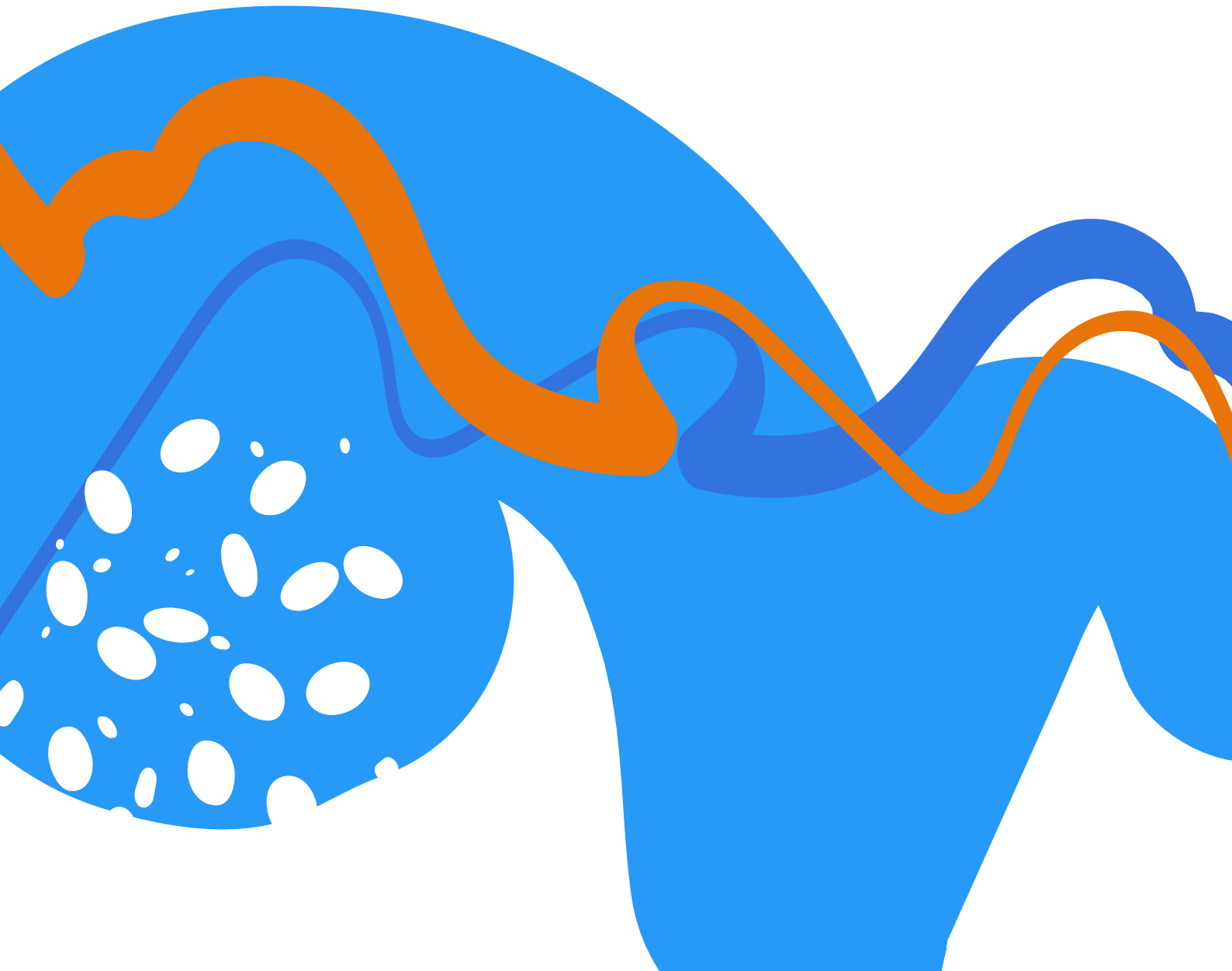
WHITEPAPER

Sicherheit bei Adobe-Produkten: Überblick.



Inhalt

Einführung 3

Strategie 3

Adobe Secure Product Lifecycle 3

Adobe Application Security Stack 4

- Nativ sichere Plattformen 4
- Automatisierung 5
- Prozess 5

Fazit 7

Einführung.

Für Adobe steht Sicherheit an erster Stelle. Aus diesem Grund investieren wir umfassend in Sicherheitsforschung und -technologie. Unser Team für Programmsicherheit arbeitet gemeinsam mit Produkt- und Serviceteams an der Entwicklung von Lösungen, die technologisch auf dem neuesten Stand sind und native Sicherheit gewährleisten. Verschiedene Automatisierungsmechanismen helfen dem Team, Daten zu potenziellen Risiken zu sammeln und Entscheidungen zu vereinfachen, die die Sicherheit bei Adobe insgesamt verbessern.

Dieses Whitepaper behandelt Adobes Strategie für sichere Software. Im Fokus steht die frühzeitige Einbindung von Sicherheitskontrollen in den Entwicklungszyklus mit dem Ziel, Prozesse zu skalieren, Gesamtkosten zu reduzieren und Sicherheitsrisiken zu minimieren. Wir setzen auf moderne Sicherheitsverfahren zum Schutz der Daten und Workflows sowohl von Adobe als auch von Userinnen und Usern.

Strategie.

Statt Symptome zu behandeln, konzentriert sich Adobe darauf, die Ursachen von Sicherheitsproblemen zu beheben. Wir nutzen dazu die sogenannte „Shift Left"-Methode und binden Sicherheit schon früh in die Programmentwicklung ein. Von den Spezifikationen über Architektur und Design bis zur Programmierung kommen Sicherheitskontrollen und -mechanismen in allen Phasen der Entwicklung zum Einsatz. So vermeiden wir kostspielige Änderungen in den späteren Testphasen. Außerdem reduzieren wir mit diesem Ansatz die Wahrscheinlichkeit von Sicherheitsrisiken bei der Nutzung des betreffenden Programms.

Adobe Secure Product Lifecycle.

Der Adobe Secure Product Lifecycle (SPLC) bildet die Grundlage für Sicherheit bei Adobe und wird im gesamten Produktzyklus berücksichtigt – von Design und Entwicklung bis zu Qualitätssicherung, Test und Bereitstellung. Das Regelwerk aus mehreren Hundert strengen, auf größtmögliche Sicherheit ausgerichteten Aktivitäten gibt klar strukturierte, reproduzierbare Prozesse und Funktionen vor, die unsere Teams dabei unterstützen, Produkte und Services inhärent sicher zu machen.

SPLC-Richtlinien werden im gesamten Unternehmen implementiert und vom Adobe-Team für Programmsicherheit überprüft. Dieses Team berät unsere Produkt- und Serviceteams zu Best Practices für Sicherheitskontrollen und validiert diese Kontrollen mithilfe von automatisierten Verfahren. Zu den Kontrollen des SPLC zählen Roadmaps, Sicherheitswerkzeuge und Testmethoden, mit denen das Sicherheits-Team die vom Open Web Application Security Project (OWASP) veröffentlichten Top 10 schwerwiegender Sicherheitslücken in Programmen und die von CWE/SANS veröffentlichten 25 riskantesten Software-Fehler leichter erkennen und vermeiden kann. Weitere Informationen zum SPLC sind im Adobe Trust Center zu finden.

Adobe Application Security Stack.

Das Grundgerüst für die Entwicklung sicherer Programme heißt Adobe Application Security Stack. Die Produkt-Teams nutzen nativ sichere Plattformen, überprüfen Programme mit verschiedenen automatisierten Sicherheitsfunktionen und ergänzen diese Maßnahmen um Sicherheitsprüfungen und manuelle Tests.

Die drei Ebenen des Stacks umfassen eine Reihe von Werkzeugen und Services, die auf modernen Verfahren zum Schutz der Daten und Workflows von Userinnen und Usern beruhen. Die Produkt-Teams von Adobe können diese Verfahren bei der Programmentwicklung nutzen, um die Sicherheit zu erhöhen.

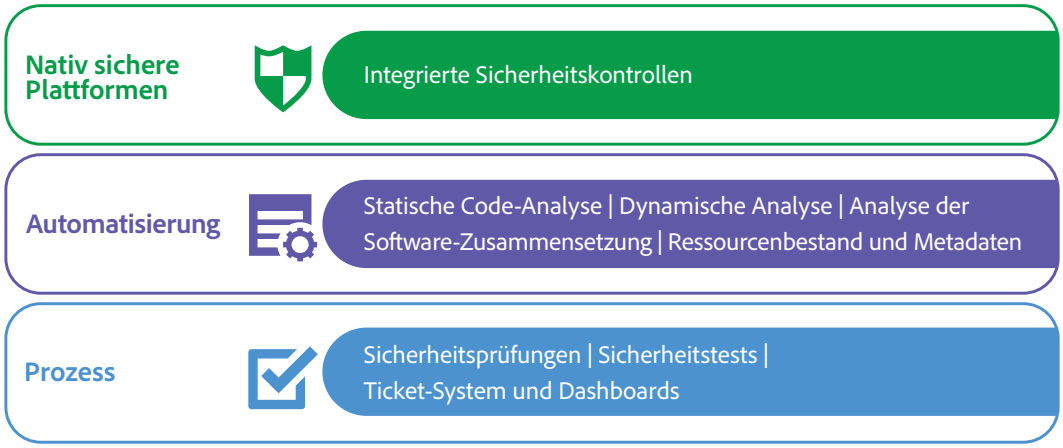


Abbildung 1: Adobe Application Security Stack

Nativ sichere Plattformen.

Die Entwicklungs-Teams erstellen auf der Grundlage vorab genehmigter, nativ sicherer Plattformen sorgfältig geplante Pfade, die bei der Entwicklung von Produkten und Services als sicherheitstechnische Orientierungshilfe dienen. Hierzu zählen geprüfte und genehmigte Identitäts- und Autorisierungs-Services, ein API-Gateway, Messaging-Systeme, SDKs und Frameworks.

Nativ sichere Plattformen vereinfachen die Skalierung und die Überprüfung der implementierten Sicherheitsfunktionen und -konfigurationen. Diese Plattformen basieren auf den zwei Grundprinzipien Erkennung und Prävention. Sie beinhalten mehrere Lösungen für kontinuierliche Erkennung, die eine mögliche unsichere Nutzung aufdecken können, sowie Präventivkontrollen, mit denen die Entwicklungs-Teams von Adobe bei Produkten und Services für inhärente Sicherheit sorgen können.

Nativ sichere Plattformen tragen zu Folgendem bei:

- **Sichere Nutzung:** Durch die kontinuierliche Analyse umfangreicher Mengen an Konfigurationsdaten, Protokollen und Quell-Code können wir sicherheitsrelevante Konfigurationsfehler in unseren Produkten und Services sowie Abweichungen schnell identifizieren und die zuständigen Produkt-Teams darüber informieren.
- **Integrierte Sicherheitskontrollen:** Investitionen in Sicherheitskontrollen, die Best Practices wie das Prinzip der geringsten Rechte („Principle of Least Privilege"), grundsätzliche Ablehnung („Default Deny") und integrierte Authentifizierung umfassen, ermöglichen es unseren Produkt-Teams, sich ganz auf die Produktentwicklung zu konzentrieren. Daten und Workflows von Userinnen und Usern werden zuverlässig geschützt.

Automatisierung.

Bei Adobe schafft Automatisierung die Voraussetzung für skalierbare, kontinuierliche Programmsicherheit, die mit dem schnellen Innovationstempo in der digitalen Welt Schritt hält. Initiativen zur statischen und dynamischen Analyse von Software-Code, Konfigurationsdaten, Anfragen/Antworten und Programmprotokollen tragen bei Adobe zum Schutz des gesamten Software-Entwicklungszyklus bei.

- **Statische Code-Analyse:** Auf unserer Plattform für automatisierte Code-Analysen werden Code-Repositorys mithilfe von Open-Source- und kommerziellen Tools gescannt. Wir geben unseren Entwicklungs-Teams Feedback an Punkten in ihrem Entwicklungs-Workflow, an denen Probleme am einfachsten zu beheben sind. Mit den genannten Tools sowie einzigartigen Funktionen in unserer Umgebung kann Adobe ein Höchstmaß an Sicherheit im Quell-Code erzielen.
- **Dynamische Analyse:** Ähnlich wie bei der statischen Code-Analyse ermittelt Adobe mit selbst entwickelten und kommerziellen Tools Sicherheitsschwachstellen zur Laufzeit.
- **Analyse der Software-Zusammensetzung:** Wir überwachen die Nutzung von Drittanbieter-Komponenten in unseren Produkten und Services und überprüfen die Sicherheit dieser Komponenten regelmäßig mit eigenen und kommerziellen Lösungen. Wenn wir eine Schwachstelle oder eine veraltete Komponente finden, benachrichtigen wir das zuständige Entwicklungs-Team.
- **Ressourcenbestand und Metadaten:** Anhand umfassender Metadaten aus dem gesamten Unternehmen erhält unser Team für Programmsicherheit genauere Einblicke in Adobe-Produkte und -Services.

Prozess.

Die Sicherheitsfachleute und speziellen Prozesse von Adobe bilden die Grundlage unserer Sicherheitsinitiativen. Wir investieren kontinuierlich in Training für unsere Sicherheits-Teams sowie für unsere „Security Champions", die sich mit neuen Technologien und Ansätzen befassen. Ein Ticket-System, Dashboards sowie Threat-Intelligence und Threat-Modeling zur effektiven Risikominderung verbinden Sicherheitsinitiativen zu einer effektiven Pipeline.

Sicherheitsprüfungen.

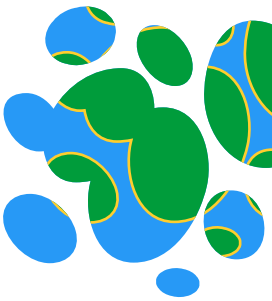
In enger Zusammenarbeit prüfen unsere Teams Adobe-Produkte und -Services auf mögliche sicherheitsrelevante Probleme hin, bewerten Risiken im Zusammenhang entdeckter Probleme und entscheiden, ob Risiken gemindert oder akzeptiert werden können. Unser Prüfprozess umfasst folgende Aktivitäten:

- **Threat-Modeling:** Threat-Modeling in der Design-Phase trägt zur frühzeitigen Ermittlung von Sicherheitslücken bei und schafft eine solide Grundlage für die Sicherheit von Adobe-Produkten und -Services. Durch Threat-Modeling ermitteln wir, in welchen Bereichen möglicherweise Änderungen an der Architektur erforderlich sind, um bekannte Bedrohungen zu verhindern. Automatisierung trägt beim Threat-Modeling zur effektiven Skalierung bei. Sicherheitsanforderungen werden automatisch erstellt und erhöhen so die Effizienz unseres Prüfprozesses.
- **Gezielte Code-Prüfungen:** Bei bestimmten Code-Abschnitten, die vertrauliche Daten betreffen, sowie bei von mehreren Services verwendeten Komponenten führen unsere Teams für Sicherheitsforschung manuelle Code-Prüfungen durch, um sicherzugehen, dass der Code den Best Practices für Sicherheit entspricht.
- **Schwerpunkttests:** Sicherheitsforschende bei Adobe testen unsere Produkte und Services regelmäßig nach verschiedenen Kriterien, z. B. bekannten Angriffsmustern oder -motiven.

Sicherheitstests.

Neben regelmäßigen Sicherheitsprüfungen stärken wir mit Penetrationstests an unseren Produkten und Services Bereiche mit bekannten Schwachstellen. Außerdem laden wir die User-Community dazu ein, Probleme oder Schwachstellen im Rahmen von Bug-Bounty-Programmen zu melden. Unsere Sicherheitstests umfassen u. a. folgende Aktivitäten:

- **Interne Penetrationstests:** Interne Sicherheits-Teams führen Code-gestützte Penetrationstests mit einer Kombination aus automatisierten und manuellen Techniken durch, die auf Bereiche abzielen, in denen bei Sicherheitsprüfungen Schwachstellen erkannt wurden.
- **Externe Penetrationstests:** Wir beauftragen führende Sicherheitsunternehmen mit der Durchführung von Penetrationstests, um potenzielle Sicherheitslücken aufzudecken und die Sicherheit von Adobe-Produkten und -Services insgesamt zu verbessern. Nach Erhalt eines Reports von einem Sicherheitsunternehmen dokumentiert Adobe die genannten Sicherheitslücken, bewertet deren Schweregrad und Priorität und entwirft eine Strategie zur Risikominimierung oder einen Plan zur Problembehebung. Nach Behebung des Problems wiederholen wir die Penetrationstests, um uns zu vergewissern, dass die Maßnahmen erfolgreich waren.
- **Bug-Bounty-Programme:** Adobe unterhält interne und externe Bug-Bounty-Programme, bei denen Personen, die Software-Fehler entdecken und melden, als Belohnung öffentliche Anerkennung oder Geldprämien erhalten. Mit unseren internen Bug-Bounty-Programmen schöpfen wir aus dem Know-how unserer Sicherheitsfachkräfte und schärfen das Sicherheitsbewusstsein unserer Entwicklungs-Teams. Zusätzlich ruft Adobe externe Sicherheitsforschende dazu auf, Schwachstellen, die sich auf Adobe oder Userinnen und User auswirken können, verantwortungsvoll offenzulegen. Als Anreiz werden Geldprämien für gerechtfertigte Meldungen ausgegeben.



Ticket-System und Dashboards.

Ein automatisiertes Ticket-System benachrichtigt Produkt-Teams über bekannte, ausgenutzte oder ausnutzbare Sicherheitsschwachstellen, damit Probleme zügig behoben werden können. Tickets werden basierend auf Kompetenz, Erfahrung und Produkt-Know-how automatisch dem passenden Team zugewiesen. Mithilfe von Dashboards und Key Performance Indicators (KPIs) kann unser Team für Programmsicherheit messen, wie gut der Adobe Application Security Stack im Unternehmen implementiert wird und wie wirksam unsere automatisierten Sicherheitslösungen sind.

Fazit.

Der Adobe Application Security Stack unterstützt die Produkt- und Serviceteams von Adobe, nativ sichere Programme zu entwickeln. Durch die frühe Einbindung von Sicherheits-kontrollen in den Entwicklungszyklus trägt das Team für Programmsicherheit proaktiv zur Vermeidung von Sicherheitsrisiken und zur durchgängigen Sicherheit von Adobe-Produkten und -Services bei. Zusätzlich setzen wir Automatisierung ein und überwachen die Sicherheit kontinuierlich mit Reports, Dashboards und vierteljährlichen Compliance-Prüfungen.

Adobe

11/22