# Beschreibung des IBM Cloud-Service

# IBM Security AppScan Mobile Analyzer

**Servicebeschreibung für die Bestellung des Kunden:**

## 1. Cloud-Service

Im Folgenden wird das Cloud-Service-Angebot beschrieben, das im Auftragsdokument des Kunden näher spezifiziert wird. Das Auftragsdokument besteht aus dem vorgelegten Angebot und dem Berechtigungsnachweis (Proof of Entitlement = PoE), mit dem IBM das Startdatum und die Laufzeit der Cloud-Services bestätigt. Die Rechnungsstellung beginnt nach der Bereitstellung des Cloud-Service.

### 1.1 IBM Security AppScan Mobile Analyzer

Dieser Service identifiziert Sicherheitsprobleme auf der Codeebene mobiler Android-Anwendungen. Mit diesem Service kann ein Entwickler nach Sicherheitslücken suchen, ohne dass der Anwendungsquellcode bereitgestellt werden muss. Bei Abschluss des Scans wird ein Sicherheitsbericht generiert, der Einzelheiten über erkannte Sicherheitslücken, die dadurch verursachten potenziellen Sicherheitsrisiken für die mobile Anwendung und Vorschläge zur Behebung der Sicherheitslücken enthält.

## 2. Sicherheitsbeschreibung

### 2.1 Sicherheitsrichtlinien

IBM verfügt über ein Team für Informationssicherheit und hat außerdem Datenschutz- und Sicherheitsrichtlinien festgelegt, die an die IBM Mitarbeiter kommuniziert werden. Mitarbeiter, die in IBM Rechenzentren Support leisten, sind verpflichtet, an Schulungen zu Datenschutz und Sicherheit teilzunehmen. Die IBM Sicherheitsrichtlinien und -standards werden jährlich überprüft und neu bewertet. Bei IBM internen Sicherheitsverstößen wird ein umfassendes Verfahren zur Behebung von Sicherheitsvorfällen in Gang gesetzt.

### 2.2 Zugriffskontrolle

Der Zugriff auf Kundendaten, sofern erforderlich, ist nur autorisierten IBM Support- und Servicemitarbeitern nach dem Grundsatz der Aufgabentrennung gestattet. Die IBM Mitarbeiter verwenden Zwei-Faktor-Authentifizierung für einen zwischengeschalteten „Gateway“-Management-Host. Beim Zugriff auf Kundendaten laufen alle Verbindungen über verschlüsselte Kanäle.

### 2.3 Service-Integrität und Verfügbarkeit

Änderungen an Betriebssystemen und Anwendungssoftware werden gemäß dem Change-Management-Prozess von IBM durchgeführt. Änderungen an Firewallregeln unterliegen ebenfalls dem Change-Management-Prozess und werden vor der Implementierung vom IBM Sicherheitsteam geprüft. Das Rechenzentrum wird von IBM rund um die Uhr (24x7) überwacht. Autorisierte Administratoren und externe Anbieter führen regelmäßig Scans zur Ermittlung interner und externer Schwachstellen durch, um potenzielle Systemsicherheitsrisiken aufzudecken und zu beheben. In allen IBM Rechenzentren sind Malware-Erkennungssysteme (Virenschutz, Erkennung unbefugter Zugriffe, Schwachstellensuche und Abwehr unbefugter Zugriffe) installiert. Die Services der IBM Rechenzentren unterstützen eine Vielzahl von Protokollen für die Übertragung von Daten über öffentliche Netze. Beispiele dafür sind HTTPS/SFTP/FTPS/S/MIME und Site-to-Site-VPN. Sicherungsdaten, die zur Auslagerung an einen anderen Standort vorgesehen sind, werden vor dem Transport verschlüsselt.

### 2.4 Aktivitätsprotokollierung

IBM protokolliert alle Aktivitäten für Systeme, Anwendungen, Datenrepositorys, Middleware und Netzinfrastrukturgeräte, die sich zur Protokollierung eignen und entsprechend konfiguriert sind. Um Manipulationsmöglichkeiten zu minimieren sowie zentrale Analyse, Alerting und Berichterstellung zu ermöglichen, wird die Aktivitätsprotokollierung in Echtzeit durchgeführt und die Protokolle werden in zentralen Protokollrepositorys abgelegt. Zur Vermeidung von Manipulationen werden die Daten signiert. Die Protokolle werden in Echtzeit und mithilfe periodischer Analyseberichte analysiert, um Unregelmäßigkeiten aufzudecken. Die Systembediener werden bei Unregelmäßigkeiten benachrichtigt und wenden sich bei Bedarf an einen rund um die Uhr im Einsatz befindlichen Sicherheitsspezialisten.

### 2.5 Physische Sicherheit

Die IBM Standards für physische Sicherheit sind dazu ausgelegt, den unbefugten Zutritt zu IBM Rechenzentren zu verhindern. Die Rechenzentren verfügen nur über eine begrenzte Anzahl von Eingängen, die durch Zwei-Faktor-Authentifizierung kontrolliert und mit Kameras überwacht werden. Der Zutritt ist nur autorisierten Mitarbeitern gestattet, die über eine Zutrittsgenehmigung verfügen. Das Betriebspersonal überprüft die Zutrittsgenehmigungen und stellt Ausweise aus, die den Zutritt ermöglichen. Mitarbeiter, für die Ausweise ausgestellt werden, müssen alle anderen Zutrittsausweise abgeben und dürfen für die Dauer ihrer Tätigkeit nur im Besitz des Ausweises für den Zutritt zum Rechenzentrum sein. Die Nutzung der Ausweise wird protokolliert. Externe Besucher werden beim Betreten der Rechenzentren registriert und während ihres Aufenthalts dort begleitet. Anlieferungsbereiche und Ladedocks sowie andere Eingänge, über die unbefugte Personen in die Rechenzentren gelangen können, werden kontrolliert und isoliert.

### 2.6 Compliance

IBM zertifiziert jährlich ihre Datenschutzverfahren auf Übereinstimmung mit den Safe-Harbor-Grundsätzen des United States Department of Commerce in Bezug auf Benachrichtigung, Wahlmöglichkeit, Weitergabe (Übermittlung an Dritte), Zugriff und Richtigkeit, Sicherheit, Durchsetzung und Überwachung. In den IBM Produktionsrechenzentren werden jährlich Prüfungen nach dem Branchenstandard SSAE 16 oder einem vergleichbaren Standard durchgeführt. IBM überprüft die IBM Geschäftstätigkeit auf Einhaltung aller sicherheits- und datenschutzrelevanten Anforderungen. Von IBM werden regelmäßig Prüfungen und Audits durchgeführt, um die Einhaltung der IBM Richtlinien zur Informationssicherheit zu gewährleisten. Sowohl die IBM Mitarbeiter als auch die externen Mitarbeiter nehmen einmal pro Jahr an Sicherheitsschulungen und Sensibilisierungstrainings teil. Die Mitarbeiter werden jährlich an ihre Zielvorgaben erinnert und auf ihre Verantwortung zur Einhaltung der Unternehmensethik, der Vertraulichkeit und der IBM Sicherheitsverpflichtungen hingewiesen.

## 3. Informationen zu Berechtigungen und Abrechnung

### 3.1 Gebührenmetriken

Der Cloud-Service wird unter der folgenden Gebührenmetrik entsprechend der Angabe im Auftragsdokument zur Verfügung gestellt:

- „Anwendungsinstanz“ ist eine Maßeinheit für den Erwerb von IBM SaaS. Für jede Instanz einer Anwendung, die mit IBM SaaS verbunden wird, muss eine Berechtigung erworben werden. Besteht eine Anwendung aus mehreren Komponenten, die jeweils einem bestimmten Zweck und/oder einer bestimmten Benutzerschaft dienen und mit IBM SaaS verbunden oder von IBM SaaS verwaltet werden können, dann wird jede dieser Komponenten als separate Anwendung betrachtet. Ferner werden Test-, Entwicklungs-, Staging- und Produktionsumgebungen für eine Anwendung als separate Instanzen der Anwendung betrachtet, die jeweils eine Berechtigung benötigen. Mehrere Anwendungsinstanzen in einer einzelnen Umgebung werden als separate Instanzen der Anwendung betrachtet, die jeweils eine Berechtigung benötigen. Der Kunde muss ausreichende Berechtigungen erwerben, um die Anzahl der Anwendungsinstanzen abzudecken, die während des Abrechnungszeitraums, der im Berechtigungsnachweis (PoE) oder Auftragsdokument angegeben ist, mit IBM SaaS verbunden werden.

### 3.2 Gebühren und Abrechnung

Der für den Cloud-Service zu zahlende Betrag ist im Auftragsdokument angegeben.

### 3.3 Nutzungsabhängige Gebühren (Pay as you Go)

'Pay as you Go'-Optionen werden in dem Monat nach der Inanspruchnahme des Service zu dem im Auftragsdokument angegebenen Gebührensatz in Rechnung gestellt.

## 4. Technische Unterstützung

Während der Subscription-Laufzeit wird technische Unterstützung für den Cloud-Service erbracht.

**Unterstützungszeiten:**

Informationen über die Zeiten der Erreichbarkeit, Onlinesysteme für die Problemmeldung und andere Übertragungswege und Prozesse der technischen Unterstützung werden im IBM Software as a Service Support Handbook beschrieben.

**Unterstützung außerhalb der regulären Geschäftszeiten:**

Unterstützung an Arbeitstagen, Wochenenden und Feiertagen außerhalb der regulären Geschäftszeiten (siehe oben) ist nur für Probleme der Fehlerklasse 1 verfügbar. Bei Problemen der Fehlerklasse 1 wird davon ausgegangen, dass der Kunde zur Unterstützung bei der Problemdiagnose rund um die Uhr (24x7) erreichbar ist, andernfalls werden die Probleme auf Fehlerklasse 2 heruntergestuft.

### 4.1 Supportforum

Alle Kunden erhalten Unterstützung über ein Supportforum, das regelmäßig von IBM Supportmitarbeitern und Entwicklern überwacht wird.

a. Fragen können über die folgende Adresse gestellt werden:
https://developer.ibm.com/answers/questions/ask/?topics=appscan-mobile-analyzer

b. Aktuelle Beiträge können über die folgende Adresse eingesehen werden:
https://developer.ibm.com/answers/topics/appscan-mobile-analyzer/

### 4.2 Standardunterstützung

Standardunterstützung wird in dem Zeitraum erbracht, in dem beim Kunden 'Pay as you Go'-Gebühren anfallen. Die Kunden können Support-Tickets direkt im Cloud-Service einstellen oder eine Chatsitzung öffnen, um Unterstützung zu erhalten. Weitere Informationen über Supportverfahren sind im IBM Support-Webportal unter https://support.ibmcloud.com oder im IBM SaaS Software Support Handbook unter http://www.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf zu finden.

| Fehlerklasse | Definition der Fehlerklasse | Angestrebte Reaktionszeiten | Deckungszeiten |
|---|---|---|---|
| 1 | **Kritische Auswirkung auf den Geschäftsbetrieb/Serviceausfall:** Geschäftskritische Funktionen sind nicht funktionsfähig oder eine kritische Schnittstelle ist ausgefallen. Dies betrifft normalerweise eine Produktionsumgebung und weist darauf hin, dass der Zugriff auf die Services nicht möglich ist, mit kritischen Auswirkungen auf betriebliche Abläufe. In diesem Fall ist eine sofortige Lösung erforderlich. | Innerhalb von 1 Stunde | 24x7 |
| 2 | **Erhebliche Auswirkung auf den Geschäftsbetrieb:** Die Nutzung eines geschäftsrelevanten Service-Features oder einer Servicefunktion ist stark eingeschränkt, oder es besteht die Gefahr, dass der Kunde Abgabefristen nicht einhalten kann. | Innerhalb von 2 Stunden während der Geschäftszeiten | Mo-Fr zu den Geschäftszeiten |
| 3 | **Geringe Auswirkung auf den Geschäftsbetrieb:** Der Service oder die Funktionalität kann genutzt werden und das Problem hat keine kritische Auswirkung auf betriebliche Abläufe. | Innerhalb von 4 Stunden während der Geschäftszeiten | Mo-Fr zu den Geschäftszeiten |
| 4 | **Minimale Auswirkung auf den Geschäftsbetrieb:** Eine Anfrage oder eine Frage nicht technischer Art. | Innerhalb 1 Arbeitstages | Mo-Fr zu den Geschäftszeiten |

## 5. Einhaltung des Safe-Harbor-Abkommens

IBM hat nicht geprüft, ob durch diesen Cloud-Service die Einhaltung des Safe-Harbor-Abkommens zwischen den USA und der EU bzw. den USA und der Schweiz gewährleistet ist.

## 6. Zusätzliche Informationen

Der Cloud-Service ist für die Erkennung einer Vielzahl potenzieller Sicherheits- und Compliance-Probleme in mobilen Anwendungen und mobilen Web-Services ausgelegt. Es werden weder alle Sicherheitslücken oder Compliance-Risiken überprüft noch fungiert der Service als Schutz vor Sicherheitsattacken. Da sich Sicherheitsbedrohungen, Regelungen und Standards ständig ändern, kann der Service nicht alle Änderungen berücksichtigen. Die Sicherheit und Compliance der mobilen Anwendung des Kunden, seiner Systeme und Mitarbeiter sowie alle Abhilfemaßnahmen liegen in der

alleinigen Verantwortung des Kunden. Der Kunde entscheidet alleine über die Nutzung der vom Service bereitgestellten Informationen.

## 6.1 Bevorzugte Standorte

Soweit möglich, basieren die Steuern auf dem Standort, den der Kunde als bevorzugten Standort für die Cloud-Services angibt. IBM weist die Steuern gemäß der Geschäftsadresse aus, die bei der Bestellung des Cloud-Service als primärer Standort angegeben wird, es sei denn, der Kunde stellt IBM zusätzliche Informationen bereit. Der Kunde ist dafür verantwortlich, diese Informationen auf dem aktuellen Stand zu halten und IBM über Änderungen zu informieren.

## 6.2 Cookies

Der Kunde ist sich dessen bewusst und stimmt zu, dass IBM während des normalen Betriebs und im Rahmen des Supports für den Cloud-Service über Tracking und andere Technologien personenbezogene Daten des Kunden (sowie seiner Mitarbeiter und Auftragnehmer) erfassen kann, die mit der Nutzung des Cloud-Service im Zusammenhang stehen. Auf diese Weise kann IBM Nutzungsstatistiken und -informationen über die Effektivität des Cloud-Service erfassen, die dazu beitragen sollen, das Benutzererlebnis zu verbessern und/oder die Interaktionen mit dem Kunden anzupassen. Der Kunde bestätigt, dass er die Zustimmung der betroffenen Personen einholt oder eingeholt hat, damit IBM die erhobenen personenbezogenen Daten für die vorstehenden Zwecke innerhalb von IBM, durch andere IBM Unternehmen und deren Unterauftragnehmer in allen Ländern, in denen sie geschäftlich tätig sind, in Übereinstimmung mit der geltenden Gesetzgebung verarbeiten darf. IBM wird den Anforderungen der Mitarbeiter und Auftragnehmer des Kunden nachkommen, die sich auf den Zugriff, die Aktualisierung, die Korrektur oder die Löschung ihrer personenbezogenen Daten beziehen.