IBM Nutzungsbedingungen – SaaS-spezifische Angebotsbedingungen

IBM Application Security on Cloud

Die Nutzungsbedingungen bestehen aus diesen IBM Nutzungsbedingungen – SaaS-spezifische Angebotsbedingungen (nachfolgend „SaaS-spezifische Angebotsbedingungen“ genannt) und einem Dokument mit dem Titel IBM Nutzungsbedingungen – Allgemeine Bedingungen (nachfolgend „Allgemeine Bedingungen“ genannt), das unter der folgende Adresse zu finden ist: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Im Falle eines Widerspruchs haben die SaaS-spezifischen Angebotsbedingungen Vorrang vor den Allgemeinen Bedingungen. Durch die Bestellung von IBM SaaS, den Zugriff darauf oder die Nutzung von IBM SaaS erklärt der Kunde sein Einverständnis mit diesen Nutzungsbedingungen.

Die Nutzungsbedingungen unterliegen dem IBM International Passport Advantage Vertrag, dem IBM International Passport Advantage Express Vertrag oder dem IBM Internationalen Vertrag über ausgewählte IBM SaaS-Angebote (nachfolgend „Vertrag“ genannt) und bilden zusammen mit dem jeweils anwendbaren Vertrag die vollständige Vereinbarung.

1. IBM SaaS

Diese SaaS-spezifischen Angebotsbedingungen gelten für das folgende IBM SaaS-Angebot:

- IBM Application Security Analyzer

2. Gebührenmetriken

Das IBM SaaS-Angebot wird unter den folgenden Gebührenmetriken entsprechend der Angabe im Auftragsdokument verkauft:

a. **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 Benutzerbasis dienen und mit IBM SaaS verbunden oder von IBM SaaS verwaltet werden können, dann wird jede Komponente als separate Anwendung betrachtet. Test-, Entwicklungs-, Staging- und Produktionsumgebungen für eine Anwendung werden ebenfalls 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 (Proof of Entitlement = PoE) oder Auftragsdokument angegeben ist, mit IBM SaaS verbunden werden.

b. **Zugriff** ist eine Maßeinheit für den Erwerb von IBM SaaS. Unter „Zugriff“ versteht man die Rechte zur Nutzung von IBM SaaS. Der Kunde muss eine einzige Zugriffsberechtigung erwerben, um IBM SaaS während des Abrechnungszeitraums nutzen zu können, der im Berechtigungsnachweis (PoE) oder Auftragsdokument angegeben ist.

3. Gebühren und Abrechnung

Der für IBM SaaS zu bezahlende Betrag ist im Auftragsdokument angegeben.

3.1 Nutzungsabhängige Gebühren

Optionen mit nutzungsabhängigen Gebühren (Pay per Use) werden in dem Monat nach der Inanspruchnahme des Service zu dem im Auftragsdokument angegebenen Verrechnungssatz in Rechnung gestellt.

3.2 Anteilige Monatsgebühr

Die im Auftragsdokument angegebene anteilige Monatsgebühr wird anteilig basierend auf der Nutzung ermittelt.

4. Technische Unterstützung

Während der Subscription-Laufzeit und nachdem IBM dem Kunden mitgeteilt hat, dass sein Zugriff auf IBM SaaS freigeschaltet ist, wird technische Unterstützung über Onlineforen und als Standardunterstützung während des Zeitraums erbracht, in dem beim Kunden nutzungsabhängige Gebühren anfallen. Die Kunden können Support-Tickets direkt in IBM SaaS einstellen oder eine Chatsitzung öffnen, um Unterstützung zu erhalten. IBM stellt das IBM Software as a Service Support Handbook zur Verfügung, das Kontaktinformationen für die technische Unterstützung sowie weitere Informationen und Prozesse enthält.

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

4.1 Zugriff auf Kundendaten

IBM kann zur Diagnose von Problemen mit dem Service und um das Scannen von Kundenanwendungen mithilfe des Service zu vereinfachen, auf Kundendaten zugreifen. Der Datenzugriff erfolgt ausschließlich zum Zwecke der Fehlerbehebung oder zur Unterstützung von IBM Produkten oder Services.

5. Zusätzliche Bedingungen für das IBM SaaS-Angebot

Durch Sicherheitsscans werden unter Umständen nicht alle Sicherheitsrisiken in einer Anwendung aufgedeckt.

IBM SaaS kann verwendet werden, um den Kunden bei der Einhaltung seiner Compliance-Verpflichtungen zu unterstützen, die auf Gesetzen, Verordnungen, Normen oder Verfahren beruhen können. Sämtliche Anweisungen, empfohlenen Vorgehensweisen oder Anleitungen, die vom Service bereitgestellt werden, stellen keine rechtliche, betriebswirtschaftliche oder anderweitige fachliche Beratung dar, und dem Kunden wird dringend geraten, sich von juristisch oder fachlich kompetenter Stelle beraten zu lassen. Der Kunde ist allein dafür verantwortlich, sicherzustellen, dass von ihm selbst und durch die von ihm ausgeübten Tätigkeiten sowie durch seine Anwendungen und Systeme alle anwendbaren Gesetze, Verordnungen, Normen oder Verfahren eingehalten werden. Durch die Verwendung des Service ist die Einhaltung von Gesetzen, Verordnungen, Normen oder Verfahren nicht garantiert.

IBM SaaS führt invasive und nicht invasive Tests für die Website, die Webanwendung oder die mobile Anwendung durch, die der Kunde für den Scanvorgang auswählt. Diese Tests bergen bestimmte Risiken, einschließlich der folgenden:

a. Auf den Computersystemen des Kunden kann es während der Ausführung der zu testenden Anwendungen zu Blockierungen oder Ausfällen kommen, die eine vorübergehende Nichtverfügbarkeit der Systeme oder Datenverluste zur Folge haben können.

b. Während der Tests können Leistung und Durchsatz der Kundensysteme als auch der zugeordneten Router und Firewalls vorübergehend beeinträchtigt sein.

c. Unter Umständen werden große Mengen an Protokollnachrichten generiert, wodurch übermäßig viel Plattenspeicherplatz durch Protokolldateien belegt wird.

d. Durch das Testen auf Sicherheitslücken könnten Daten verändert oder gelöscht werden.

e. Durch Intrusion Detection Systems (Warnsysteme gegen Angriffe von außen) könnten Alarmnachrichten ausgelöst werden.

f. Von der E-Mail-Funktion der getesteten Webanwendung könnten E-Mails ausgelöst werden.

und

g. Der Cloud-Service könnte den Datenverkehr des überwachten Netzes abfangen, um nach Ereignissen zu suchen.

Falls authentifizierte Anmeldedaten für die zu testende Anwendung im Service verwendet werden, sollten nur die Anmeldedaten von Testkonten und nicht von Produktionsbenutzern eingegeben werden. Die Verwendung der Anmeldedaten von Produktionsbenutzern kann zur Folge haben, dass personenbezogene Daten über den Service übertragen werden.

IBM SaaS kann für das Scannen von Webproduktionsanwendungen konfiguriert werden. Wenn vom Kunden der Scantyp „Produktion“ festgelegt wird, werden die Scans so ausgeführt, dass die oben aufgeführten Risiken reduziert werden. In bestimmten Situationen kann der Cloud-Service jedoch zu Leistungseinbußen oder Instabilität innerhalb der getesteten Produktionssites und Infrastruktur führen. IBM übernimmt keinerlei Gewährleistung oder Haftung in Bezug auf die Eignung des Cloud-Service für das Scannen von Produktionssites.

Es liegt in der Verantwortung des Kunden, zu entscheiden, ob der Service für seine Website, seine Webanwendung, seine mobile Anwendung oder seine technische Umgebung geeignet ist und den Sicherheitsanforderungen entspricht.

IBM SaaS ist für die Erkennung einer Vielzahl potenzieller Sicherheits- und Compliance-Probleme in mobilen Anwendungen, Webanwendungen und 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 Webanwendung 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.

Das unbefugte Eindringen oder Zugreifen auf Computersysteme ist durch bestimmte Gesetze verboten. Der Kunde ist dafür verantwortlich, sicherzustellen, dass mit dem Service nur seine eigenen Websites und/oder Anwendungen oder diejenigen Websites und/oder Anwendungen gescannt werden, für die er entsprechend berechtigt ist.

5.2 Cookies

Der Kunde ist sich dessen bewusst und stimmt zu, dass IBM während des normalen Betriebs und im Rahmen des Supports für IBM SaaS über Tracking und andere Technologien personenbezogene Daten des Kunden (sowie seiner Mitarbeiter und Auftragnehmer) erfassen kann, die mit der IBM SaaS-Nutzung im Zusammenhang stehen. Auf diese Weise kann IBM Nutzungsstatistiken und -informationen über die Effektivität von IBM SaaS zusammenstellen, 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 einholen wird 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 wir und unsere Unterauftragnehmer 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 erhobenen personenbezogenen Daten beziehen.

5.3 Bevorzugte Standorte

Soweit möglich, orientieren sich die Steuern an dem Standort/den Standorten, für den/die IBM SaaS erbracht wird. IBM weist die Steuern gemäß der Geschäftsadresse aus, die bei der Bestellung von IBM SaaS 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.

Anhang A

1. Allgemeine Beschreibung von IBM Application Security on Cloud

IBM Application Security on Cloud ermöglicht es dem Kunden, Sicherheitslücken (z. B. SQL-Injection, Cross-Site Scripting und Datenlecks) für eine Reihe von Anwendungen von einem einzigen Ort aus zu identifizieren. Der Service beinhaltet verschiedene Scanning-Verfahren für Anwendungssicherheit, die Sicherheitsprobleme in den Anwendungen aufdecken.

IBM Application Security on Cloud bietet folgende Funktionen:

- Scannen mobiler Anwendungen zur Ermittlung von Sicherheitslücken. Dabei kommen dynamische (Blackbox) und interaktive (Glass-Box) Sicherheitsanalyseverfahren zum Einsatz.
- Scannen von Produktions- und Vorproduktionswebsites zur Ermittlung von Sicherheitslücken. Dabei kommen dynamische (Blackbox) Sicherheitsanalyseverfahren zum Einsatz.
- Scannen der Datenflüsse innerhalb von Web- und Desktopanwendungen zur Ermittlung von Sicherheitslücken. Dabei kommen statische (Whitebox) Sicherheitsanalyseverfahren zum Einsatz.
- Ausführliche Berichte über Sicherheitslücken, die sowohl Gesamtübersichten der Ergebnisse als auch Korrekturmaßnahmen enthalten, die von den Entwicklern Schritt für Schritt durchgeführt werden können.
- Integration mit verschiedenen DevOps-Plattformen, wie beispielsweise Maven und IBM UrbanCode.