Überblick über die Sicherheit von Adobe Sign

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. 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 Dokument erfahrt ihr, wie Adobe für sichere Adobe Sign-Workflows sorgt und eure Daten zuverlässig schützt.

Über Adobe Sign.

Mithilfe von Adobe Sign können Unternehmen herkömmliche Unterschriftsprozesse vollständig digitalisieren – über sämtliche Workflow-Anforderungen hinweg, von einfachen Unterschriften bis hin zu qualifizierten, Cloud-basierten Signaturen. Mit Adobe Sign lassen sich Dokumente per Browser, Smartphone oder Tablet versenden, unterschreiben, nachverfolgen und Unterschriftsprozesse verwalten. Die Lösung umfasst schlüsselfertige Integrationen und APIs zur Einbindung von Workflows für elektronische Unterschriften in Enterprise-Services, Datensysteme und gängige Cloud-basierte Produktivitäts-Tools wie Microsoft 365.

Adobe Sign erfüllt zahlreiche gesetzliche Auflagen und Branchenstandards. Dazu gehört auch die Unterstützung von zertifikatbasierten, digitalen Signaturen für Unterschriftsprozesse mit höheren Sicherheitsanforderungen. Der zuverlässige, Cloud-basierte Service unterstützt umfangreiche Online-Prozesse für elektronische Unterschriften und bietet unter anderem folgende Funktionen:

- Identitäts-Management, Authentifizierung und Zugriffskontrolle
- Zertifizierung der Integrität von Dokumenten
- Überprüfung von elektronischen Signaturen
- Protokollierung von Einverständniserklärungen oder Eingangsbestätigungen
- Verwaltung von Prüfprotokollen
- Einbindung von elektronischen Unterschriften in wichtige Business-Programme und Enterprise-Systeme

Im Rahmen von verifizierten Standardintegrationen des Cloud Signature Consortium unterstützt Adobe Sign zudem Cloud-basierte Fernsignaturen mit digitalen Zertifikaten von Vertrauensdiensten[1].

Details zur Gültigkeit von elektronischen Unterschriften weltweit findet ihr auf der Adobe Trust Center-Seite zur Rechtsgültigkeit von elektronischen Unterschriften nach Land/Region[1]. Weitere Informationen zu Adobe Sign findet ihr unter www.adobe.com/go/adobesign-de.

Lösungsarchitektur von Adobe Sign.

Die Architektur von Adobe Sign ist darauf ausgerichtet, Transaktionen in großem Umfang zu skalieren und zu verarbeiten, ohne dass die Leistung beeinträchtigt wird. Um ein hohes Maß an Verfügbarkeit und Skalierbarkeit zu gewährleisten, werden sämtliche Transaktionsdaten aus Adobe Sign in mehreren verteilten, redundanten Datenbank-Clustern mit automatischem Failover- und Recovery-System gespeichert.[2]

Die folgende Abbildung zeigt die logische Architektur der Komponenten und Funktionen von Adobe Sign:

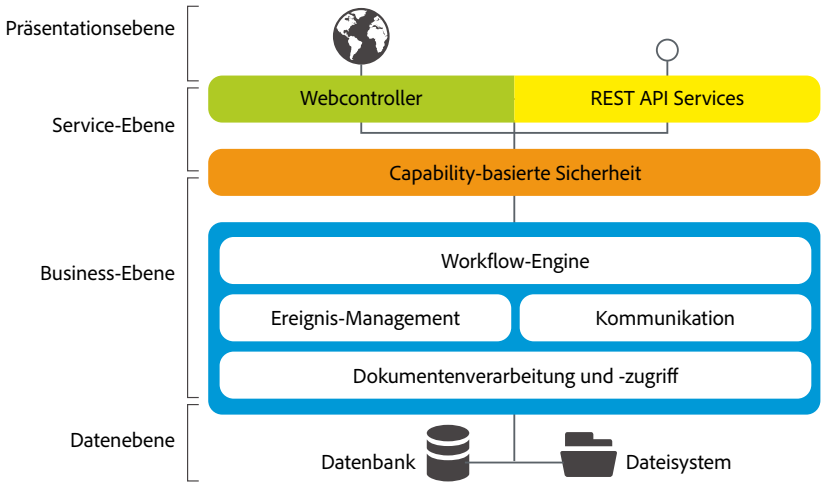

Abb. 1: Architektur von Adobe Sign

Jede logische Ebene der Adobe Sign-Architektur wird durch mehrere Werkzeuge überwacht, mit denen wiederum Schlüsselindikatoren verfolgt werden, darunter die durchschnittliche Dauer der PDF-Umwandlung oder die Ressourcennutzung.

Mit dem Überwachungs-Dashboard können Techniker den Zustand des Service im Auge behalten. Wird einer der definierten Schwellenwerte für die Schlüsselindikatoren überschritten, werden die Techniker in Echtzeit benachrichtigt. Falls sich ein Problem nicht verhindern lässt, speichert Adobe Sign umfangreiche Diagnoseprotokolle und forensische Analysen, damit die Ursache schnell behoben und ein Wiederauftreten des Problems vermieden werden kann.

Präsentationsebene.

Die Präsentationsebene beinhaltet die Web-basierte Benutzeroberfläche (UI) sowie die Funktionen zum Erstellen und Rendern von Dokumenten, die zur Unterzeichnung und Durchführung anderer Workflows versendet werden, sowie von finalen, zertifizierten PDF-Dateien.

Service-Ebene.

Die Service-Ebene umfasst die erforderlichen Kontrollen für die Client- und REST-API-Services. Die Webserver für externe Systeme verarbeiten Browser- und API-Anfragen, während die E-Mail-Server eingehenden und ausgehenden Traffic verwalten.

Mithilfe von Lastverteilern verteilen die Webserver komplexe dynamische Anfragen an die Programm-Server von Adobe Sign auf der Business-Ebene. Die Webserver wenden zudem Filterregeln an, um Angriffe aus dem Web zu verhindern, sowie Firewall-Schutz, um die Zugriffskontrolle zu erhöhen.

Business-Ebene.

Die Business-Ebene von Adobe Sign erfüllt folgende Funktionen:

- **Workflow-Engine** – Mit der Workflow-Engine werden alle Geschäftsprozesse und Schritte ausgeführt und verwaltet, die für den Unterschriftsprozess notwendig sind. Die Workflow-Engine verwendet eine deklarative XML-basierte Definitionssprache, um die Bedingungen zur Ausführung kundenspezifischer Workflows und die Abfolge von Ereignissen zu beschreiben, die erforderlich sind, um einen Unterschrifts- oder Genehmigungsprozess abzuschließen.
- **Capability-basierte Sicherheit** – Mit dieser Sicherheitsmethode wird kontrolliert und überprüft, welche Ressourcen verfügbar sind und welche Vorgänge im Zusammenhang mit diesen Ressourcen durch einen authentifizierten Anwender oder ein Programm ausgeführt werden dürfen. Ressourcen umfassen sämtliche Informationen in Form von Dokumenten, Daten, Metadaten, Anwenderdaten, Berichten und APIs.
- **Dokumentenverarbeitung und -zugriff** – Die Dokumenten-Engine bietet zustandslose Funktionen zur Umwandlung verschiedener Dateiformate in PDF, Verschlüsselung und Entschlüsselung von Dateien und Rasterung von Bildern für die Anzeige in einem Webbrowser. Für sämtliche Prozesse zur Dokumentenverarbeitung greift Adobe Sign auf ein asynchrones, Warteschlangen-basiertes Nachrichtensystem zurück, das über alle Systemressourcen hinweg kommuniziert. Die gesamte Dokumentenverarbeitung und der Zugriff auf den Network Attached Storage (NAS) erfolgen im Hintergrund. Das heißt, alle Änderungen innerhalb von Adobe Sign werden für den Anwender sofort ersichtlich – in jedem Schritt des Workflows.
- **Ereignis-Management** – Mit den Funktionen für Ereignis-Management wird in jedem Schritt des Workflows ein Prüfprotokoll erstellt und gespeichert, das relevante Informationen zu jedem Anwender und Dokument enthält. In jeder Phase des Workflows erzeugt Adobe Sign ein Ereignis und sendet über ein asynchrones Nachrichtensystem eine Meldung an die entsprechenden Systemressourcen.
- **Kommunikation** – Adobe Sign informiert Anwender über Ereignisse im Zusammenhang mit Unterschriften und stellt (optional) unterzeichnete und zertifizierte Dokumente am Ende des Unterschriftsprozesses bereit. Um Spamming und Phishing zu vermeiden, ermöglicht Adobe Sign die Authentifizierung auf Basis von Systemen wie Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC) und Sender Policy Framework (SPF).

Datenebene.

Die Datenebene ist für den Zugriff auf die Transaktionsdatenbank, die Datenbank für das asynchrone Nachrichtensystem und den Dokumentenspeicher zuständig. Transaktionsdaten, die in der Datenzugriffsebene gespeichert werden, umfassen das ursprüngliche Kundendokument, Zwischenversionen des Dokuments, die während des Unterschriftsprozesses generiert wurden, Metadaten, Anwenderdaten, Ereignisse und das finale unterzeichnete PDF-Dokument, das von Adobe Sign verarbeitet wurde.

Integration über REST-API-Services.

Adobe Sign umfasst schlüsselfertige Integrationen für viele Business-Programme, Enterprise-Systeme und Vertrauensdienste. Darüber hinaus bietet Adobe Sign umfassende REST-APIs für die Anbindung an proprietäre Business-Systeme oder Firmen-Websites über sichere Webservices. Eine Liste der Business-Programme und Enterprise-Systeme, die von Adobe Sign unterstützt werden, findet ihr auf der Document Cloud-Seite mit dem Überblick über alle Integrationen für Business-Anwender. Unter www.adobe.com/trust/document-cloud-security/cloud-signatures-compliance.html[1] findet ihr eine vollständige Liste der Vertrauensdienste.

Datenfluss mit Adobe Sign.

Im Folgenden wird die Interaktion eines Anwenders mit Adobe Sign im Rahmen eines Unterschriftsprozesses beschrieben. Die Schrittfolge entspricht Abbildung 2.

1. **Repository-Elemente definieren:** Vor dem ersten Einsatz von Adobe Sign können Anwender eigene, wiederverwendbare Workflow-Definitionen, Bibliotheksvorlagen und Web-Formulare erstellen und im Adobe Sign-Repository speichern. Jeder Anwender mit Zugriffsrechten für diese Elemente kann eine Bibliotheksvorlage versenden, einen Workflow initiieren oder ein Web-Formular veröffentlichen, um Unterschriftsprozesse in die Wege zu leiten.

2. **Dokument zusammenstellen:** Um einen Workflow zum Versenden einer Vereinbarung mit Adobe Sign zu initiieren, legt der Anwender die Teilnehmer fest, die Reihenfolge, in der sie am Prozess teilnehmen, sowie verschiedene Optionen zur genaueren Definition ihrer Teilnahme. Der Workflow kann auch über eine schlüsselfertige Integration von Adobe oder über das Programm eines Partners oder Kunden erfolgen, das mit der Adobe Sign-API erstellt wurde. Vereinbarungen können basierend auf einer hochgeladenen Liste mit E-Mail-Adressen an mehrere Empfänger gleichzeitig verschickt werden.

   Als Nächstes lädt der Anwender die Quelldokumente hoch, die zur Vereinbarung gehören. Adobe Sign unterstützt den Import von Dokumenten aus dem Cloud-Speicher eines Drittanbieters, aus einem angebundenen Kunden- oder Partnerprogramm, aus einer vorhandene Bibliotheksvorlage oder vom Desktop des Anwenders.

3. **Vereinbarung erstellen:** Ein Dokument, das in Adobe Sign hochgeladen wurde, wird automatisch als Vereinbarung betrachtet. Wenn es sich um ein Formular mit vordefinierten Feldern auf Basis einer Bibliotheksvorlage handelt, fügt Adobe Sign diese Felder automatisch in die Vereinbarung ein. Wenn keine Bibliotheksvorlage verwendet wurde, muss der Anwender die gewünschten Felder manuell zur Vereinbarung hinzufügen, damit der Empfänger weiß, an welchen Stellen er unterschreiben muss.

   Adobe Sign bietet Anwendern die Möglichkeit, Unterschriftsfelder an logischen Positionen in der Vereinbarung zu platzieren und Formularfelder zur Angabe von Informationen wie E-Mail-Adresse, Vorname, Name und Titel hinzuzufügen. Dieser Prozess wird als Authoring bezeichnet.

   Jede Vereinbarung muss mindestens ein Unterschriftsfeld enthalten. Das Unterschriftsfeld kann beim Authoring oder automatisch von Adobe Sign platziert werden. Bei der automatischen Variante wird das Unterschriftsfeld am Ende der Vereinbarung hinzugefügt (wenn genügend Platz vorhanden ist). Alternativ wird die Vereinbarung durch eine zusätzliche Seite zum Unterschreiben ergänzt. Diese Informationen können später exportiert und in nachgelagerten Prozessen verwendet werden.

4. **Link weitergeben:** Sobald der Anwender das Authoring abgeschlossen hat, wird die Vereinbarung allen Teilnehmern per E-Mail, Web-Formular oder mithilfe der Adobe Sign-API in einem benutzer-definierten Programm bereitgestellt.

5. **Unterschriften einholen:** Je nachdem, welche Parameter die Vereinbarung umfasst, werden Unterzeichner dazu aufgefordert, ihre Genehmigung zu übermitteln, eine Unterschrift zu leisten und/oder Formularfelder auszufüllen. Die Formularfelder können vom Verfasser als optionale Felder oder Pflichtfelder festgelegt und maskiert oder auf verschiedene Weise formatiert werden. Alle Informationen werden zusammen mit dem aktuellen Status der Vereinbarung (Wer hat unterschrieben? Wer muss als Nächstes unterschreiben?) im Adobe Sign-Datenspeicher in der Cloud gespeichert. In dieser Phase können auch Anhänge erfasst werden.

6. **Unterzeichnete Vereinbarung verwerten:** Nachdem alle Unterzeichner den Workfow zur Unterzeichnung abgeschlossen haben, wird die vollständig ausgefüllte und unterzeichnete Vereinbarung für alle Teilnehmer am Unterschriftsprozess bereitgestellt und automatisch im Cloud-Speicher von Adobe Sign gespeichert. Über Adobe Sign-Clients können Anwender alle Artefakte im Zusammenhang mit dem Unterschriftsprozess herunterladen, darunter die unterzeichnete Vereinbarung (zertifizierte PDF-Datei), ein Prüfprotokoll (zertifizierte PDF-Datei) und einen separaten Bericht mit Datenwerten aus Formularfeldern (als CSV-Datei exportierbar). Optional kann die Verein-barung über Adobe Sign-APIs oder den Archivierungs-Service eines Partners in das gewünschte System verschoben oder kopiert werden.

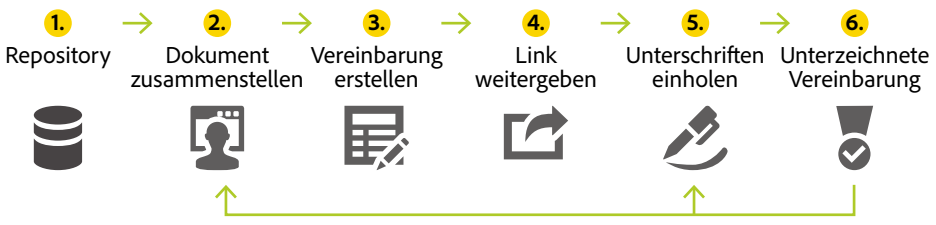

Abb. 2: Datenfluss mit Adobe Sign

Sicherheitsarchitektur von Adobe Sign.

Das folgende Diagramm veranschaulicht die Sicherheitsarchitektur von Adobe Sign, einschließlich Servern für externe Anfragen, Cloud-Servern und Client-Zugriff.

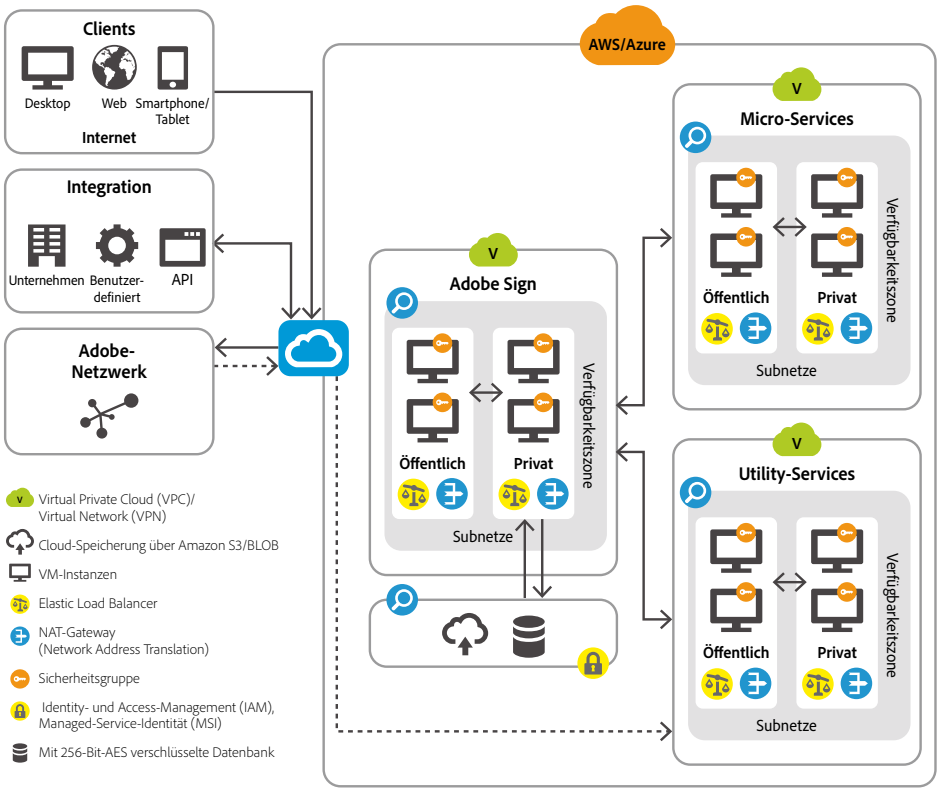

Abb. 3: Architektur der Netzwerksicherheit von Adobe Sign

Extern erreichbare Server.

Extern erreichbare Server innerhalb der gehosteten Netzwerkarchitektur von Adobe Sign sind *Webserver*, die Browser- und API-Anfragen verarbeiten, und *Mailserver* für den eingehenden und ausgehenden E-Mail-Verkehr. Die Webserver und zugewiesenen Lastverteiler verteilen dynamische Anfragen an die Programm-Server. Die Webserver wenden zudem integrierte Filterregeln an, um Angriffe aus dem Web abzuwehren, sowie Firewall-Schutz, um die Zugriffskontrolle zu erhöhen.

Virtuelle Cloud-Netzwerke.

Die Sicherheitsarchitektur von Adobe Sign umfasst zudem mehrere virtuelle Cloud-Netzwerke. Bei AWS werden diese Netzwerke als „Virtual Private Cloud" (VPC) bezeichnet, bei Microsoft Azure als „Virtual Network" (VNet).

VPCs/VNets sind logisch isolierte Netzwerke, die von außen nur über stark beschränkte Eingangs- und Ausgangspunkte zugänglich sind. Innerhalb eines VPC/VNet gibt es Subnetze mit einer Reihe von IP-Adressen. Subnetze können entweder privat oder öffentlich sein. Ein öffentliches Subnetz ist mit dem Internet verbunden, ein privates Subnetz nicht. Adobe Sign verwendet VPCs/VNets wie folgt:

- ein VPC/VNet als Kernelement für zentrale Business-Prozesse mit Adobe Sign
- ein VPC/VNet für Micro-Services wie die Integration mit dem Cloud Signature Consortium, die Validierung von Signaturen oder das Entfernen von Signaturbildern im Hintergrund
- ein VPCs/VNet für Utility-Services, um die Überwachung von Ereignissen und andere administrative Funktionen zu verwalten

Alle diese Services werden auf skalierbaren, sicheren, virtuellen Cloud-Servern ausgeführt, auf die nur über das gesicherte Subnetz und die Netzwerkbeschränkungen für VPC/VNET zugegriffen werden kann.

Um eine hohe Verfügbarkeit sicherzustellen, werden VPC-/VNet-Instanzen in mehrere redundante Verfügbarkeitszonen unterteilt. Verfügbarkeitszonen werden physisch voneinander isoliert, damit Strom-, Netzwerk- oder sonstige Ausfälle der Infrastruktur in einer Verfügbarkeitszone den Betrieb

in anderen Verfügbarkeitszonen nicht beeinträchtigen. Alle Daten werden über alle Verfügbarkeitszonen hinweg repliziert, und innerhalb jeder Verfügbarkeitszone auf mehreren Servern.

Der Netzwerkzugriff innerhalb einer VPC-/VNet-Instanz wird über eine Sicherheitsgruppe geschützt. Wie virtuelle Firewalls ermöglichen Sicherheitsgruppen die genauere Kontrolle des eingehenden und ausgehenden Datenverkehrs von einer VPC-/VNet-Instanz. Adobe kann auf diese Weise sicherstellen, dass nur berechtigte Anwender autorisierte Aktionen ausführen. Die Adobe Sign-Architektur integriert zusätzlich Sensoren zur Erkennung von Angriffen an kritischen Stellen, um Service-übergreifende Systemintegrität und -sichtbarkeit zu garantieren.

Client-Zugriff.
Der Adobe Sign-Service ist über verschiedene Client-Endpunkte zugänglich, z. B. Browser und Mobile Apps. Verbindet sich ein Client mit Adobe Sign in der jeweiligen Region, erfolgt die Verbindung per Internet-Gateway mit einem bestimmten VPC/VNet. Sämtliche Client-Verbindungen erfolgen über HTTPS-Verbindungen mit dem TLS-Protokoll Version 1.2 und mindestens mit 128-Bit-AES-Verschlüsselung.

Datenverschlüsselung.

Adobe Sign verwendet PCI DSS-geprüfte Verschlüsselungsalgorithmen[1], um Dateien im Ruhemodus mit 256-Bit-AES zu verschlüsseln. Um die sichere Datenübertragung über HTTPS zu gewährleisten, unterstützt Adobe Sign das TLS-Protokoll Version 1.2.

Der Zugriff auf Dokumente im Ruhemodus ist nur mit Capability-basierten Berechtigungen über die Datenzugriffsebene in einem privaten Subnetz möglich. Absender haben zudem die Option, ein Dokument mit einem privaten Kennwort zusätzlich zu schützen. Verschlüsselungsschlüssel werden in einer sicheren Umgebung mit eingeschränktem Zugriff gespeichert und verwaltet.

Identitäts-Management in Adobe Sign.

Adobe Sign setzt rollenbasiertes Identitäts-Management ein, um die Authentifizierung, Autorisierung und Zugriffskontrolle innerhalb des gesamten Adobe Sign-Systems zu steuern. Die Capability-basierten Sicherheits- und Authentifizierungsprozesse für Kundenorganisationen werden von einem Adobe Sign-Administrator definiert und aktiviert. Adobe Sign unterstützt die Definition folgender Anwenderrollen:

- **Absender** – Lizenzierter Anwender, der von seinem Administrator spezielle Adobe Sign-Berechtigungen erhalten hat, um Unterschrifts-Workflows für Dokumente zu erstellen und Dokumente zur Unterzeichnung, Genehmigung oder Ansicht zu versenden.
- **Unterzeichner** – Verifizierter Anwender, der von einem Absender die Genehmigung erhalten hat, ein bestimmtes Dokument zu unterzeichnen. Standardmäßig sendet Adobe Sign eine E-Mail an den Unterzeichner, die eine eindeutige URL für das Dokument enthält, das unterzeichnet werden soll. Die URL enthält exklusive IDs für die betreffenden Transaktionen.
- **Genehmiger** – Verifizierter Anwender, der von einem Absender die Berechtigung erhalten hat, ein bestimmtes Dokument zu genehmigen.
- **Andere** – Verifizierte Anwender, die von einem Absender die Berechtigung erhalten haben, ein bestimmtes Dokument oder Prüfprotokoll anzuzeigen.

Authentifizierung von Anwendern.

Adobe Sign unterstützt mehrere Authentifizierungsmethoden, darunter Ein- und Multi-Faktor-Authentifizierung.

Ein lizenzierter Anwender muss sich in der Regel mit einer verifizierten E-Mail-Adresse und einem Kennwort bei Adobe Sign anmelden, die beide einer authentifizierten Identität zugeordnet sind, z. B. einer Adobe ID. Administratoren können die Sicherheitsstufe und Komplexität eines Kennworts festlegen, die Häufigkeit der erlaubten Änderungen, den Vergleich mit früheren Kennwörtern sowie Richtlinien zum Sperren eines Kennworts (beispielsweise eine Frist zur Kennworterneuerung).

Adobe Sign unterstützt folgende Authentifizierungsoptionen:

- **Adobe Sign ID** – Eine Kombination aus verifizierter E-Mail-Adresse und Kennwort, die von einem lizenzierten Anwender für die sichere Anmeldung bei Adobe Sign verwendet wird.
- **Adobe ID** – Eine Adobe ID ermöglicht den Zugriff auf alle lizenzierten Adobe-Services, darunter auch Adobe Sign.

- **Google ID** – Anwender werden durch einen Google-Service wie Google Mail oder Google Apps authentifiziert.
- **Single Sign-on (SSO)** – Unternehmen, die striktere Zugriffskontrollen benötigen, können SSO über Security Assertion Markup Language (SAML) nutzen, um Adobe Sign-Anwender auf Basis ihres internen Identitätssystems zu verwalten. Adobe Sign kann außerdem für die Systeme führender Anbieter im Bereich Identitäts-Management konfiguriert werden, z. B. Okta und OneLogin.

Weitere Informationen zur Aktivierung von Single Sign-on über SAML findet ihr unter www.adobe.com/go/adobesign_saml_configuration[1].

Mehr über Adobe Identity Management Services (IMS) erfahrt ihr im Überblick über die Sicherheit von Adobe Identity Management Services[1].

Geografischer Standort von ID-Daten.

Adobe Sign-Kunden verwenden in der Regel die Admin Console zur Anwenderverwaltung. In diesem Szenario werden ID-Daten in dem Rechenzentrum gespeichert, in dem Adobe Sign gehostet wird, und in allen Rechenzentren repliziert, die Adobe IMS-Informationen verarbeiten (unabhängig vom Standort des Kunden). Die Rechenzentren, die zur Lastenverteilung auf mehrere Regionen verteilt sind, befinden sich in Virginia (USA Ost), Oregon (USA West), Irland (EU West) und Singapur.

Hinweis: ID-Daten von Kunden werden in dem Rechenzentrum gespeichert, das dem geografischen Standort des jeweiligen Kunden zugeordnet ist. Für Adobe Sign-Kunden, die Adobe IMS und die Admin Console zur Anwenderverwaltung verwenden, werden ID-Daten zusätzlich in hochverfügbaren Adobe IMS-Rechenzentren in Virginia (USA Ost), Oregon (USA West), Irland (EU West) und Singapur repliziert.

Verifizierung der Identität eines Unterzeichners.

Die grundlegende Verifizierung der Identität bei Adobe Sign erfolgt mittels einer E-Mail-Anfrage an den betreffenden Unterzeichner. Diese Methode wird als erste Stufe der Verifizierung betrachtet, weil die Mehrheit der Anwender alleinigen Zugriff auf ihr E-Mail-Konto hat. Die erste Stufe der Verifizierung wird oft für Unterzeichner, Genehmiger und andere Anwenderrollen verwendet. Um die Sicherheit zu erhöhen und Manipulationen vorzubeugen, können zusätzliche Authentifizierungsmethoden wie Telefon, SMS, wissensbasierte Authentifizierung (Knowledge-Based Authentication, KBA) oder die Identitätsprüfung anhand offizieller Ausweisdokumente in den Prozess eingebunden werden, sofern sie in der Region des Kunden verfügbar sind. Weitere Informationen über die aktuellen Methoden zur Verifizierung der Identität von Unterzeichnern findet ihr unter helpx.adobe.com/de/sign/using/signer-identity-authentication-methods.html.

Zertifizierung von Dokumenten in Adobe Sign.

In jeder Phase des Workflows schützt Adobe Sign das Dokument, um seine Integrität und Authentizität sicherzustellen. Über eine PKI (Public Key Infrastructure) werden finale PDF-Dokumente und Prüfprotokolle mit einer digitalen Signatur zertifiziert, bevor sie an alle Beteiligten verteilt werden.

Die Signatur zur Zertifizierung wird mit einem SHA-256-Hash-Algorithmus erstellt, der einen eindeutigen, verschlüsselten Fingerabdruck aus der finalen unterzeichneten PDF-Datei ermittelt. Die grafisch als blaues Banner mit Zertifizierungs-Badge dargestellte digitale Signatur im oberen Bereich des unterzeichneten PDF-Dokuments verifiziert die Integrität des Dokuments (siehe Abbildung 4) und bestätigt, dass das Dokument innerhalb von Adobe Sign generiert und seit der Anwendung des Zertifikats nicht verändert wurde. Das zertifizierte PDF-Dokument kann bei Bedarf zusätzlich durch ein Kennwort geschützt werden.

Abb. 4: Zertifizierungs-Banner von Adobe Sign

Um die Schlüssel zum Sperren und Zertifizieren des unterzeichneten PDF-Dokuments zu erzeugen, verwendet Adobe Sign Zertifikate, die von mehreren Vertrauens- und Zeitstempeldiensten ausgegeben werden. Unter bestimmten Umständen kann Adobe Sign so konfiguriert werden, dass die Signatur zur Zertifizierung unter Verwendung eines speziellen Zertifikats erfolgt, das bestimmte regionale oder Compliance-Anforderungen voraussetzt. PKI-Schlüssel zur Zertifizierung des finalen PDF-Dokuments werden in Hardware-Sicherheitsmodulen gespeichert, um ein Höchstmaß an Sicherheit und Compliance zu erfüllen.

Hosting und Sicherheit von Adobe Sign.

Die Service-Infrastruktur von Adobe Sign wird in Rechenzentren der Kategorie „Tier 4" des American National Standards Institute (ANSI) gehostet und von Amazon Web Services (AWS) und Microsoft Azure verwaltet, unseren bevorzugten Anbietern für Cloud-Hosting. Alle Hosting-Partner führen äußerst strenge Kontrollen in Bezug auf den Zugriff auf Rechenzentren, Fehlertoleranz, Umgebungssicherung und Netzwerksicherheit durch. Nur zugelassene, autorisierte Adobe-Mitarbeiter, Mitarbeiter bei Anbietern von Cloud-Services und Vertragspartner mit einem legitimen und anerkannten Unternehmen haben Zugriff auf die gesicherten Standorte. Weitere Informationen zu den Rechenzentren, die für Adobe Sign-Services verwendet werden, findet ihr im Support-Bereich der Adobe-Website[1].

Weitere Informationen zur Sicherheit von Amazon Web Services findet ihr unter https://aws.amazon.com/de/security

Weitere Informationen zur Sicherheit von Microsoft Azure findet ihr unter https://azure.microsoft.com/de-de/services/security-center/

Adobe Sign-Netzwerk-Management.

Da über das Adobe Sign-Netzwerk Daten gesammelt, bereitgestellt und für Auswertungen aufbereitet werden, hat seine Sicherheit hohe Priorität. Die Sicherheitsmaßnahmen zum Schutz der Netzwerkarchitektur umfassen zum Beispiel die Segmentierung der Entwicklungs- und Produktionsumgebungen und rollenbasierte Zugriffskontrolle (RBAC).

Sicheres Management.

Alle Management-Zugriffe auf die Server erfolgen über verschlüsselte Kanäle, die nur über das Firmennetzwerk von Adobe zugänglich sind. Bei jedem Zugriff ist eine Zwei-Faktor-Authentifizierung erforderlich.

Service-Monitoring.

Alle Server, Router, Switches, Load-Balancer und andere wichtige Komponenten des Adobe Sign-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.

Adobe Sign nutzt zudem moderne Technologien und branchenführende Anbieter für die programmspezifische Überwachung und Ausgabe von Warnmeldungen. SLIs und SLOs werden kontinuierlich nachverfolgt, und Verstöße führen zu Warnmeldungen auf der entsprechenden Warnstufe.

Datenverfügbarkeit.

Adobe Sign-Daten werden in Datenbanken und Cloud-Repositorys gespeichert. Datenbanken werden über mehrere Verfügbarkeitszonen hinweg repliziert und regelmäßig gesichert. Cloud-Repositorys bieten eigene Redundanzmechanismen mit einer hohen Beständigkeit von 99,999999999 % im Jahr. In Regionen, in denen Disaster-Recovery-Pläne für Adobe Sign verfügbar sind, werden alle Daten in eine sekundäre Region repliziert.

Änderungs-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 Adobe Sign-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.

Adobe Sign-Instanzen und Produkt-Updates einschließlich Sicherheits-Updates werden über die Implementierungs-Pipeline angewendet (weitere Informationen zum Implementierungsmodell findet ihr weiter vorne im Dokument).

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 Sign. Für Adobe Sign-Umgebungen stellt Adobe integrierte Sicherheitsfunktionen zur Verfügung, die die Zugriffskontrolle über Gruppen und Berechtigungen ermöglichen.

Administratoren bei Adobe haben nur in Ausnahmefällen Zugriff auf Kundenvereinbarungen, z. B., wenn dies zur Problembehebung erforderlich ist. Wenn ein Administrator zur Umsetzung seiner Aufgaben Zugriff benötigt, wird ihm eine rollenbasierte Zugriffsberechtigung zugewiesen. Jeder Zugriff erfordert die Genehmigung sowohl vom Kunden als auch von einem Administrator, dem die Rolle als Genehmiger zugewiesen wurde. Der Zugriff erfordert außerdem eine Zwei-Faktor-Authentifizierung und wird protokolliert.

Protokolle.

Schutz vor nicht autorisierten Zugriffen und Änderungen bieten Netzwerk- und OS-bezogene Protokolle sowie Intrusion-Detection-Systeme, die eine Kombination aus branchenüblichen Technologien und Tools von Adobe umfassen. Adobe überprüft regelmäßig (und erweitert bei Bedarf) die Speicherkapazität für Protokolle. Von Adobe-Systemen generierte Protokolle werden speziell gesichert. Der Zugriff auf Protokolle und Protokollierungs-Software ist auf autorisierte Adobe-Mitarbeiter beschränkt. Adobe bewahrt die Originalprotokolle ein Jahr lang auf. Zugriff auf die Protokolle erfolgt ausschließlich durch Adobe-Mitarbeiter.

Physische Sicherheit und Umgebungssicherung in 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 Sign 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 Sign 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 gegebenenfalls 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.

Verfügbarkeit und Benachrichtigung.

Adobe Sign wird über kontinuierlich aktive Rechenzentrumkonfigurationen in Verfügbarkeitszonen von Amazon Web Services (AWS) und Microsoft Azure gehostet. Alle Adobe Sign-Rechenzentren sind äußerst belastbar, auf hohe Verfügbarkeit ausgerichtet und so konzipiert, dass System- oder Hardware-Ausfälle nur minimale Auswirkungen auf die Kunden haben. Jedes Rechenzentrum wird in seiner eigenen, unabhängigen Infrastruktur ausgeführt, um bei einem Ausfall die betriebliche Kontinuität sicherzustellen. Weitere Informationen zu unseren Rechenzentrumkonfigurationen, darunter die angestrebten Parameter für Recovery Point Objective (RPO) and Recovery Time Objective (RTO), findet ihr im Support-Bereich der Adobe-Website[1].

Informationen zu den Betriebszeitdaten von Adobe Sign erhaltet ihr auf der Adobe Status-Website[1]. Darüber hinaus werden Adobe Sign-Kunden sowohl über geplante als auch ungeplante Ausfallzeiten und den jeweiligen Status des Service benachrichtigt. Wenn die Notwendigkeit besteht, den Betrieb von einem Hauptstandort zu einem alternativen Standort für den Disaster-Recovery-Prozess zu migrieren, erhalten Kunden spezielle Benachrichtigungen mit folgenden Informationen:

- Benachrichtigung zur geplanten Migration der Services zum Disaster-Recovery-Standort
- Stündliche Updates zum Fortschritt der Migration
- Benachrichtigung nach Abschluss der Migration

Die Benachrichtigungen umfassen auch Kontaktinformationen und Hinweise zur Verfügbarkeit des Kunden-Supports und der Success Manager. Diese Mitarbeiter beantworten Fragen während und nach der Migration, um die reibungslose Wiederaufnahme des Betriebs am alternativen Standort zu gewährleisten.

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 von Adobe Secure Product Lifecycle (SPLC) zuständig.

Der CSO leitet auch das Adobe Secure Software Engineering Team (ASSET), ein zentrales Team von Sicherheitsexperten, die den Produkt- und Entwickler-Teams von Adobe, u. a. den Adobe Sign-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.

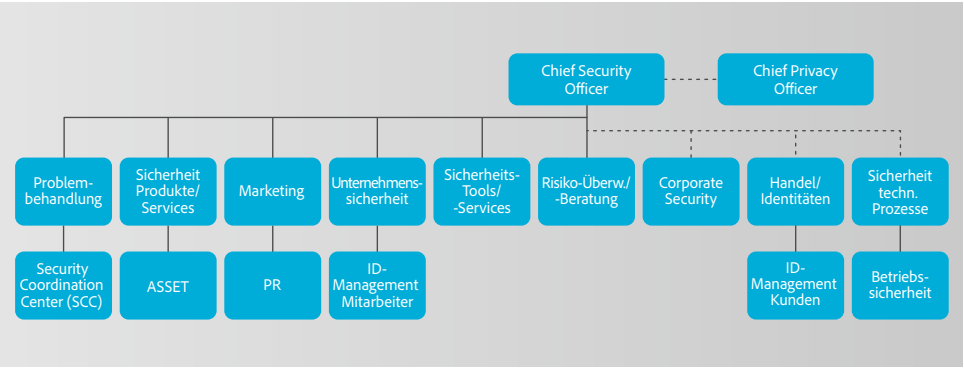

Abb. 6: Adobe-Sicherheitsorganisation

Entwicklung sicherer Adobe-Produkte.

Wie bei anderen wichtigen Produkten und Services von Adobe wird für die Adobe Sign-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 Sicherheitsmethoden und Bedrohungen stets auf dem neuesten Stand.

Adobe Secure Product Lifecycle.

Die Adobe SPLC-Aktivitäten umfassen, je nach betroffener Adobe Sign-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-Programmen 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 Programmen und Netzwerken
- Beurteilung der Produktreife, Notfallpläne, Veröffentlichung von Unterlagen für Entwickler

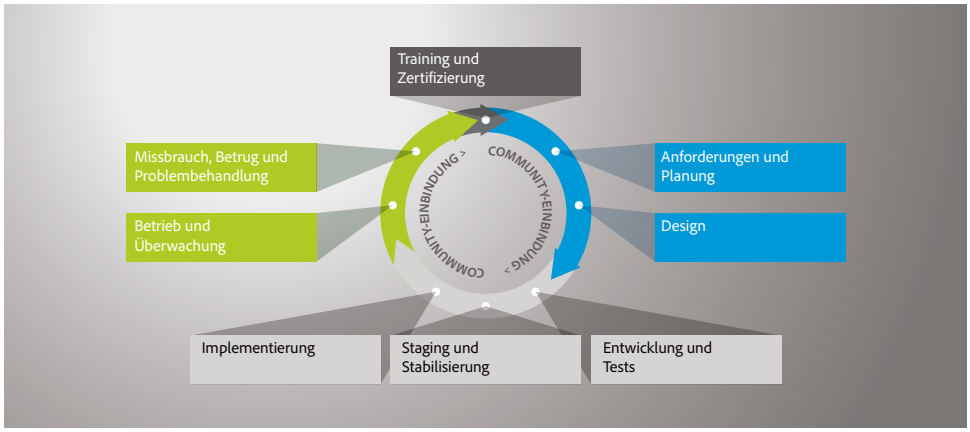

Abb. 7: Adobe Software Product Lifecycle (SPLC)

Weitere Informationen über die Adobe-Sicherheitsorganisation und den SPLC findet ihr unter www.adobe.com/de/security.

Adobe Software Security Certification Program.

Im Rahmen des Adobe Secure Product Lifecycle führt Adobe regelmäßig Sicherheits-Trainings 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.

Einige Adobe Sign-Teams nehmen an zusätzlichen Sicherheits-Trainings und -Workshops teil, in denen vermittelt wird, welche Auswirkungen das Thema Sicherheit auf ihre jeweiligen Funktionen innerhalb ihrer Organisation und im gesamten Unternehmen haben. Weitere Informationen findet ihr im Whitepaper zur Sicherheitskultur bei Adobe[1].

Adobe Sign und Compliance.

Adobe Sign ermöglicht verifizierten Unterzeichnern weltweit die Interaktion mit digitalen Dokumenten von überall und mit jedem Gerät – in Übereinstimmung mit zahlreichen branchenüblichen und gesetzlichen Standards. Kunden behalten die Kontrolle über ihre Dokumente, Daten und Workflows und können steuern, wie sie die lokalen oder regionalen Vorschriften wie die Datenschutz-Grundverordnung (DSGVO) der EU am besten einhalten. Weitere Informationen zu Adobes Richtlinien für Datenschutz findet ihr unter www.adobe.com/de/privacy.

Mehr über regionale Gesetze zu elektronischen Signaturen sowie die Compliance von Adobe Sign erfahrt ihr unter www.adobe.com/de/trust.html.

Adobe Common Controls Framework.

Das Adobe Common Controls Framework (CCF) umfasst eine Reihe von Sicherheitsmaßnahmen und Compliance-Kontrollen, die in den Produkt-Teams sowie in verschiedenen Teilen der Infrastruktur- und Anwendungsteams im Einsatz sind. Bei der Entwicklung des CCF hat Adobe die Kriterien der gängigsten Sicherheitszertifikate für Cloud-basierte Unternehmen analysiert. Mehr als 1.350 Anforderungen wurden in Adobe-spezifische Kontrollmechanismen umgesetzt, die etwa einem Dutzend Branchenstandards entsprechen.

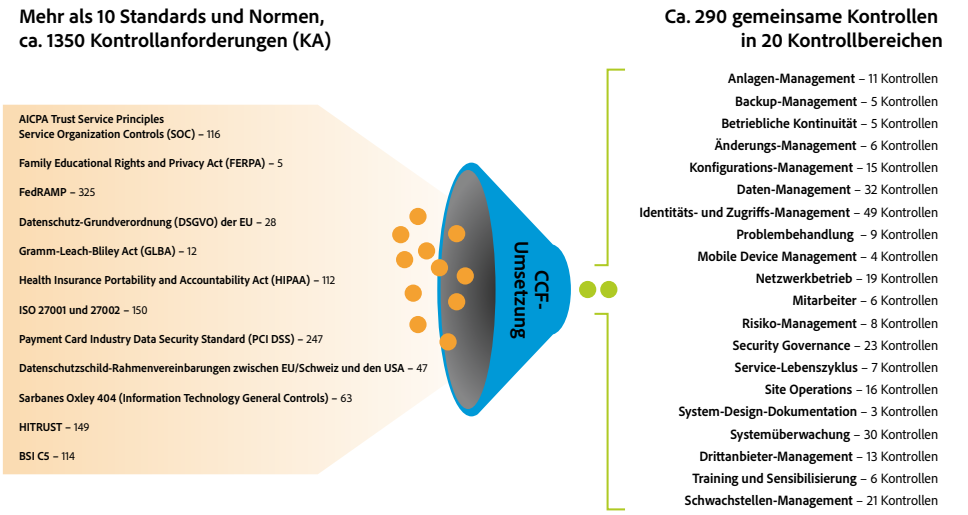

Abb. 8: Adobe Common Controls Framework (CCF)

Risiko- und Schwachstellen-Management bei Adobe.

Das Ziel sind kurze Reaktionszeiten, erfolgreiche Risikominderung und effektive Fehlerbehebung. Im Rahmen des Risiko- und Schwachstellen-Managements überwacht Adobe die aktuelle Bedrohungslage, tauscht Informationen mit Sicherheitsexperten auf der ganzen Welt aus, behebt Vorfälle innerhalb kürzester Zeit und leitet sämtliche Informationen an seine Entwickler-Teams weiter. So wird für alle Adobe-Produkte die größtmögliche Sicherheit erzielt.

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. Adobe führt einmal im Jahr und vor jedem größeren Release einen Penetrationstest durch. Schwachstellen-Scans werden monatlich, Web- und Datenbank-Scans vierteljährlich ausgeführt.

Einmal im Jahr und vor jedem Release führt das Sicherheits-Team für Adobe Sign eine Risikoeinschätzung aller Komponenten durch. Das Sicherheits-Team für Adobe Sign arbeitet gemeinsam mit den Leitern für Technik/IT und Entwicklung vor jedem Release an der Behebung aller riskanten Schwachstellen. Weitere Informationen zu den Penetrationstests findet ihr im Whitepaper zum Thema Sicherheit in der Entwicklung bei Adobe[1].

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.

Weitere Informationen zu diesem Thema findet ihr im Whitepaper über den Umgang mit Zwischenfällen bei Adobe[1].

Forensische Analyse.

Bei der Untersuchung von Vorfällen verwendet das Adobe Sign-Team den forensischen Analyseprozess, der je nach Bedarf ein vollständiges Image bzw. ein Speicherabbild des/r betroffenen Rechner(s), eine sichere Beweisaufbewahrung sowie eine lückenlose Dokumentation der Überwachungskette umfasst. Adobe bietet eine Funktion zur Datenhaltung, mit der Adobe Sign-Vereinbarungsdaten nach Vertragserfüllung in einem vom Kunden definierten Intervall automatisch gelöscht werden. Darüber steht Kunden eine Verwaltungsoberfläche zur Verfügung, über die sie ausgewählte Daten manuell löschen können.

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 Sign verwendet Adobe segmentierte Entwicklungs- und Produktionsumgebungen, bei denen der Zugriff auf Live-Produktionssysteme auf Netzwerk- und Programmebene 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 Dokument beschrieben wurden, dienen dem Schutz von Adobe Sign 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 findet ihr auf der Website des Adobe Trust Center.

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

[1] In englischer Sprache.
[2] Die automatische Wiederherstellung ist auf die Infrastruktur von Amazon Web Services beschränkt.

9/20