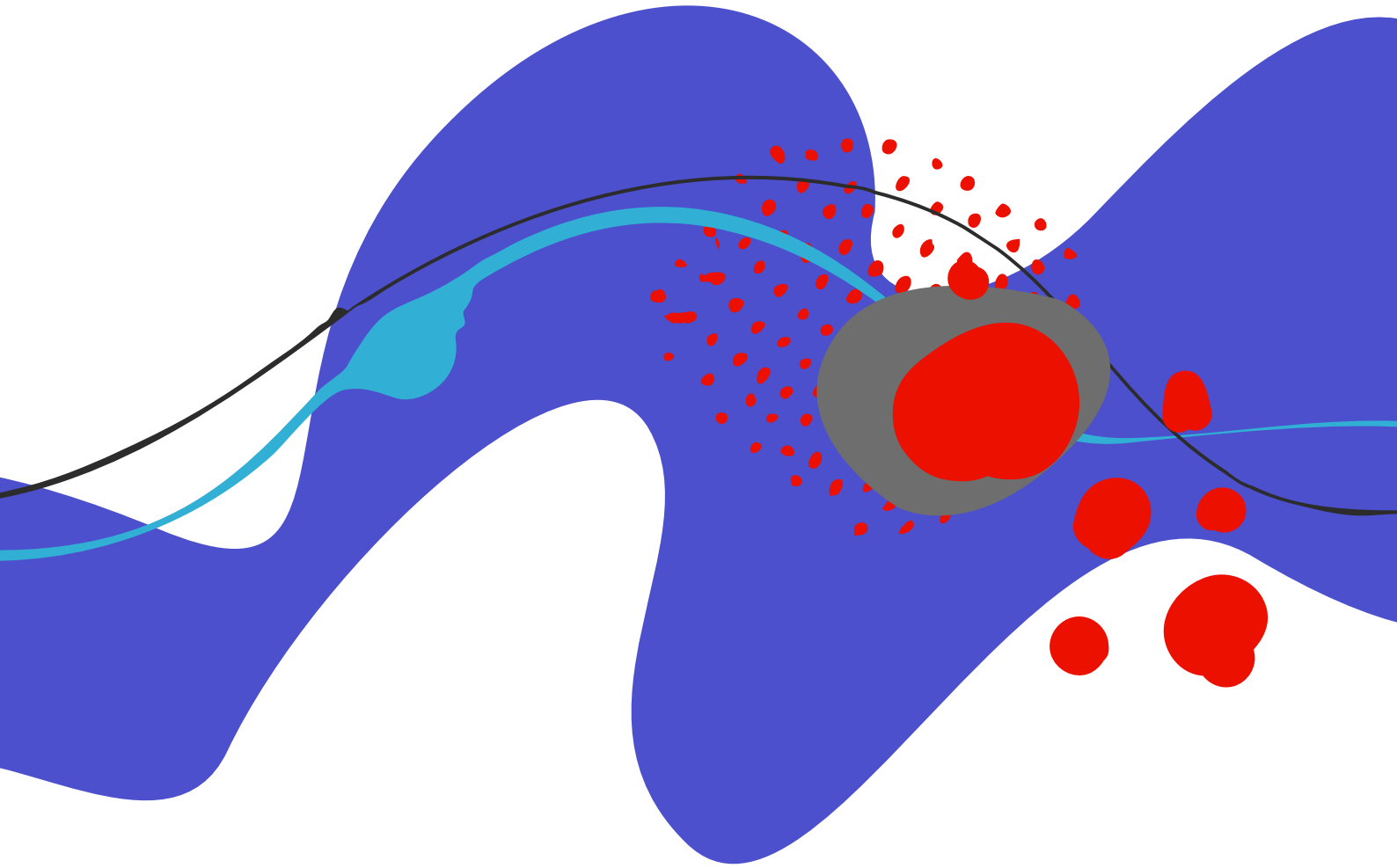
WHITEPAPER

Überblick über die Sicherheit von Adobe Identity Management Services.



Inhalt.

Sicherheit bei Adobe.

Adobe® nimmt die Sicherheit eurer digitalen Inhalte ernst. Bei Adobe sind Sicherheitsmaßnahmen ein fester Bestandteil der Software-Entwicklung, Prozesse und Programme. Die von interdisziplinären Teams implementierten Adobe Secure Product Lifecyle (SPLC)-Kontrollen tragen dazu bei, etwaigen Zwischenfällen vorzubeugen, diese aufzudecken und angemessen darauf zu reagieren. Darüber hinaus halten wir uns durch Kooperation mit Partnerunternehmen, Forschenden, Sicherheitsinstitutionen und anderen Organisationen über aktuelle Bedrohungen und Schwachstellen auf dem neuesten Stand und integrieren fortlaufend hochentwickelte Sicherheitstechnologien und -verfahren in unsere Produkte und Services.

In diesem Whitepaper erfahrt ihr, welchen Stellenwert Sicherheit bei Adobe Identity Management Services und den zugehörigen Daten hat.

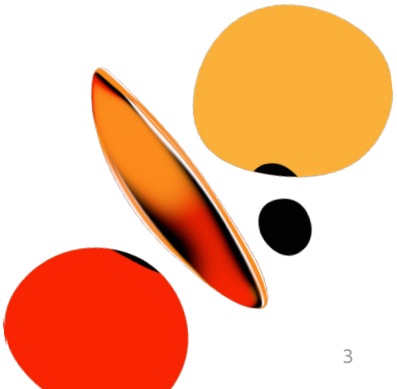
Über Adobe Identity Management Services.

Adobe Identity Management Services (IMS) verarbeiten die Authentifizierung von Endanwenderinnen und Endanwendern bei allen Adobe-Lösungen. IMS bestehen aus drei (3) Komponenten:

- **Adobe Identity Service** – verarbeitet die Anwenderauthentifizierung und -validierung, einschließlich Federation und Laufzeit-SSO (Single Sign-on).
- **Adobe Admin Console** – ermöglicht die zentrale Verwaltung aller Adobe-Berechtigungen im Unternehmen. Die Adobe Admin Console verarbeitet Anwenderverwaltung, Desktop-Lizenz- und Cloud-Service-Berechtigung, Federation-Konfiguration sowie Schutzmaßnahmen gegen Datenverlust.
- **Adobe User Management API (UMAPI)** – ermöglicht Organisationen die Verwaltung von Unternehmensanwenderinnen und -anwendern sowie von -berechtigungen in der Adobe Admin Console auf API-Ebene.

Anwendergebundene Lizenzen.

Die Adobe IMS-Plattform verwaltet die Berechtigungen und eindeutigen IDs, die auch als „Anwendergebundene Lizenzen“ bezeichnet werden, und ermöglicht es Anwenderinnen und Anwendern, sich für ihre Desktop-Programme und Cloud-Services von Adobe zu authentifizieren.



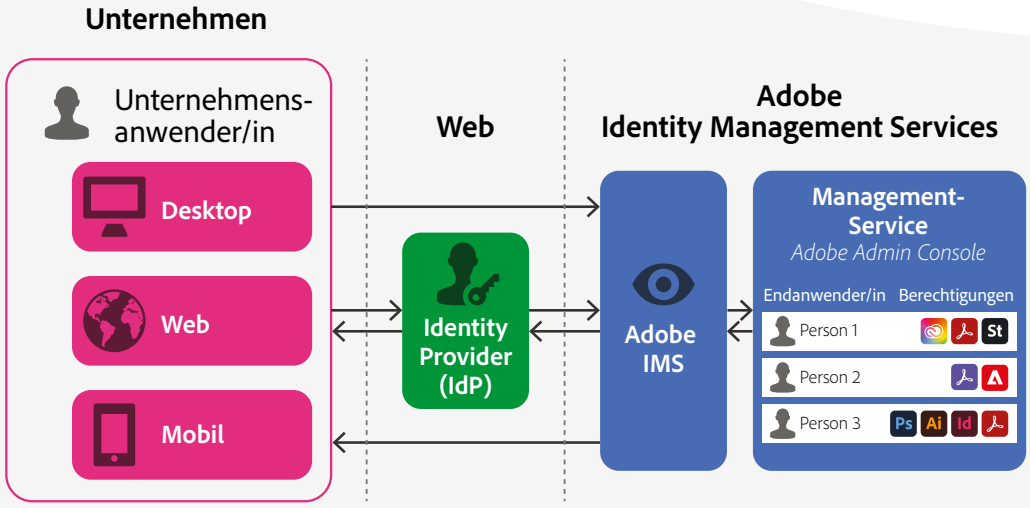


Abb. 1: Architektur der Adobe Identity Management Services

Abbildung 1 (oben) veranschaulicht die Anwenderinteraktion mit Adobe IMS im Rahmen anwendergebundener Lizenzen. Im Beispiel sind die Adobe-Programme auf dem Desktop sowie Smartphone oder Tablet der Anwenderin bzw. des Anwenders installiert. Bei Aktivierung oder Start eines Desktop-Programms oder einer Mobile App von Adobe sowie beim Zugriff auf einen Cloud-Service von Adobe kommuniziert der jeweilige Endpunkt mit Adobe IMS.

Je nach Identitätstyp (siehe nächster Abschnitt) gestattet Adobe IMS die direkte Anmeldung oder übergibt die Kontrolle an den Identity Provider des Kundenunternehmens zur föderierten SSO-Authentifizierung. Bei erfolgreicher Authentifizierung prüft Adobe IMS die Berechtigung und schließt die angeforderte Aktion ab. Endanwenderinnen und Endanwender können dann die Software und Services verwenden, für die sie im Rahmen ihrer anwendergebundenen Lizenz berechtigt sind.

Identitätstypen.

Für Installationen in Unternehmen unterstützt Adobe drei (3) anwendergebundene Identitätstypen:

Die **Business ID** ist eine von Adobe gehostete und vom Unternehmen verwaltete Option für Organisationen, die E-Mail-Adressen außerhalb ihrer eigenen Domain als Anwender-ID verwenden, sowie für Unternehmen, die keine Domain für ID-Zwecke verwenden. Adobe Business ID ist die bevorzugte Option für Organisationen, die mit externen Vertragspartnern oder Selbstständigen arbeiten, die keine Unternehmens-ID oder -E-Mail-Adresse haben.

Die **Enterprise ID** ist eine von Adobe gehostete und vom Unternehmen verwaltete Option für Konten, die durch die IT des Unternehmens erstellt werden. Die Organisation ist Eigentümerin der Anwenderkonten und aller zugehörigen Inhalte. Die Anwenderkonten werden über die Adobe Admin Console und/oder das UMAPI verwaltet. Auch die Definition der Richtlinien für die Anwenderauthentifizierung kann auf Administratorenseite erfolgen. Verwaltet werden Authentifizierung und Zugangsdaten jedoch vollständig durch Adobe.

Die **Federated ID** ist ein vom Unternehmen verwaltetes Konto, bei dem alle Identitätsprofile durch ein Identitäts-Management-System über Single Sign-on (SSO) bereitgestellt werden. Sämtliche Konten werden von der IT des Unternehmens erstellt und verwaltet. Adobe unterstützt zahlreiche Anbieter für SAML 2.0-Authentifizierung. Die Anwenderkonten werden durch den Identity Provider authentifiziert und über die Adobe Admin Console autorisiert. Festlegung und Durchsetzung der Authentifizierungsrichtlinien unterliegen dem Identity Provider der Organisation. Für Federated ID-Services unterstützt Adobe zudem die Verbindung und Synchronisation mit Microsoft Azure Active Directory und Google Workspace Directory über OpenID Connect.

Die meisten Unternehmen verwenden eine Enterprise ID oder eine Federated ID für interne und externe Mitarbeitende, die dafür eine E-Mail-Adresse mit der firmeneigenen E-Mail-Domain benötigen. Für Mitarbeitende, die keine E-Mail-Adresse mit Firmen-Domain haben, empfiehlt Adobe die Verwendung von Business IDs. Weitere Informationen stehen auf der Seite zu den Identitätstypen auf Adobe HelpX.

Die Adobe ID eignet sich besser für Einzelpersonen und den privaten Gebrauch. Dieser Identitätstyp sollte nicht für Implementierungen in Unternehmen verwendet werden.

Identitäts-Management.

Die Verwaltung der Anwender-IDs in Unternehmen kann manuell und automatisiert erfolgen.

Manuelles Identitäts-Management.

Die manuelle Anwenderverwaltung erfolgt über die Adobe Admin Console. Admins können hier Anwenderinnen und Anwender einzeln hinzufügen, löschen und ändern oder CSV-Dateien mit mehreren Anwenderdaten hochladen.

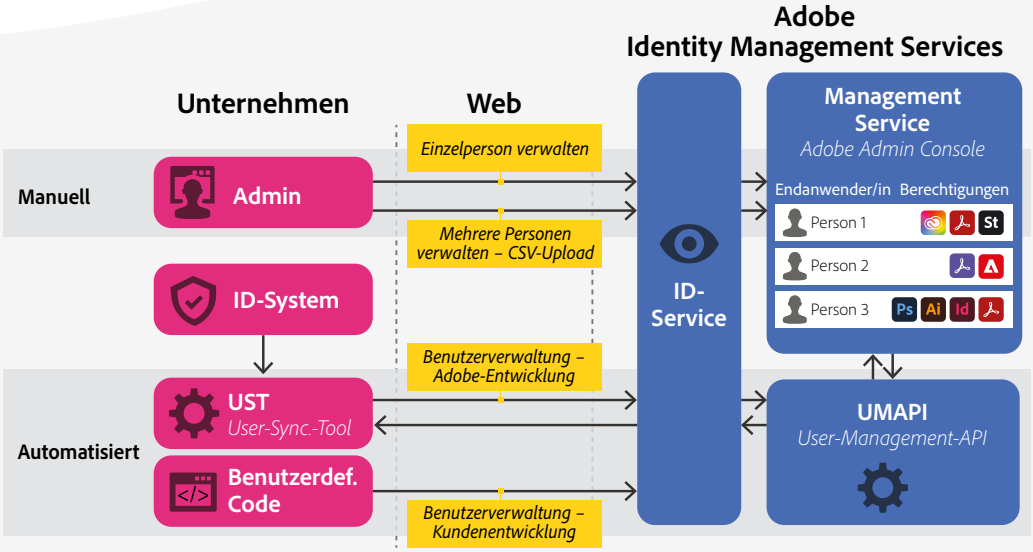


Abb. 2: Optionen für Identitäts-Management

Automatisiertes Identitäts-Management.

Für die automatisierte Anwenderverwaltung stehen drei (3) Optionen zur Verfügung:

- Programmgesteuertes Hinzufügen, Aktualisieren oder Entfernen von Anwenderinnen und Anwendern mit eigenem Code per **UMAPI**
- Synchronisieren aller Anwenderinnen und Anwender mit Microsoft Azure Active Directory und Google Workspace Directory über den offenen Standard **SCIM (System for Cross-domain Identity Management)** für Cloud-basierte Synchronisation
- Synchronisieren bestimmter Anwenderinnen und Anwender aus dem Unternehmens-verzeichnis und anschließendes Hinzufügen oder Entfernen der Personen zu bzw. aus den entsprechenden Lizenz-Pools in der Adobe Admin Console mit **Adobe User Sync Tool** (**UST**, ein von Adobe entwickeltes und verwaltetes Set an Phyton-Skripten)

User-Synchronisations-Tool.

Das UST liest die Identitätsdaten aus allen LDAP-Gruppen (Lightweight Directory Access Protocol) im Directory-Service des Unternehmens, z. B. Microsoft Active Directory und andere Directorys, die von OpenID Connect unterstützt werden. Mit gesicherten REST-Aufrufen des UMAPI werden Anwenderinnen und Anwender auf den Adobe-Servern erstellt, aktualisiert und gelöscht.

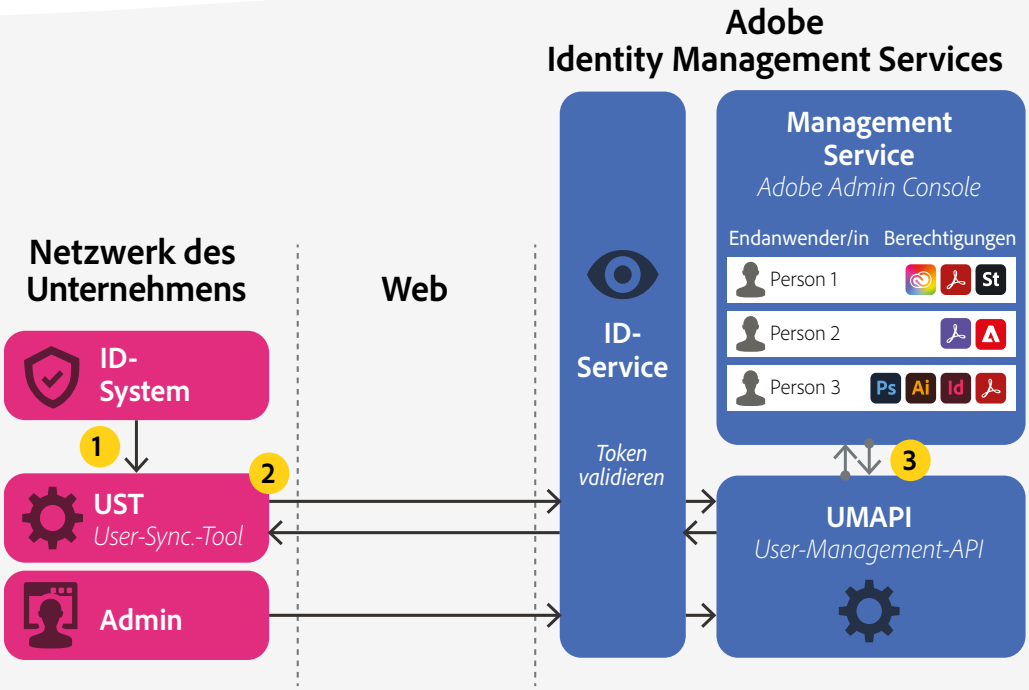


Abb. 3: Das User-Synchronisations-Tool (UST)

Bei jeder UST-Ausführung werden:

1. Mitarbeiterdatensätze aus den Gruppen im Unternehmensverzeichnis angefordert. Die Gruppen und LDAP-Abfragen können an die unternehmensspezifische Umgebung angepasst werden.
2. aktuelle Anwenderinnen und Anwender und zugehörige Produktkonfigurationen aus der Adobe Admin Console angefordert. Das UST erstellt eine Verbindung zum UMAPI mittels REST-Aufrufen über HTTPS und verwendet dabei ein verifiziertes, zeitlich begrenztes Zugriffs-Token, das von einem signierten, kodierten JWT (JSON Web Token) generiert wird.
3. Anwenderinnen und Anwender ermittelt, die gemäß den Regeln in den Konfigurationsdateien erstellt, gelöscht oder aktualisiert werden müssen.
4. erforderliche Änderungen über das UMAPI in der Adobe Admin Console vorgenommen, um Anwenderinnen und Anwender die jeweiligen Software- und Service-Berechtigungen zuzuweisen.

Das UST kann die Adobe-Berechtigungen für Unternehmensanwender automatisch mit den Gruppierungen im Verzeichnisservice synchronisieren. Beispiel: Wenn eine Person zum LDAP-Verzeichnis hinzugefügt wurde, ruft das UMAPI bei der nächsten UST-Ausführung die Personendaten aus dem Verzeichnis ab und fügt diese zur entsprechenden Gruppe in der Adobe Admin Console hinzu. Wenn Anwenderinnen und Anwender im LDAP-Verzeichnis geändert oder daraus gelöscht werden, ruft das UST das UMAPI auf und führt die entsprechende Aktion in der Adobe Admin Console aus.

Ausführliche Anleitungen zur Installation, Registrierung und Ausführung des UST findet ihr auf der Seite Einrichten des Benutzer-Synchronisationstools auf Adobe HelpX.

Weitere Informationen zur Anwenderverwaltung enthält die Seite Adobe Admin Console-Anwender auf Adobe HelpX.

Datenfluss bei Authentifizierung und Autorisierung.

Adobe aktiviert die Anwenderauthentifizierung und -autorisierung mit zwei (2) Optionen:

Eine **interaktive Authentifizierung und Autorisierung** findet statt, wenn sich Anwenderinnen und Anwender explizit in einem Desktop-Programm oder einem Cloud-Service von Adobe anmelden und ihre Daten in einem Dialogfeld auf der Benutzeroberfläche eingeben. In diesem Fall erfolgt die Autorisierung nahtlos und – aus Anwendersicht – als Teil des Authentifizierungsprozesses.

Adobe unterstützt außerdem Multi-Faktor-Authentifizierung (MFA), um eine zusätzliche Sicherheitsebene zu ermöglichen. Userinnen und User müssen hier nach der zweistufigen Verifizierung weitere individuelle Informationen eingeben. Adobe bietet Richtlinien zur MFA-Anwendung mit Adobe ID und Business ID. Die Autorisierung erfolgt auch mit MFA nahtlos und – aus Anwendersicht – als Teil des Authentifizierungsprozesses.

Eine **automatisierte Authentifizierung und Autorisierung** findet nach erfolgter interaktiver Authentifizierung statt. Die automatische Authentifizierung verwendet ein eindeutiges Identifizierungs-Token. Daher ist während der Sitzung keine erneute Anmeldung erforderlich, und die Autorisierung erfolgt ebenfalls nahtlos. Bei allen Interaktionen mit einem Programm oder Service, für die keine explizite Anmeldung vorgenommen werden muss, werden Nutzerinnen und Nutzer automatisch authentifiziert. Nach erfolgter Abmeldung werden die Autorisierungen bei der nächsten Anmeldung erneut zur Verifizierung der Zugriffsrechte geprüft.

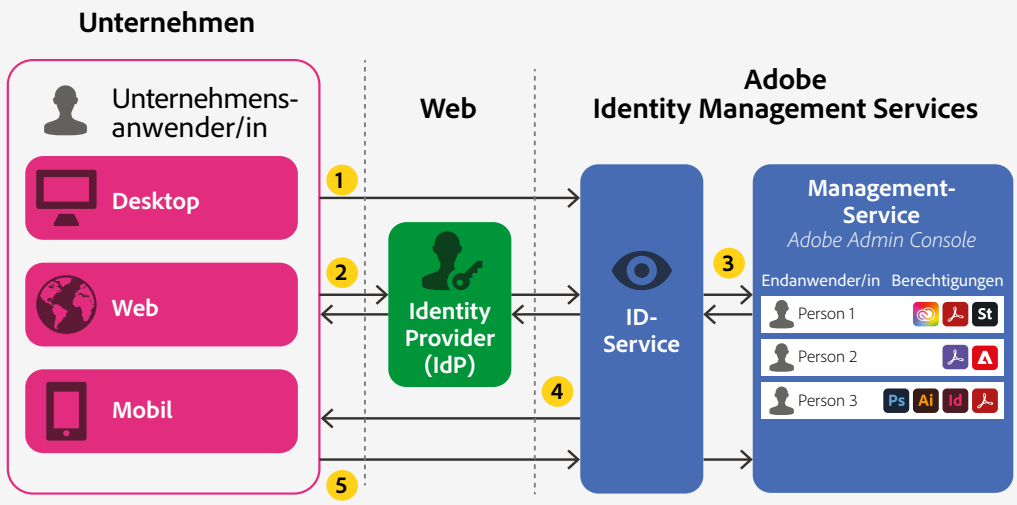


Abb. 4: Datenfluss bei Adobe-Anwenderauthentifizierung

Der Datenfluss bei der Anwenderauthentifizierung hängt vom jeweiligen Identitätstyp ab. Ein typischer Authentifizierungsprozess besteht jedoch immer aus den folgenden Schritten, die den Ziffern im vorstehenden Diagramm entsprechen:

1. Anwenderinnen und Anwender starten erstmals ein Desktop-Programm von Adobe oder greifen erstmals auf einen Cloud-Service von Adobe zu. Bei Verwendung einer Business ID oder Enterprise ID melden sie sich über Adobe IMS an.
2. Wenn die Organisation Federated ID verwendet und die Anwenderinnen und Anwender ihre E-Mail-Adresse oder nur die Domain (z. B. @companydomain) im Feld „Benutzername“ eingeben, startet Adobe IMS eine SAML-Anforderung. Diese leitet die Person zum jeweiligen Identity Provider, um sich mit den Firmenzugangsdaten anzumelden.
3. Nach erfolgter Authentifizierung nimmt Adobe IMS die erforderlichen Prüfungen von Berechtigung und Richtlinienkonformität vor und leitet die Person zum jeweiligen Adobe-Cloud-Service bzw. aktiviert die jeweilige Desktop-Programmlizenz.
4. Adobe IMS speichert ein Geräte-Token auf dem Rechner des Endanwenders bzw. der Endanwenderin und generiert damit ein Zugriffs-Token (vergleichbar mit einem Sitzungs-Token für Programme). Anhand dieser beiden Token wird eine signierte Lizenz für das Programm generiert, die mit dem Geräte-Token verschlüsselt und in den Benutzereinstellungen gespeichert wird. Da das Token nicht vom Betriebssystem abhängig ist, ist beim erneuten Starten des Systems keine erneute Authentifizierung für das Desktop-Programm oder den Cloud-Service von Adobe erforderlich.

5. Anwenderinnen und Anwender können damit gleichzeitig verschiedene Desktop-Programme oder Cloud-Services von Adobe verwenden, ohne sich für jedes Produkt einzeln authentifizieren zu müssen (= automatisierte Authentifizierung). Beim Start eines neuen Programms während einer Sitzung wird Adobe IMS kontaktiert, und es werden für einen Zugriffs-Token die Geräte-ID und das Geräte-Token ausgetauscht. In diesem Prozess erfolgen die Richtlinienüberprüfung und Bestätigung der Berechtigung. Bei einer Änderung oder Deaktivierung der Zugriffsrechte oder Berechtigungen werden die Zugriffs- und Geräte-Token ungültig.

Adobe bietet optional administrative Richtlinien, die die Gültigkeitsdauer von Zugriffs-Token durch eine häufigere Authentifizierung begrenzen. Das kann insbesondere für bestimmte Adobe Experience Cloud-Programme nützlich sein. Adobe empfiehlt die Verwendung dieser Richtlinien jedoch nur für Unternehmen mit speziellen Sicherheitsanforderungen.

Identitätsdaten.

Welche Daten werden aus welchen Gründen erfasst?

Die von Adobe erfassten Identitätsdaten stellen sicher, dass alle Anwenderinnen und Anwender eine eindeutige ID haben, sodass die Lizenzberechtigung geprüft und der Kennwortschutz dieser Berechtigungen für die generierten und gespeicherten Inhalte aktiviert werden kann. Adobe erfasst folgende Informationen für Identitätsdaten:

- **Benutzername und Domain** – ein Identifizierungsmerkmal für die Anwenderin oder den Anwender, in der Regel eine gültige primäre E-Mail-Adresse im Format benutzer@domain. Bei Business IDs und Enterprise IDs ist der vollständige Benutzername zur Anmeldung für Programme und Cloud-Services von Adobe erforderlich. Einige Unternehmen verwenden Benutzernamen, die nicht den E-Mail-Adressen entsprechen (z. B. vornamenachname statt benutzer@domain). Dies wird jedoch vom Unternehmen geregelt. Beim Identitätstyp Federated ID ist entweder die vollständige E-Mail-Adresse oder nur der @domain-Teil für die Kontrolle durch den jeweiligen Identity Provider erforderlich.
- **UID (nur Federated IDs)** – eine eindeutige Kennung, die der Anwenderin oder dem Anwender zugeordnet ist (normalerweise die E-Mail-Adresse). Adobe verwendet die UID als Schlüssel des Identity Providers für die Anwendersuche in Adobe IMS.
- **Kennwort (nur Business ID und Enterprise ID)** – Kennwörter werden gemäß Best Practices vor der Speicherung als Hash-Wert verschlüsselt. Adobe speichert in keinem Fall Kopien des Benutzerkennworts in Formaten, die eine Entschlüsselung des Kennworts in Klartext ermöglichen.
- **Geburtsdatum (nur Adobe ID)** – erforderliche Angabe für den Schutz der Privatsphäre von Kindern im Internet (COPPA), gemäß Datenschutz-Grundverordnung (DSGVO) und zur Altersüberprüfung bei Website-Zugriffen.

- **Länder-Code** – Die Länder-Codes ISO Alpha-2 und ISO Alpha-3 werden bei der Erstellung von Identitätsprofilen erfasst. Adobe verwendet den Länder-Code in der Regel zur Bestimmung des regionalen Speicherorts für anwendergenerierte Inhalte. Die Speicherorte für Enterprise ID und Federated ID werden von der Organisation definiert.
- **Vor- und Nachname** – werden bei Erstellung des Identitätsprofils erfasst. Bei den Identitätstypen Enterprise ID und Federated ID können IT-Admins im Zuge der Benutzerkontenerstellung die Felder für UID, Länder-Code, Vorname und Nachname konfigurieren. Auch die Menge an Benutzerinformationen, die in diesen Feldern gespeichert werden, kann festgelegt werden.

Wo werden Identitätsdaten gespeichert?

Alle Identitätsdaten werden unabhängig vom geografischen Kundenstandort zur Lastenverteilung über mehrere Regionen verteilt, bei Cloud-Infrastrukturdiensten mit Rechenzentren in Nordamerika (Oregon und Virginia), Europa (Irland) und APAC (Singapur) gespeichert und zur Gewährleistung der Verfügbarkeit über alle Rechenzentren repliziert.

Wie werden Identitätsdaten geschützt?

Gemäß Adobe Common Compliance Framework (CCF) und unseren internen Richtlinien zur Verschlüsselung und Speicherung vertraulicher Daten werden alle Identitätsdaten im Ruhezustand („at rest“) mit 256-Bit-AES-Verschlüsselung gesichert.

Wie lange werden Identitätsdaten gespeichert?

Zur Lastenverteilung und aus Redundanzgründen werden die Daten zwischen den Rechenzentren (innerhalb der Region und überregional) repliziert und gesichert. In den Rechenzentren wird täglich ein Backup der Identitätsdaten erstellt, das sieben (7) Tage lang gespeichert wird. Adobe erfüllt außerdem alle gesetzlichen Anforderungen an grenzüberschreitende Datenübertragungen.

Adobe ID-Konten werden von Einzelanwenderinnen und Einzelanwendern erstellt, verwaltet und kontrolliert. Sie entscheiden damit auch über die Gültigkeitsdauer ihrer Konten – sofern nicht die Aufbewahrungsrichtlinien gemäß Consumer Personal Information Retention (CPIR)-Standard greifen, der eine Löschung der Identitätstypen Adobe ID und Business ID vorsieht, wenn diese mehr als vier (4) Jahre inaktiv waren. Adobe deaktiviert Adobe ID-Konten und löscht damit verbundene persönliche Daten und Zahlungsdaten sowie das als Hash-Wert verschlüsselte Kennwort auf Anforderung durch die Kontoinhaber bzw. wenn das Konto 48 Monate durchgängig inaktiv war.

Für die ID-Typen Enterprise ID und Federated ID wird der Zeitraum bis zur Löschung eines Kontos vom Unternehmen festgelegt. Die Kontrolle kann über die Adobe Admin Console erfolgen. Enterprise IDs und Federated IDs, die einem Unternehmenskonto zugeordnet sind und vom Unternehmen nicht mehr gewünscht werden, können durch autorisierte Admins in der Adobe Admin Console entfernt werden. Weitere Informationen findet ihr auf der Seite Adobe Admin Console-Anwender auf Adobe HelpX.

Wie erfolgt die Protokollierung?

Adobe protokolliert die folgenden Aktionen von Anwenderinnen und Anwendern:

- Aktivierung eines Programms oder Services von Adobe
- Anmeldung bei einem Programm oder Service von Adobe
- Öffnung eines Adobe-Programms auf dem Desktop, Smartphone oder Tablet
- Zugriff auf Cloud-Speicher oder -Services

Die erfassten Daten können Benutzer-ID, E-Mail-Adresse und IP-Adresse der Anwenderin/des Anwenders sowie Ereignisverfolgungsdaten enthalten. Mitunter protokolliert Adobe auch Analysedaten über die Verwendung des Programms und der Services. Anwenderinnen und Anwender können jederzeit die Erfassung von Analysedaten deaktivieren.

Wer darf auf Identitätsdaten zugreifen?

Gemäß unserer ISO 27001-Zertifizierung erhalten ausschließlich autorisierte Mitarbeitende von Adobe Zugriff auf Identitätsdaten. Ein Zugriff ist nur bei Bedarf und nur mit den unbedingt erforderlichen Rechten (Least-Privilege-Prinzip) zulässig. Die von Adobe IMS protokollierten Daten sind „most privileged“ (entsprechend Adobe Data Classification und Handling Standard). Der Zugriff ist daher auf eine noch kleinere Zahl Mitarbeitender von Adobe beschränkt.

Überblick über das Sicherheitsprogramm von Adobe.

Das integrierte Sicherheitsprogramm von Adobe besteht aus fünf Centers of Excellence. Mit neuen und fortschrittlichen Technologien wie Automatisierung, künstlicher Intelligenz und Machine Learning trägt jedes Center kontinuierlich zur Ausführung und Verbesserung der Methoden zur Erkennung und Vermeidung von Risiken bei.

Abb. 5: Fünf Centers of Excellence für Sicherheit

Die Centers of Excellence im Rahmen des Sicherheitsprogramms von Adobe umfassen:

- **Programmsicherheit** – Schutz des Produkt-Codes, Untersuchungen zu Bedrohungen und Implementierung der Ergebnisse aus dem Bug-Bounty-Programm
- **Betriebssicherheit** – Überwachung und Schutz der Systeme, Netzwerke und Cloud-basierten Produktionssysteme von Adobe
- **Unternehmenssicherheit** – Gewährleistung des sicheren Zugriffs auf die Unternehmensumgebung von Adobe sowie der zuverlässigen Authentifizierung
- **Compliance** – Überwachung unseres Modells für Sicherheits-Governance, der Audit- und Compliance-Programme sowie der Risikoanalyse
- **Problembehandlung** – Rund um die Uhr verfügbares Security Operations Center (SOC) und sofortige Reaktion auf Bedrohungen

Die Centers of Excellence, die sich der Sicherheit unserer Produkte und Services widmen, sind dem Büro des oder der Chief Security Officer (CSO) unterstellt, das sämtliche Maßnahmen zum Schutz unserer Produkte und Services koordiniert und auch das zukünftige Sicherheitskonzept bei Adobe ausarbeitet.

Adobe-Sicherheitsorganisation.

Die Adobe-Sicherheitsorganisation basiert auf transparenter, verantwortlicher und fundierter Entscheidungsfindung und vereint sämtliche Sicherheits-Services in einem einzigen Governance-Modell. Auf Führungsebene arbeiten CSO, Chief Information Officer (CIO) und Chief Privacy Officer (CPO) eng zusammen, um Sicherheitsstrategie und Betrieb im Einklang zu halten.

Zusätzlich zu den oben beschriebenen Centers auf Excellence bezieht Adobe auch Team-Mitglieder aus den Bereichen Recht, Datenschutz, Marketing und PR in die Sicherheitsorganisation ein, um Transparenz und Verantwortungsbewusstsein bei sicherheitsbezogenen Entscheidungen zu gewährleisten.

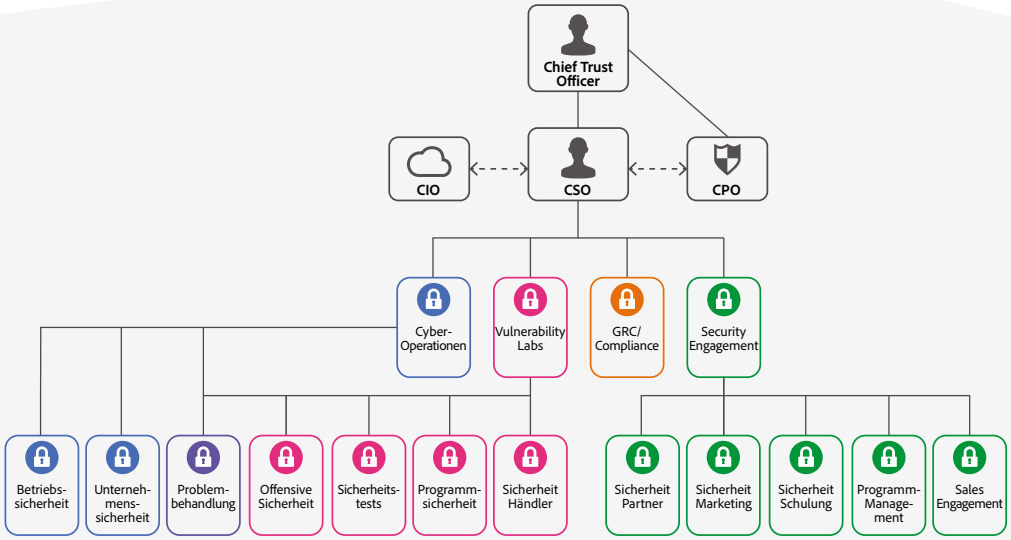


Abb. 6: Adobe-Sicherheitsorganisation

Im Rahmen der unternehmensweiten Sicherheitskultur müssen alle Mitarbeitenden von Adobe jedes Jahr ein Training zum Thema Sicherheit und Datenschutz absolvieren. Dadurch wird gewährleistet, dass alle zum Schutz des Unternehmenseigentums sowie der Daten von Kundinnen und Kunden sowie Mitarbeitenden beitragen. Mitarbeitende in technischen Abteilungen, darunter Software-Entwicklung und technischer Betrieb, werden bei Aufnahme ihrer Beschäftigung automatisch für ein intensives Trainings-Programm angemeldet, das auf ihre jeweiligen Aufgaben zugeschnitten ist.

Ausführliche Informationen zu unserer Sicherheitskultur und den Trainings-Programmen finden sich im englischsprachigen Whitepaper zur Sicherheitskultur von Adobe.

Adobe Secure Product Lifecycle.

Der Adobe Secure Product Lifecycle (SPLC) ist die Grundlage für Sicherheit bei Adobe. SPLC-Maßnahmen kommen während des gesamten Produktzyklus zum Einsatz – von Design und Entwicklung bis zu Qualitätssicherung, Test und Bereitstellung. Das Regelwerk aus mehreren Hundert strengen, auf größtmögliche Sicherheit ausgerichteten Methoden, Prozessen und Werkzeugen gibt klar strukturierte, reproduzierbare Prozesse für die Software-Entwicklung vor, sodass Sicherheit Teil jedes Produkts und jedes Service ist. Das Adobe SPLC wird kontinuierlich weiterentwickelt, um aktuelle Best Practices zu berücksichtigen.

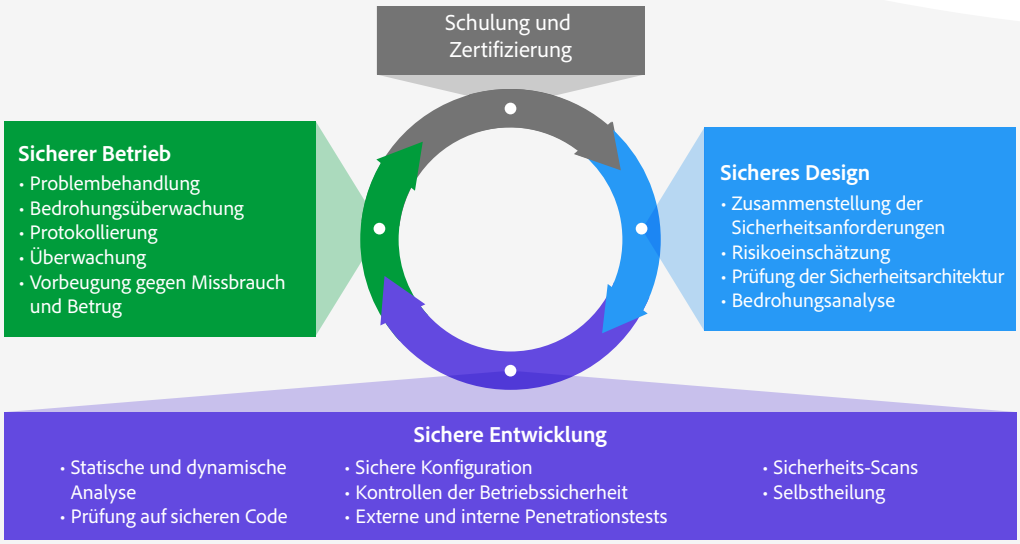


Abb. 7: Adobe Secure Product Lifecycle

Adobe befolgt einen veröffentlichten Standard für den Secure Product Lifecycle, der auf Anfrage eingesehen werden kann. Weitere Informationen über den Adobe SPLC sind dem englischsprachigen Überblick über die Programmsicherheit bei Adobe zu entnehmen.

Programmsicherheit bei Adobe.

Das Grundgerüst für die Entwicklung von Adobe-Programmen, die „nativ sicher" sind, heißt „Adobe Application Security Stack". Mit dem Adobe Application Security Stack hat Adobe klare, wiederholbare Prozesse auf Basis fundierter Untersuchungen und Erfahrungen entwickelt. In Kombination mit Automatisierung sorgen diese Prozesse für die konsistente Durchführung von Sicherheitskontrollen. Ziel ist es, die Effizienz während der Entwicklung zu verbessern und das Risiko von Sicherheitslücken zu minimieren. Durch die Verwendung von getesteten und vorab genehmigten, sicheren Coding-Blöcken müssen häufig verwendete Muster und Blöcke nicht neu programmiert werden. So können sich Teams auf andere Aufgaben konzentrieren, mit der Gewissheit, dass der eingesetzte Code sicher ist. Zusammen mit Tests, speziellen Werkzeugen und Überwachungsfunktionen ermöglicht der Adobe Application Security Stack eine standardmäßig sichere Software-Programmierung.

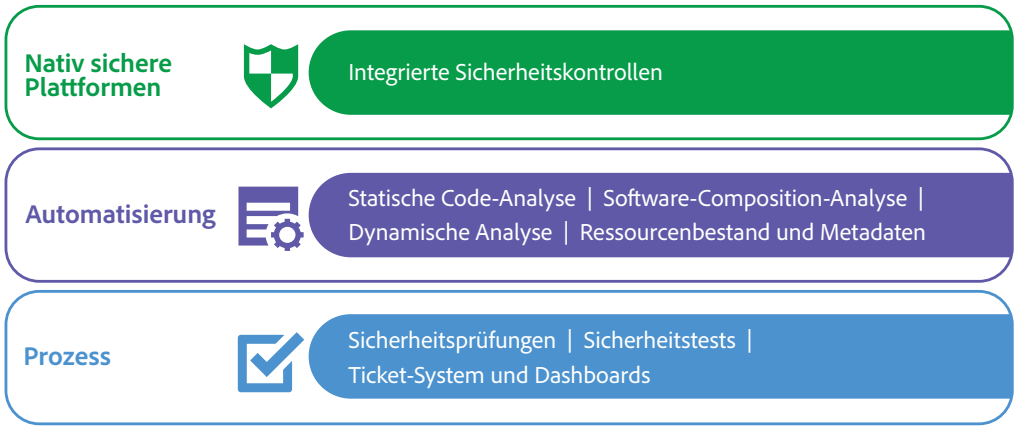


Abb. 8: Adobe Application Security Stack

Adobe befolgt außerdem mehrere veröffentlichte Standards zur Programmsicherheit, darunter arbeitsspezifische Standards für unsere Public-Cloud-Infrastruktur auf Basis von Amazon Web Services (AWS) und Microsoft Azure. Diese Standards können auf Anfrage eingesehen werden. Der englischsprachige Überblick über die Programmsicherheit bei Adobe enthält Details zu unseren Maßnahmen und Prozessen zur Gewährleistung der Sicherheit bei Adobe-Produkten.

Betriebssicherheit bei Adobe.

Um sicherzustellen, dass alle Adobe-Produkte und -Services von Anfang an unter Berücksichtigung der Best Practices für Sicherheit entwickelt werden, hat das Team für Betriebssicherheit den Adobe Operational Security Stack (OSS) ins Leben gerufen. Der OSS ist eine Sammlung von Tools, die Produktentwickelnden und Software-Ingenieuren und -Ingenieurinnen dabei helfen, die Sicherheit zu verbessern und Risiken sowohl für Adobe als auch für Kunden und Kundinnen zu minimieren. Gleichzeitig trägt der OSS dazu bei, dass im gesamten Unternehmen die Governance-Richtlinien wie Compliance und Datenschutz eingehalten werden.

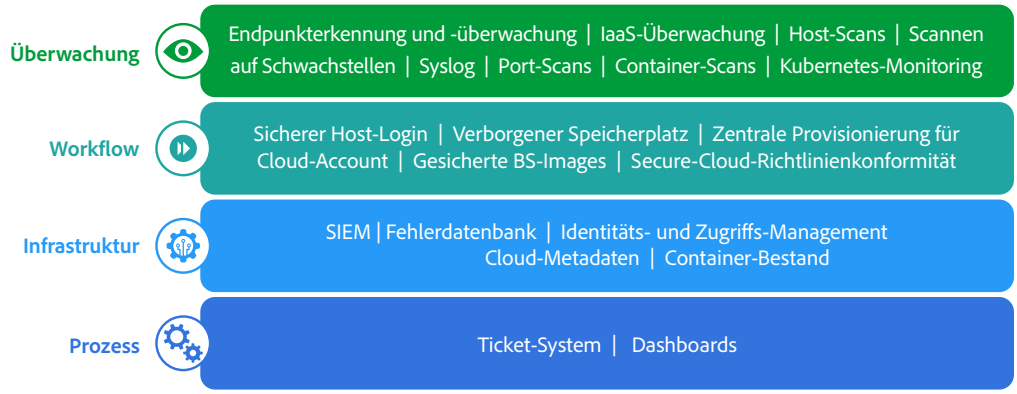


Abb. 9: Adobe Operational Security Stack

Adobe befolgt mehrere veröffentlichte Standards zum Schutz des Cloud-Betriebs, die auf Anfrage eingesehen werden können. Eine detaillierte Beschreibung des Adobe OSS und der in diesem Rahmen eingesetzten Tools findet ihr im englischsprachigen Überblick über die Betriebssicherheit bei Adobe.

Unternehmenssicherheit bei Adobe.

Zusätzlich zu den Maßnahmen zum Schutz unserer Produkte, Services und des Cloud-Hosting-Betriebs setzt Adobe eine Reihe von internen Sicherheitskontrollen unserer internen Netzwerke und Systeme, physischen Standorte sowie Mitarbeitenden und Daten ein.

Nähere Informationen zu unseren Sicherheitsmechanismen und den zugehörigen Standards findet ihr im englischsprachigen Überblick über die Unternehmenssicherheit bei Adobe.

Compliance bei Adobe.

Alle Produkte und Services von Adobe unterliegen dem Adobe Common Controls Framework (CCF). Es umfasst eine Reihe von Sicherheitsmaßnahmen und Compliance-Kontrollen, die in den Produkt-Teams sowie in verschiedenen Teilen der Infrastruktur- und Programm-Teams im Einsatz sind. Adobe setzt auf modernste Automatisierungsprozesse, um Teams auf mögliche Verstöße gegen Richtlinien aufmerksam zu machen und ihnen die schnelle Problemlösung zu ermöglichen.

Adobe-Produkte und -Services erfüllen entweder geltende gesetzliche Vorgaben oder können von Kundinnen und Kunden so genutzt werden, dass sie die jeweiligen gesetzlichen Vorgaben in Bezug auf die Inanspruchnahme von Dienstleistungen erfüllen. Kundinnen und Kunden behalten die Kontrolle über ihre Dokumente, Daten und Workflows und können steuern, wie sie regionale Vorgaben (z. B. die Datenschutz-Grundverordnung (DSGVO) der EU) am besten einhalten.

Adobe führt zudem Compliance-Trainings durch und befolgt entsprechende Standards, die auf Anfrage eingesehen werden können. Weitere Informationen zum CCF von Adobe und den wichtigsten Zertifizierungen findet ihr in der Liste der Zertifizierungen, Standards und Vorschriften.

Problembehandlung.

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 Fachkräften für Sicherheit auf der ganzen Welt aus, beheben Vorfälle innerhalb kürzester Zeit und leiten sämtliche Informationen an unsere Entwicklungs-Teams weiter. So erzielen wir für alle Adobe-Produkte die größtmögliche Sicherheit.

Wir befolgen außerdem interne Standards für den Umgang mit Zwischenfällen und Schwachstellen, die auf Anfrage eingesehen werden können.

Weitere Informationen zu diesem Thema findet ihr im englischsprachigen Whitepaper über den Umgang mit Zwischenfällen bei Adobe.

Betriebliche Kontinuität und Disaster Recovery.

Das Adobe-Programm für betriebliche Kontinuität und Disaster Recovery (Business Continuity and Disaster Recovery, BCDR) setzt sich aus dem Adobe Corporate Business Continuity Plan (BCP) und produktspezifischen Disaster-Recovery-Plänen (DR) zusammen, die gemeinsam die kontinuierliche Verfügbarkeit und Bereitstellung unserer Produkte und Services gewährleisten. Das nach ISO 22301 zertifizierte BCDR-Programm ermöglicht eine bessere Reaktion auf unvorhergesehene Störungen und minimiert deren potenzielle Folgen. Weitere Informationen zum BCDR-Programm von Adobe findet ihr im englischsprachigen Überblick zu Business Continuity und Disaster Recovery bei Adobe.

Fazit.

Das proaktive Sicherheitskonzept und die strikten Verfahren, die in diesem Dokument beschrieben wurden, dienen dem Schutz von Adobe-Lösungen und eurer vertraulichen Daten. Adobe nimmt die Sicherheit eurer 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 zur Sicherheit bei Adobe findet ihr im Adobe Trust Center.

12/22