Beschreibung des IBM Cloud-Service

IBM Intelligent Operations Center on IBM SmartCloud

Servicebeschreibung für die Bestellung des Kunden:

1. Cloud-Service

Im Folgenden werden die Cloud-Service-Angebote, einschließlich des Basisangebots und der verfügbaren optionalen Features beschrieben, die zur Auswahl stehen. Das Auftragsdokument besteht aus dem speziellen Angebot und dem Berechtigungsnachweis (Proof of Entitlement = PoE), mit dem IBM das Startdatum sowie die Laufzeit der Cloud-Services und den Beginn der Abrechnung bestätigt.

1.1 IBM Intelligent Operations Center Standard User on IBM SmartCloud

Funktionen für Standardbenutzer:

- Intelligent Operations Center-Konsole (auch IOC-Konsole) – die Hauptschnittstelle, über die Ereignisse und der Ereignisstatus sowie Geodaten (dazu ist die Einbindung eines GIS-Service erforderlich, der nicht zum Lieferumfang des Cloud-Service gehört) und Berichte mit Langzeittrendanalysen, zur Optimierung der Ressourcenbereitstellung und mit den vom Benutzer gewählten Key Performance Indicators (KPIs) angezeigt werden können
- Ermöglichen den Benutzern das Anzeigen von Analyseergebnissen auf einem Plan, abhängig von Zeit und Ort der Ereignisse oder von anderen Daten, die von den IBM Cloud-Services verarbeitet werden
- Ermöglichen den Benutzern, Ereignisse basierend auf den vom IBM Cloud-Service verarbeiteten Daten darzustellen
- Ermöglichen den Benutzern das Anzeigen von Berichten über Ereignisse oder Daten, die an der IOC-Konsole erfasst wurden
- Vorlagen für Standard Operating Procedures, die von den Benutzern für Notfallmaßnahmen angepasst werden können
- Ermöglichen den Benutzern die Ausführung von Standard Operating Procedures, die das Automatisieren von Standardantworten auf ein Ereignis, einen KPI-Grenzwert oder eine in einem Bericht definierte Bedingung unterstützen
- Bieten Benutzern eine Gesamtansicht der Informationen für alle Ereignisse in einer Stadt

1.2 IBM Intelligent Operations Center Premium User on IBM SmartCloud

Premium-Benutzer haben Zugriff auf alle Funktionen von IBM Intelligent Operations Center Standard User on IBM SmartCloud, die oben aufgeführt sind, sowie auf die folgenden zusätzlichen Funktionen:

- Ermöglichen den Benutzern die Erstellung und Änderung von KPIs und Berichten
- Ermöglichen den Benutzern die Erstellung und Änderung von Standard Operating Procedures, einschließlich Vorlagen für Notfallmaßnahmen
- Ermöglichen den Benutzern die Verwaltung des IBM Cloud-Service über Verwaltungsschnittstellen
- Ermöglichen den Benutzern den Import von Daten aus dem kundeneigenen System oder aus Systemen Dritter über Integrations-APIs
- Ermöglichen den Benutzern das Konfigurieren von Analysefunktionen, die Korrelationen zwischen Ereignissen in der Stadt basierend auf Zeit und Ort erkennen
- Ermöglichen den Benutzern das Definieren und Verwalten von Schnittstellen sowie das Konfigurieren von Berichten im Citizen Collaboration Portal (siehe die Beschreibung des Citizen Collaboration Portals unten)
- Ermöglichen den Benutzern das Einreichen von Serviceanforderungen, um dem System neue Benutzer hinzuzufügen, Benutzerkonfigurationen zu ändern und neue Anzeigen zur Benutzerschnittstelle hinzuzufügen

1.3 IBM Intelligent Operations Center Consumer User on IBM SmartCloud

Private Anwender (Consumer Users) können das Citizen Collaboration Portal nutzen, bei dem es sich um eine spezielle Schnittstelle handelt, die externen öffentlichen Zugriff auf den IBM Cloud-Service durch private Anwender ermöglicht. Private Anwender können Serviceanforderungen einreichen, den Status ihrer

Anforderung anzeigen sowie Berichte über das Citizen Collaboration Portal einsehen. Private Anwender haben keinen Zugriff auf den Funktionsumfang, der einem IBM Intelligent Operations Center Standard User on IBM SmartCloud oder IBM Intelligent Operations Center Premium User on IBM SmartCloud zur Verfügung steht.

2. Sicherheitsbeschreibung

2.1 Sicherheitsrichtlinien

IBM verfügt über Datenschutz- und Sicherheitsrichtlinien, die veröffentlicht und an die IBM Mitarbeiter weitergegeben werden. IBM verlangt, dass Mitarbeiter, die in IBM Rechenzentren weltweit Support leisten, an Schulungen zu Datenschutz- und Sicherheitsmaßnahmen teilnehmen. Des Weiteren verfügt IBM über ein Sicherheitsteam, das sich ausschließlich mit Fragen der Informationssicherheit beschäftigt. Die IBM Sicherheitsrichtlinien und Standards werden jährlich überprüft und neu bewertet. Bei IBM internen Sicherheitsverstößen wird ein Verfahren zur Behebung von Sicherheitsvorfällen in Gang gesetzt.

2.2 Zugriffskontrolle

Der Zugriff auf Kundendaten ist nur autorisierten IBM Support-Mitarbeitern nach dem Grundsatz der Aufgabentrennung gestattet. Die Mitarbeiter des IBM Support-Teams verwenden Zwei-Faktor-Authentifizierung für einen zwischengeschalteten „Gateway"-Management-Host. Beim Zugriff auf Kundendaten laufen alle Verbindungen über verschlüsselte Kanäle. Sämtliche Zugriffe auf Kundendaten und alle Datenübertragungen in die oder aus der Hosting-Umgebung werden protokolliert. In IBM IOC-Rechenzentren kommt Wifi nicht zum Einsatz. Zugriffskontrollprotokolle werden regelmäßig geprüft. Bei Kündigungen oder Arbeitsplatzwechsel kommen spezielle Verfahren zum Einsatz, die eine Rückgabe von Assets und das Löschen von Zugriffsberechtigungen einschließen.

2.3 Service-Integrität und Verfügbarkeit

Änderungen an Betriebssystemressourcen 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 gesondert geprüft. Die Ressourcen in IBM Rechenzentren werden von IBM Mitarbeitern 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

Sofern technisch möglich, werden vom IBM Team die Aktivitäten für alle Systeme, Anwendungen, Datenrepositorys, Netzinfrastrukturgeräte und die Middleware in Protokollen aufgezeichnet. 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, wobei nach Unregelmäßigkeiten gesucht wird. 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 RZ-Ressourcen zu verhindern. IBM 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 Sicherheitspersonal 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. Physische Schutzmaßnahmen gegen Beschädigung durch Brände, Überflutungen, Erdbeben, Explosionen, innere Unruhen und andere natürliche oder von Menschen verursachte Katastrophen kommen ebenfalls zur Anwendung. Anlieferungsbereiche und Ladedocks sowie andere Eingänge, über die unbefugte Personen in die Rechenzentren gelangen können, werden kontrolliert und isoliert. An- und Abtransporte von Ausrüstungsgegenständen werden protokolliert.

2.6 Compliance

In den IBM Produktionsrechenzentren werden jährlich Prüfungen nach dem Branchenstandard SAS 70 Typ II, jetzt SSAE 16, oder einem vergleichbaren Standard durchgeführt. Das IBM Team prüft die IBM Geschäftstätigkeit auf Einhaltung aller sicherheits- und datenschutzrelevanten Anforderungen. Vom IBM Team werden regelmäßig Prüfungen und Audits durchgeführt, um die Einhaltung der IBM Richtlinien zur Informationssicherheit zu gewährleisten. Sowohl IBM Mitarbeiter als auch externe Mitarbeiter müssen einmal pro Jahr an Sicherheitsschulungen und Sensibilisierungstrainings teilnehmen. Die Mitarbeiter werden an ihre Zielvorgaben erinnert und auf ihre Verantwortung zur Einhaltung der Unternehmensethik, der Vertraulichkeit und der IBM Sicherheitsverpflichtungen hingewiesen.

3. Service-Level-Ziel

Die Service-Level-Ziele für diesen Cloud-Service sind:

- Verfügbarkeit von 99,5 % außerhalb der regulären, planmäßigen Wartungszeiten
- Maximale Reaktionszeit von fünf Sekunden bis zum Hinweis, dass eine Webseitenaktivität stattfindet

Die Angabe der Service-Level-Ziele sind Zielvorgaben und können gegenüber dem Kunden nicht garantiert werden. Für den Fall, dass IBM die Service-Level-Ziele nicht einhält, erhält der Kunde keine Rückerstattung, Gutschrift oder sonstige Ersatzleistungen.

4. Informationen zu Berechtigungen und Abrechnung

4.1 Gebührenmetriken

Die IBM Cloud-Services werden unter den folgenden Gebührenmetriken entsprechend der Angabe im Auftragsdokument verkauft:

a. „Gleichzeitig angemeldeter Benutzer“ ist eine Maßeinheit für den Erwerb des Cloud-Service. Ein gleichzeitig angemeldeter Benutzer ist eine Person, die zu einem beliebigen Zeitpunkt auf den Cloud-Service zugreift. Ungeachtet dessen, ob die Person mehrmals zur gleichen Zeit auf den Cloud-Service zugreift, zählt sie nur als ein einziger gleichzeitig angemeldeter Benutzer. Der Kunde muss Berechtigungen für die maximale Anzahl der gleichzeitig angemeldeten Benutzer erwerben, die simultan auf beliebige Weise direkt oder indirekt (z. B. über ein Multiplexing-Programm, eine Einheit oder einen Anwendungsserver) während des Abrechnungszeitraums, der im PoE-Teil des Auftragsdokuments angegeben ist, auf den Cloud-Service zugreifen.

4.2 Gebühren und Abrechnung

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

4.3 Anteilige Monatsgebühren

Die anteilige Monatsgebühr ist eine auf Basis des Tagessatzes ermittelte anteilige Gebühr. Die anteiligen Monatsgebühren werden, basierend auf der Anzahl der restlichen Tage in dem betreffenden Monat, ab dem Datum berechnet, an dem der Kunde von IBM darüber benachrichtigt wird, dass sein Zugriff auf das Cloud-Service-Angebot freigeschaltet ist.

5. Laufzeit und Verlängerungsoptionen

5.1 Laufzeit

Die Laufzeit des Cloud-Service beginnt an dem Datum, an dem IBM dem Kunden mitteilt, dass sein Zugriff auf den Cloud-Service gemäß der Beschreibung im Auftragsdokument freigeschaltet ist. Die Laufzeit und die Abrechnung beginnen erst, nachdem das Angebot vollständig bereitgestellt wurde. Das heißt, alle Daten müssen geladen und die Konfiguration muss abgeschlossen sein, bevor die Endbenutzer auf den Cloud-Service zugreifen. Das genaue Start- und Enddatum der Laufzeit ist im PoE-Teil des Auftragsdokuments angegeben. Der Kunde hat die Möglichkeit, den Nutzungsumfang des Cloud-Service während der Laufzeit durch eine entsprechende Mitteilung an IBM oder den zuständigen IBM Business Partner zu erhöhen. Die Erhöhung des Nutzungsumfangs wird von IBM in das Auftragsdokument aufgenommen.

5.2 Verlängerungsoptionen für die Laufzeit der Cloud-Services

Im Auftragsdokument des Kunden ist durch folgende Optionen geregelt, ob sich der Cloud-Service am Ende der Laufzeit verlängert:

5.2.1 Automatische Verlängerung

Ist im Auftragsdokument des Kunden angegeben, das sich die Laufzeit automatisch verlängert, kann der ablaufende Cloud-Service gekündigt werden, indem der Kunde IBM durch schriftliche Mitteilung mindestens neunzig (90) Tage vor dem im Auftragsdokument genannten Ablaufdatum davon in Kenntnis setzt. Wenn IBM oder der zuständige IBM Business Partner kein solches Kündigungsschreiben vor dem Ablaufdatum

erhält, wird die ablaufende Laufzeit automatisch entweder um ein (1) Jahr oder um die im Berechtigungsnachweis genannte ursprüngliche Laufzeit verlängert.

5.2.2 Fortlaufende Abrechnung

Wird gemäß dem Auftragsdokument des Kunden eine fortlaufende Abrechnung erstellt, bedeutet dies, dass der Kunde auch nach Ablauf der Laufzeit kontinuierlichen Zugriff auf den Cloud-Service hat und der Cloud-Service fortlaufend in Rechnung gestellt wird. Um die Nutzung des Cloud-Service und den fortlaufenden Abrechnungsprozess zu beenden, muss der Kunde in einer schriftlichen Mitteilung an IBM oder den zuständigen IBM Business Partner unter Einhaltung einer Frist von neunzig (90) Tagen die Einstellung des Cloud-Service beantragen. Bei Einstellung des Zugriffs werden dem Kunden evtl. ausstehende Zugriffsgebühren für den Monat berechnet, in dem die Beendigung wirksam wurde.

5.2.3 Verlängerung erforderlich

Ist im Auftragsdokument eine befristete Laufzeit angegeben, wird der Cloud-Service zum Laufzeitende abgeschaltet und der Zugriff des Kunden auf den Cloud-Service entfernt. Um den Cloud-Service über das Enddatum hinaus nutzen zu können, muss der Kunde eine neue Subscription-Laufzeit erwerben, indem er beim zuständigen IBM Vertriebsbeauftragten oder IBM Business Partner eine entsprechende Bestellung aufgibt.

6. Technische Unterstützung

Während der Laufzeit des Cloud-Service wird technische Unterstützung für den Cloud-Service und die Aktivierungssoftware erbracht. Die technische Unterstützung ist Bestandteil des Cloud-Service und nicht als separates Angebot erhältlich. Während des Zeitraums, in dem technische Unterstützung erbracht wird:

a. leistet IBM Unterstützung bei allgemeinen Fragen zur Verwendung und untersucht Vorfälle, die mit der Funktionalität des Codes in Zusammenhang stehen.

b. bietet IBM die Möglichkeit zur elektronischen Problemmeldung und Unterstützung über ein webbasiertes Unterstützungsportal während der üblichen Geschäftszeiten (veröffentlichte Hauptgeschäftszeiten) des für den Kunden zuständigen IBM Support Centers. (Diese Unterstützungsleistung wird nicht für Endbenutzer erbracht.) Unterstützung für Fehlerklasse 1 steht an 365 Tagen im Jahr rund um die Uhr zur Verfügung.

c. kann IBM Remotezugriff auf das System des Kunden anfordern, um Unterstützung bei der Eingrenzung der Problemursache zu leisten. Der Kunde bleibt für den angemessenen Schutz seines Systems und aller darin enthaltenen Daten verantwortlich, wenn IBM mit seiner Zustimmung darauf zugreift.

Technische Unterstützung wird nicht erbracht für 1) das Design und die Entwicklung von Anwendungen, 2) die Nutzung des Cloud-Service außerhalb der spezifizierten Betriebsumgebung oder 3) bei Fehlern, die von Produkten und Services verursacht werden, für die IBM im Rahmen dieser Servicebeschreibung nicht verantwortlich ist.

7. Aktivierungssoftware

Dieses Cloud-Service-Angebot kann Aktivierungssoftware enthalten. Die Aktivierungssoftware darf nur in Verbindung mit dem Cloud-Service während der Laufzeit des Cloud-Service gemäß der Beschreibung in der Dokumentation verwendet werden. Falls die Aktivierungssoftware Beispielcode enthält, hat der Kunde außerdem das Recht, abgeleitete Werke des Beispielcodes zu erstellen und in Übereinstimmung mit den hierunter gewährten Berechtigungen zu nutzen. Die Aktivierungssoftware wird auf Basis der Service-Level-Verpflichtung (sofern vorhanden) als Komponente des Cloud-Service bereitgestellt, aber ohne Wartung (auf „as-is“-Basis).

8. Einhaltung des Safe-Harbor-Abkommens

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

9. Zusätzliche Informationen

9.1 Datenerfassung

Der Kunde ist sich dessen bewusst und stimmt zu, dass IBM während des normalen Betriebs und im Rahmen des Supports für die Cloud-Services über Tracking und andere Technologien personenbezogene Daten des Kunden (sowie seiner Mitarbeiter und Auftragnehmer) erfassen kann, die mit der Nutzung der Cloud-Services im Zusammenhang stehen. Auf diese Weise kann IBM statistische Daten und Informationen über die Effektivität der Cloud-Services erfassen, um die Attraktivität für den Benutzer zu verbessern bzw. die Interaktionen mit dem Kunden optimal an die jeweiligen Bedürfnisse 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.

9.2 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.