Adobe Campaign und Sicherheit – Überblick

Inhalt

Sicherheit bei Adobe

Adobe nimmt die Sicherheit Ihrer digitalen Inhalte ernst. Bei Adobe sind Sicherheitsmaßnahmen ein fester Bestandteil der Software-Entwicklung, Prozesse und Applikationen. Sie werden von interdisziplinären Teams konsequent umgesetzt, um etwaigen Zwischenfällen vorzubeugen, diese aufzudecken und angemessen darauf zu reagieren. Darüber hinaus halten wir uns durch Kooperation mit Partnern, Experten und anderen Unternehmen über aktuelle Bedrohungen und Schwachstellen auf dem neuesten Stand und integrieren fortlaufend hochentwickelte Sicherheitstechnologien in unsere Produkte und Services.

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

Adobe Campaign

Mehr als 650 weltweit führende Marken vertrauen Adobe Campaign. Die Lösung bietet herausragende Funktionen für die Verwaltung von E-Mail-Kampagnen, Angeboten und Personalisierungen für die Automatisierung und Ausführung von kanalübergreifenden Marketing-Programmen. Mit Adobe Campaign können Marketer eine ihrer größten Herausforderungen bewältigen: die Entwicklung und den Ausbau von Kundenbeziehungen, um den Umsatz und ROI zu steigern. Durch die Möglichkeit, die Bereitstellung auf die eigene Marketing-Strategie, IT-Infrastruktur sowie interne und gesetzliche Vorgaben abzustimmen, empfiehlt sich Adobe Campaign als vollständig integrierte und gleichzeitig flexible Lösung für die Kampagnenerstellung, die als einzige vier Implementierungsmodelle bietet: vor Ort, on demand, als verwalteter Dienst (Managed Service) oder als Hybridmodell.

Anwendungsarchitektur von Adobe Campaign und Implementierungsmodelle

Die gängige Implementierung von Adobe Campaign umfasst folgende Komponenten:

Personalisierte Umgebung für Kunden – Eine intuitive grafische Oberfläche erleichtert Kunden die Veröffentlichung und Verfolgung von Marketing-Angeboten, die Erstellung von Kampagneninhalten, die Prüfung und Verwaltung von Marketing-Maßnahmen, -Programmen und -Kampagnen (inklusive E-Mails, Workflows und Landingpages), die Erstellung und Verwaltung von Kundenprofilen sowie die Zielgruppendefinition.

Entwicklungsumgebung – Über Server-seitig implementierte Software werden Marketing-Kampagnen auf Basis benutzerdefinierter Regeln und Workflow-Vorgaben für festgelegte Kanäle wie E-Mail, SMS, Direkt-Mail, Callcenter, Web, Push-Benachrichtigungen und/oder Social Media durchgeführt.

Datenbank-Container – Die auf relationaler Datenbanktechnologie basierende Adobe Campaign-Datenbank speichert alle Kundendaten, kampagnenrelevanten Komponenten, Angebote und Workflows sowie Kampagnenresultate in kundenspezifischen Datenbank-Containern.

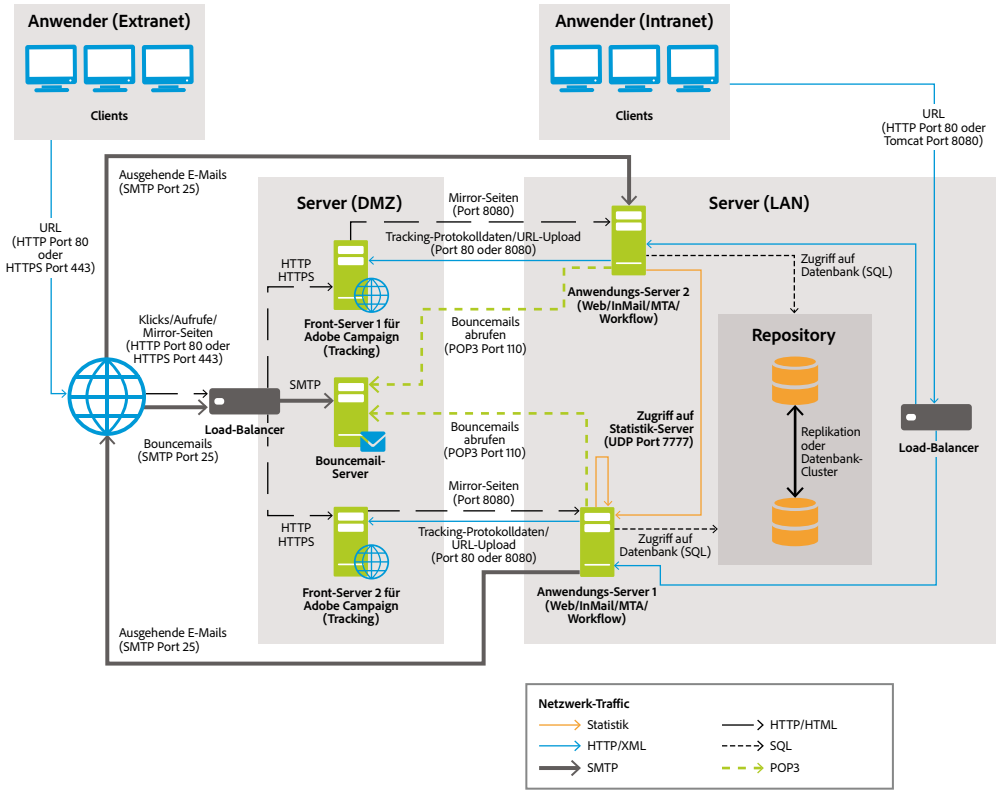

Abb. 1: Adobe Campaign-Anwendungsarchitektur

Implementierungsmodelle

Die Implementierung von Adobe Campaign kann vor Ort, on demand, als verwalteter Dienst oder als Hybridmodell ausgeführt werden.

Bei der Implementierung als verwaltetem Dienst (Managed Service) werden alle Komponenten von Adobe Campaign wie die Benutzeroberfläche, die Engine für die Ausführungsverwaltung sowie die Kampagnendatenbank des Kunden in einem von Adobe verwalteten Rechenzentrum gehostet. Adobe verfügt auf der ganzen Welt über Rechenzentren (siehe Abschnitt „Hosting-Rechenzentren für Adobe Campaign"). Dabei kommt ein Rechenzentrum in der Region des Kunden zum Einsatz (z. B. Nordamerika, Europa oder Australien).

Bei der Vor-Ort-Implementierung bleiben alle Komponenten von Adobe Campaign wie die Benutzeroberfläche, die Engine für die Ausführungsverwaltung und die Datenbank im Rechenzentrum des Kunden. Dieses Modell setzt voraus, dass der Kunde Soft- und Hardware inklusive Updates und Upgrades selbst verwaltet.

Bei einer On-Demand-Implementierung werden alle Komponenten auf von Adobe verwalteten Servern gehostet, die möglichst nahe an der Region sind, in der der Kunde operiert.

Beim Hybridmodell wird Adobe Campaign direkt am Standort des Kunden ausgeführt, die Ausführungsverwaltung wird jedoch von Adobe als Cloud-Dienst bereitgestellt. Alle Daten verbleiben in der Campaign-Datenbank im kundeneigenen Rechenzentrum, bis die Kampagne ausgeführt wird. Zu diesem Zeitpunkt werden nur diejenigen Daten an die Service-Infrastruktur von Adobe übermittelt, die für diese spezielle Kampagne benötigt werden. Eine permanente Speicherung von Daten in der Cloud erfolgt nicht.

Detaillierte Informationen zu den Implementierungsoptionen von Adobe Campaign finden Sie im Whitepaper „Deployment Options for Managing Cross-Channel Campaigns" (Deployment-Optionen zur Verwaltung von Cross-Channel-Kampagnen).

Anwendungssicherheit und Netzwerkarchitektur

Falls der Kunde sich für eine vollständig gehostete oder eine hybride Implementierung von Adobe Campaign entscheidet, werden die entsprechenden Komponenten in einem von Adobes Rechenzentren bereitgehalten. Alle Rechenzentren sind nach SSAE 16 Type II SOC 2 geprüft und zertifiziert. Genauere Angaben zu den Standorten finden Sie im Abschnitt „Hosting-Rechenzentren für Adobe Campaign".

Sämtliche über das Internet zwischen Adobe Campaign-Komponenten ausgetauschten Daten (meist zwischen der Client-Benutzeroberfläche und der Engine für die Ausführungsverwaltung) werden per HTTPS mit 256-Bit-AES verschlüsselt.

Authentifizierung von Anwendern

Für den Zugriff auf Adobe Campaign 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 entweder über die in Adobe Marketing Cloud integrierte Schnittstelle auf Adobe Campaign zugreifen (Adobe Campaign Standard) oder durch Nutzung des eigenständigen Adobe Campaign-Clients (Adobe Campaign V6). In beiden Fällen kommt eines von drei Modellen der anwenderbasierten Lizenzierung zur Anwendung:

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 Campaign 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*.

Hosting-Rechenzentren für Adobe Campaign

Adobe unterhält auf der ganzen Welt Rechenzentren für das Hosting von Adobe Campaign-Komponenten.

In der Regel wird für Implementierungen, die teilweise oder vollständig von Adobe gehostet werden, ein Rechenzentrum in der Region des Kunden genutzt.

Adobe Campaign-Netzwerk-Management

Bei Adobe Campaign hat Sicherheit hohe Priorität. In der Netzwerkarchitektur sind daher branchenübliche bewährte Verfahren für Sicherheits-Design implementiert, darunter die Segmentierung der Entwicklungs- und Produktionsumgebungen, DMZ-Segmente, speziell gesicherte 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 Campaign-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. Test- und Produktionsumgebungen sind strikt voneinander getrennt. Ohne ausdrückliche Genehmigung des Kunden werden keinerlei Kundendaten in Testumgebungen verwendet.

Sicheres Management

Adobe unterhält dedizierte Netzwerkverbindungen zwischen den Niederlassungen und Rechenzentren, um eine sichere Verwaltung der Adobe Campaign-Server nach Branchenstandards 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 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

Kundendaten 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 Campaign 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 Campaign-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 Campaign-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

Die von Adobe gehosteten Daten von Adobe Campaign-Kunden werden täglich gesichert. Jedes Backup wird standardmäßig bis zu sieben Tage gespeichert. Ebenso wird täglich eine mittels GPG verschlüsselte Kopie des Datenbank-Backups extern gesichert. Sollte es zu einem Verlust der Datenbank kommen, lässt sie sich über das Tages-Backup wiederherstellen. Im Falle eines durch den Kunden verursachten Datenverlusts ist Point-In-Time-Recovery möglich. Dabei kann jedes der letzten sieben Backups genutzt werden.

Auch die Dateien zur Infrastrukturkonfiguration von Adobe Campaign werden täglich gesichert. Zu diesem Zweck werden Snapshots angelegt. Die kompletten Konfigurationsdaten werden täglich als Snapshot gesichert und über eine SSL-verschlüsselte Verbindung ausgelagert. Auf Wunsch werden die Backups verschlüsselt gespeichert.

Da alle Backups von Adobe Campaign-Daten online durchgeführt werden, stehen Applikation und Server dem Kunden jederzeit zur Verfügung, auch während die Daten gesichert werden.

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 Campaign-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-Netzwerks 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 Campaign.

Protokolle

Schutz vor nicht autorisierten Zugriffen und Änderungen bieten Netzwerk- und OS-bezogene Protokolle sowie Intrusion Detection-Systeme. Der notwendige Speicherplatz wird in regelmäßigen Abständen von Adobe ermittelt, überprüft und bei Bedarf erweitert, um stets ausreichende Kapazität zu gewährleisten. 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.

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 Campaign eine Risikoeinschätzung der Campaign-Applikation durch. Diese wird von hochqualifizierten Mitarbeitern durchgeführt, die für den Aufbau einer sicheren Netzwerktopologie und -infrastruktur sowie den Schutz der Campaign-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 Campaign 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 Campaign, informiert das Adobe Product Security Incident Response Team (PSIRT) die entsprechenden Campaign-Teams, um die erforderlichen Maßnahmen zu koordinieren.

Für Cloud-basierte Dienste von Adobe wie Adobe Campaign 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 Campaign-Team den forensischen Analyseprozess, der ein vollständiges Image bzw. ein Speicherabbild des/r betroffenen Rechner(s), eine sichere Beweis-aufbewahrung sowie eine lückenlose Dokumentation der Überwachungskette umfasst.

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 Campaign 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 Sicher-heitsschleusen, 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 Campaign 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

Disaster Recovery ist bei Ereignissen nötig, die zum Ausfall der Datenverarbeitungsvorgänge an einem Hosting-Standort für Adobe Campaign führen. Die Ursachen können unbeabsichtigt, vorsätzlich oder umweltbedingt sein, beispielsweise Brände, Überschwemmungen, Terrorangriffe, menschliches Versagen, Streiks der Belegschaft oder Software- und Hardware-Ausfälle.

Der Schwerpunkt der Pläne für Disaster Recovery und betriebliche Kontinuität der Adobe Campaign-Implementierung liegt auf der Sicherstellung eines unterbrechungsfreien Betriebsablaufs aller kritischen Systeme in einem Störfall. Dazu gehören eine möglichst kurzfristige Unterbrechung der Hosting-Funktionen für Adobe Campaign sowie die schnellstmögliche Aktivierung von Reservestandorten. Die Notfallpläne werden einmal pro Jahr und zusätzlich bei Veränderungen der Hosting-Infrastruktur überprüft.

Ob und wann die Prozeduren für Disaster Recovery ausgelöst werden, entscheidet der operativ Verantwortliche der betroffenen Region auf Basis einer ersten Einschätzung der möglichen Auswirkungen. Falls die notwendigen Prozeduren in Gang gesetzt werden, führen alle Team-Mitglieder die festgelegten Schritte aus, bis alle Daten und Dienste vollständig wiederhergestellt wurden.

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 Campaign-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.

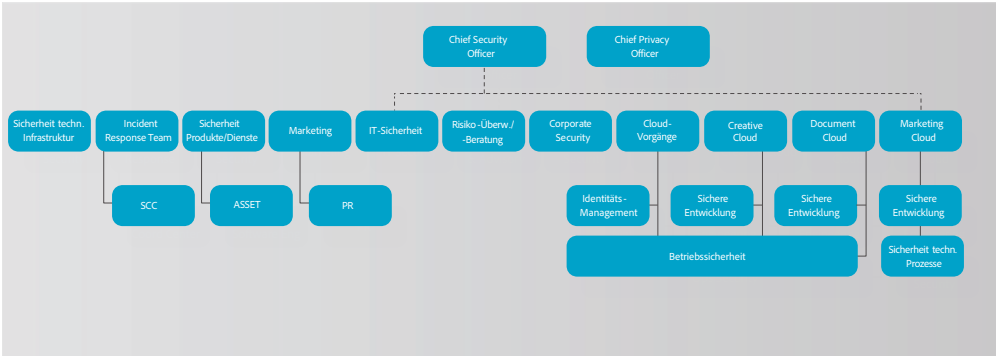

Abb. 2: Adobe-Sicherheitsorganisation

Entwicklung sicherer Adobe-Produkte

Wie bei anderen wichtigen Produkten und Services von Adobe wird für die Adobe Campaign-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 Campaign-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

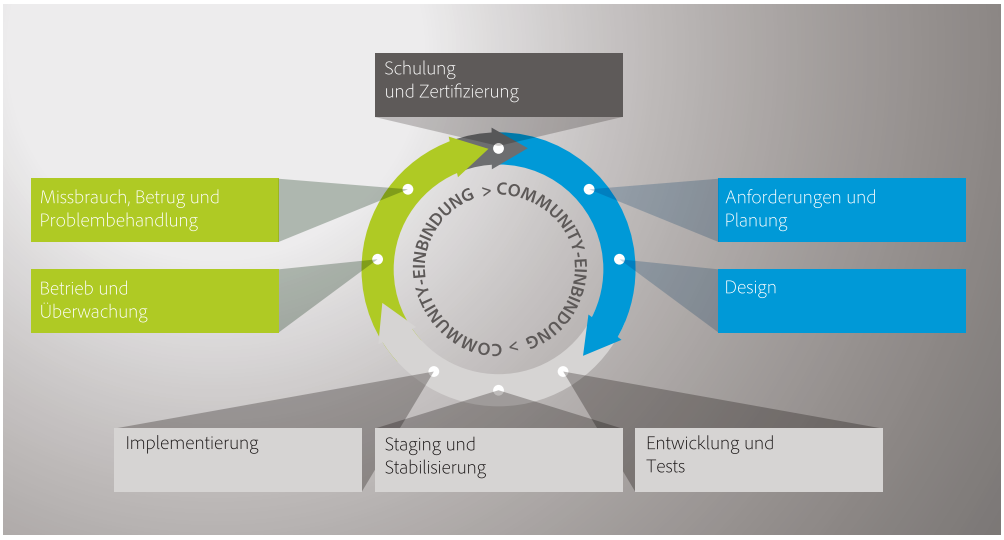

Abb. 3: Adobe Secure Product Lifecycle (SPLC)

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 Sicherheits-projekten, 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 Campaign-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 vorherigen Absatz beschrieben wurde. 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.

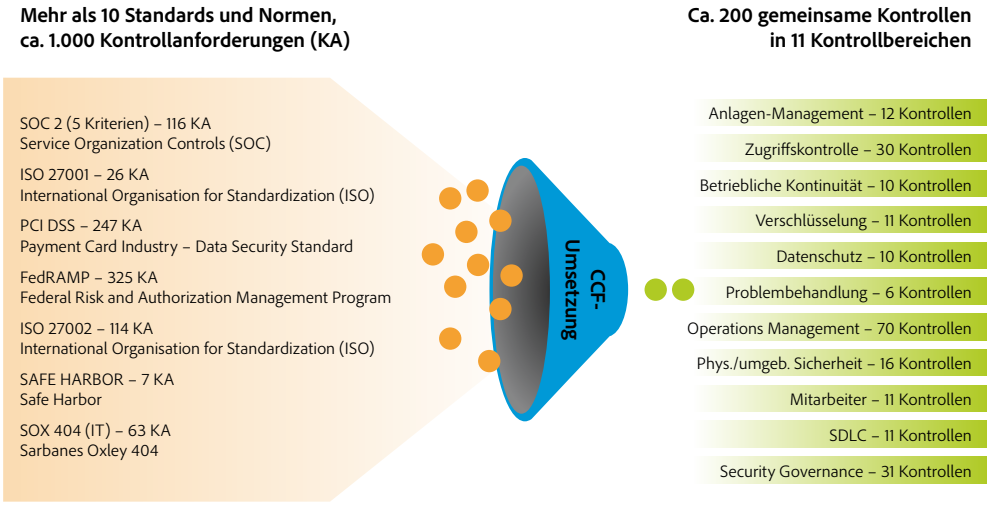

Abb. 4: Adobe Common Controls Framework (CCF)

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.

Adobe-Mitarbeiter

Mitarbeiterzugriff auf Kundendaten

Für Adobe Campaign 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.

Fazit

Das proaktive Sicherheitskonzept und die strikten Verfahren, die in diesem Whitepaper beschrieben wurden, dienen dem Schutz von Adobe Campaign 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

Die Informationen in diesem Dokument können ohne vorherige Ankündigung geändert werden. Wenn Sie weitere Informationen zu den Lösungen und Kontrollmechanismen von Adobe wünschen, wenden Sie sich bitte an Ihren Adobe-Vertriebsmitarbeiter. Weitere Informationen zu Adobe-Lösungen, z. B. zu SLAs, Änderungsgenehmigungen, Vorgehensweisen zur Zugriffssteuerung und Datenwiederherstellungs-Prozessen, stehen bei Bedarf zur Verfügung.

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2016 Adobe Systems Incorporated. All rights reserved.

8/16