe sperrt zudem manuell die Datenverarbeitung am ersten Standort, um die chronologische Reihenfolge der Seitenaufrufe beizubehalten, was für einen erfolgreichen Wiederherstellungsprozess erforderlich ist.

Die Angabe der TTL (Time To Live) für den DNS-Datensatz ermöglicht einen schnellen Wechsel zum zweiten Standort. Bei Kunden mit regionaler Datenerfassung (RDC) werden die Daten unverändert in die Warteschlange gelegt, falls das Datenverarbeitungszentrum vorübergehend nicht erreichbar sein sollte. Sollte ein RDC-Standort ausfallen, wird die Datenerfassung an anderen RDC-Standorten fortgesetzt. Solange sich die Datenerfassung im Failover-Modus befindet, werden die Kunden regelmäßig über den aktuellen Status informiert. Wenn der erste Datenerfassungsstandort voraussichtlich innerhalb von fünf Geschäftstagen wieder online ist, werden keine historischen Daten an den zweiten Standort übermittelt oder Daten dort erfasst. Falls die Störung am ersten Standort so gravierend ist, dass die historischen Daten dort zerstört wurden oder nicht mehr verfügbar sind, stellt Adobe diese Daten aus Backups wieder her, die an externen Standorten gespeichert wurden.

**Recovery-Prozess**
Sobald der primäre Datenerfassungsstandort wieder verfügbar und stabil ist, wird der Failover-Prozess umgekehrt. Der gesamte am zweiten Standort erfasste Traffic wird mit den Daten am primären Standort zusammengeführt, die DNS-Datensätze werden wiederhergestellt und die Seitenaufrufe werden in zeitlicher Reihenfolge sequenziell verarbeitet. Während der Verarbeitung der Seitenaufrufe ist Analytics zwar verfügbar, doch werden die Berichte erst nach Abschluss der Verarbeitung wieder in Echtzeit bereitgestellt. Vier Stunden eines aktiven Failover-Prozesses erfordern etwa einen Tag zur Verarbeitung der Seitenaufrufe. Die Wiederherstellung der historischen Daten von externen Standorten kann bis zu zehn weitere Tage in Anspruch nehmen.

## Die Adobe-Sicherheitsorganisation

Sämtliche Maßnahmen zur Erhöhung der Sicherheit der Produkte und Services von Adobe werden vom Chief Security Officer (CSO) koordiniert. Das Büro des CSO ist für alle Sicherheitsinitiativen für Produkte und Services sowie die Implementierung des 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 Analytics-Teams, beratend zur Seite stehen. Die ASSET-Experten arbeiten mit verschiedenen Produkt- und Entwickler-Teams von Adobe zusammen, um bei allen Produkten und Services das gewünschte Maß an Sicherheit zu erreichen. Sie empfehlen Sicherheitsmaßnahmen mit klar strukturierten und reproduzierbaren Prozessen in den Bereichen Entwicklung, Bereitstellung, Betrieb und Fehlerbehebung.

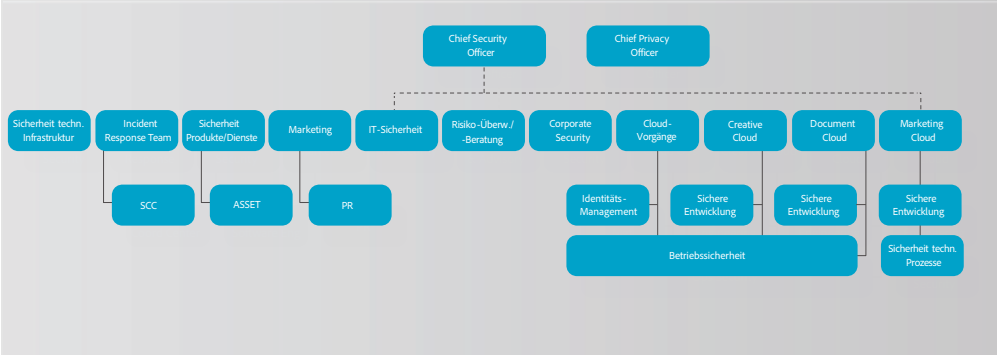



Abb. 3: Adobe-Sicherheitsorganisation

## Entwicklung sicherer Adobe-Produkte

Wie bei anderen wichtigen Produkten und Services von Adobe wird für die Adobe Analytics-Organisation der SPLC-Prozess (Adobe Secure Product Lifecycle) angewendet. 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 Design und Entwicklung bis hin zu Qualitätssicherung, Test und Bereitstellung. Die Sicherheitsexperten des ASSET geben im Rahmen des SPLC-Programms nach Bewertung potenzieller Sicherheitsrisiken Empfehlungen für einzelne Produkte und Services. Das Programm wird u. a. dank der regelmäßigen Einbindung der Community kontinuierlich weiterentwickelt und ist somit in Bezug auf Technologien, Sicherheitsmethoden und Bedrohungen stets auf dem neuesten Stand.

### Adobe Secure Product Lifecycle

Die Adobe SPLC-Aktivitäten umfassen, je nach betroffener Adobe Analytics-Komponente, 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 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

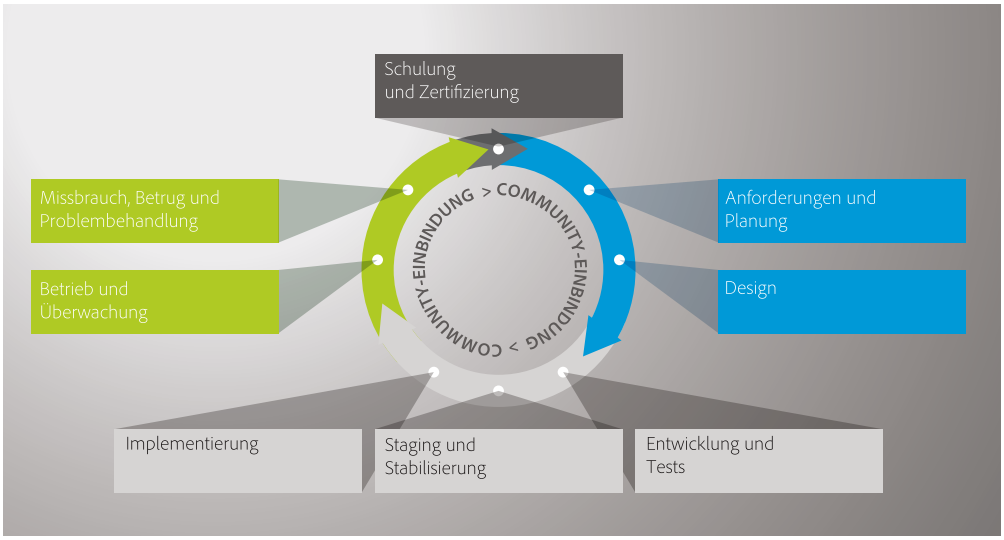



Abb. 4: Adobe Secure Product Lifecycle (SPLC)

## 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.

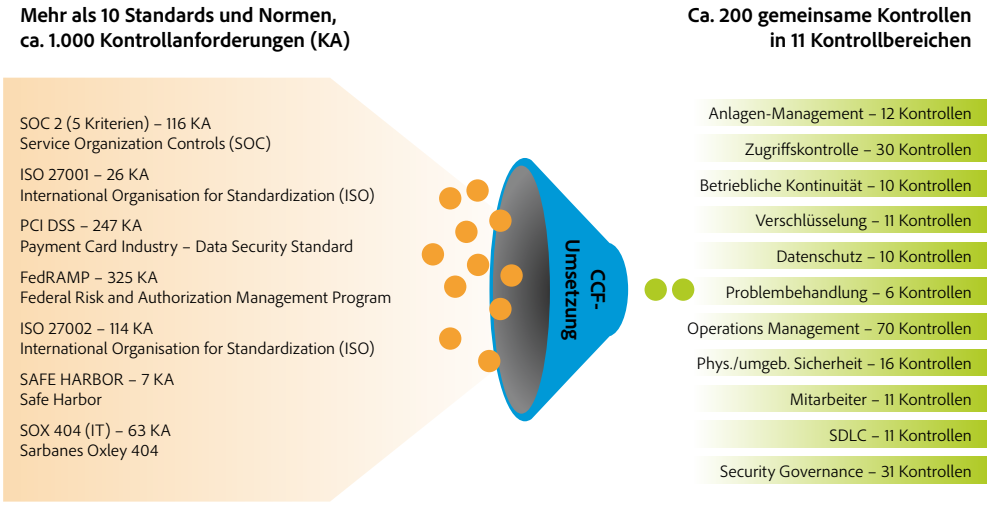
Das Programm umfasst vier Stufen, die jeweils durch einen farbigen „Gürtel" gekennzeichnet sind: weiß, grün, braun und schwarz. Die weiße und die grüne Stufe werden durch den Abschluss Computer-gestützter Schulungen erreicht. Die braune und schwarze Stufe erfordern die Teilnahme an Sicherheitsprojekten, 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 Adobe Analytics-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 Common Controls Framework

Zum Schutz der Software-Ebene verwendet Adobe das Programm Secure Product Lifecycle, das im folgenden Absatz beschrieben wird. Für den Schutz auf physischer Ebene implementiert Adobe ein grundlegendes Framework mit Sicherheitsprozessen und Kontrollmechanismen, die den Schutz der Infrastruktur sowie der Programme und Services des Unternehmens und die Einhaltung zahlreicher branchenüblicher Best Practices, Standards und Zertifizierungen gewährleisten.

Bei der Entwicklung des Adobe Common Controls Framework (CCF) hat Adobe die Kriterien gängiger Sicherheitsstandards analysiert und eine Reihe von Überschneidungen identifiziert. Mehr als 1000 Anforderungen relevanter Cloud-Sicherheits-Frameworks und -Standards wurden analysiert und in etwa 200 Adobe-spezifischen Kontrollmechanismen zusammengefasst. Die Entwickler des CCF sind bestens vertraut mit den Erwartungen unserer Partner und Kunden, wenn es um die Implementierung von Kontrollmechanismen geht.




## Risiko- und Schwachstellen-Management bei Adobe

Unser Ziel sind kurze Reaktionszeiten, erfolgreiche Risikominderung und effektive Fehlerbehebung. Im Rahmen des Risiko- und Schwachstellen-Managements überwachen wir die aktuelle Bedrohungslage, tauschen Informationen mit Sicherheitsexperten auf der ganzen Welt aus, beheben Vorfälle innerhalb kürzester Zeit und leiten sämtliche Informationen an unsere Entwickler-Teams weiter. So erzielen wir für alle Adobe-Produkte die größtmögliche Sicherheit.

### Penetrationstests

Adobe beauftragt führende Sicherheitsunternehmen mit der Durchführung von Penetrationstests, um potenzielle Sicherheitslücken aufzudecken und die Sicherheit von Produkten und Services von Adobe insgesamt zu verbessern. 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.

Vor jedem Release führt das Sicherheits-Team für Adobe Analytics eine Risikoeinschätzung aller Analytics-Komponenten durch. Diese wird von hochqualifizierten Mitarbeitern durchgeführt, die für den Aufbau einer sicheren Netzwerktopologie und -infrastruktur sowie den Schutz der Analytics-Applikation verantwortlich sind. Dabei werden etwaige Sicherheitslücken in der Netzwerkstruktur einschließlich Firewalls, Load-Balancer und Server-Hardware sowie Schwachstellen auf Anwendungsebene ermittelt. Im Rahmen dieser Maßnahmen werden Threat-Modeling-Aktivitäten und Scans zur Ermittlung von Sicherheitslücken sowie statische/dynamische Applikationsanalysen durchgeführt. Das Sicherheits-Team für Analytics arbeitet gemeinsam mit den Leitern für Technik/IT und Entwicklung vor jedem Release an der Behebung aller riskanten Schwachstellen.

### Problembehandlung und Benachrichtigung

Jeden Tag werden neue Sicherheitslücken und Bedrohungen erkannt. Adobe reagiert so schnell wie möglich darauf. 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 Analytics, informiert das Adobe Product Security Incident Response Team (PSIRT) die entsprechenden Analytics-Teams, um die erforderlichen Maßnahmen zu koordinieren.

Für On-Demand-Services von Adobe wie Adobe Analytics 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 Services)
- 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 von Vorfällen verwendet das Analytics-Team den forensischen Analyseprozess, der ein vollständiges Image bzw. ein Speicherabbild des/r betroffenen Rechner(s), eine sichere Beweisaufbewahrung sowie eine lückenlose Dokumentation der Überwachungskette umfasst.

## Adobe-Firmenstandorte

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

### 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 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 Adobe Analytics verwendet Adobe segmentierte Entwicklungs- und Produktionsumgebungen, bei denen der Zugriff auf Live-Produktionssysteme auf Netzwerk- und Anwendungsebene durch technische Kontrollen begrenzt wird. Die Mitarbeiter verfügen über spezifische Autorisierungen für den Zugriff auf Entwicklungs- und Produktionssysteme. Mitarbeiter ohne legitimen geschäftlichen Grund können nicht auf diese Systeme 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
- Aufhebung 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 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 Datenschutzrichtlinien von Adobe.

### Einhaltung von Sicherheitsvorschriften

Sämtliche Services von Adobe unterliegen umfassenden, dokumentierten Sicherheitsverfahren. Zur Erhaltung und Verbesserung der Qualität der Services wurden diese bereits zahlreichen Sicherheitsprüfungen unterzogen. Die Adobe-Services unterliegen fortlaufend Überprüfungen nach der ISO 27001-Norm. Die der „Shared Cloud“ zugrunde liegende Services-Infrastruktur verfügt über die SOC2-Sicherheitszertifizierung.

## Fazit

Das proaktive Sicherheitskonzept und die strikten Verfahren, die in diesem Whitepaper beschrieben wurden, dienen dem Schutz von Adobe Analytics und Ihrer vertraulichen Daten. Adobe nimmt die Sicherheit Ihrer digitalen Inhalte sehr ernst. Die weltweiten Bedrohungen werden fortlaufend beobachtet, um kriminellen Aktivitäten stets einen Schritt voraus zu sein und die Sicherheit der Kundendaten zu gewährleisten.

Weitere Informationen finden Sie unter *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*



8/16