Leistungsbeschreibung

IBM Infrastructure Security Services – Firewall Management – Premium

Zusätzlich zu den nachstehend aufgeführten Bedingungen enthält diese Leistungsbeschreibung die „Allgemeinen Bedingungen für IBM Managed Security Services“ (nachfolgend „Allgemeine Bedingungen“ genannt), die durch Bezugnahme Bestandteil dieser Leistungsbeschreibung werden.

1. Beschreibung der Leistung – Leistungsmerkmale

Gegenstand der Leistung der IBM Infrastructure Security Services – Firewall Management – Premium (nachfolgend „Firewall Management – Premium” oder „Services“ genannt) ist die Überwachung und Unterstützung von Netzwerk-Firewalls (nachfolgend „Agenten” oder „Managed Agents“ genannt) auf einer Vielzahl verschiedener Plattformen und Technologien. Diese Agenten dürfen nicht zu anderen Zwecken eingesetzt werden, während sie im Rahmen dieser Services von IBM betrieben werden.

Die hierin beschriebenen Merkmale der Services sind von der Verfügbarkeit und Unterstützbarkeit der genutzten Produkte und Produktmerkmale abhängig. Auch bei unterstützten Produkten werden möglicherweise nicht alle Produktmerkmale unterstützt. Informationen zu unterstützten Merkmalen sind auf Anfrage von IBM erhältlich. Zu den Produkten gehören sowohl von IBM als auch nicht von IBM bereitgestellte Hardware, Software und Firmware.

2. Begriffserklärungen

Alert Condition (AlertCon) ist eine von IBM entwickelte globale Risikomessgröße, die proprietäre Methoden nutzt. Die AlertCon-Alarmstufe (nachfolgend „AlertCon-Level“ genannt) basiert auf einer Vielzahl verschiedener Faktoren, darunter der Anzahl und dem Schweregrad bekannter Schwachstellen, Exploits, die diese Schwachstellen ausnutzen, der allgemeinen Verfügbarkeit solcher Exploits, der Aktivität sich massenhaft verbreitender Würmer und der Aktivität globaler Sicherheitsbedrohungen. Die vier AlertCon-Levels sind im IBM MSS-Kundenportal (IBM Managed Security Services) (nachfolgend „Portal“ genannt) beschrieben.

Schulungsmaterial beinhaltet u. a. Handbücher, Anweisungen für Schulungsleiter, Literatur, Methodiken, Bilder, Richtlinien und Verfahren zu elektronischen Kursen und Fallstudien sowie weitere schulungsbezogene Komponenten, die von oder für IBM erstellt wurden. Soweit zutreffend, beinhaltet das Schulungsmaterial auch Handbücher für die Schulungsteilnehmer, Übungsdokumente, Handbücher und Präsentationen, die von IBM bereitgestellt werden.

Firewall ist ein Gerät für die Netzwerksicherheit, das dafür konzipiert ist, unbefugten Zugriff zu verhindern und berechtigte Datenübertragungen zuzulassen, basierend auf einer Konfiguration von Regeln für das Zulassen, Ablehnen, Verschlüsseln, Entschlüsseln oder Weiterleiten von Daten in Übereinstimmung mit der Sicherheitsrichtlinie des Serviceempfängers.

Virtual Private Networks (VPNs) nutzen öffentliche Telekommunikationsnetze für die verschlüsselte Übertragung privater Daten. Die meisten VPN-Implementierungen verwenden das Internet als öffentliche Infrastruktur und eine Vielzahl verschiedener spezialisierter Protokolle zur Unterstützung der Übertragung privater Daten.

Webfilter unterstützen den Serviceempfänger dabei, anstößige Inhalte zu blockieren, Gefahren aus dem Internet zu entschärfen und das Webnutzungsverhalten von Mitarbeitern hinter dem von IBM betriebenen Agenten (nachfolgend „Managed Agent“ genannt) zu steuern.

3. Leistungen

Die folgende Tabelle hebt die messbaren Merkmale der Services hervor. Die an die Tabelle anschließenden Abschnitte beschreiben jedes Merkmal der Services in Textform.

Zusammenfassung der Servicemerkmale

Servicemerkmal	Messgröße oder Anzahl	Angestrebte Service-Levels
Verfügbarkeit der Services	100 %	SL für die Verfügbarkeit der Services
Verfügbarkeit des IBM MSS-Portals	99,9 %	SL für die Verfügbarkeit des IBM MSS-Portals

Servicemerkmal	Messgröße oder Anzahl	Service-Level-Agreements
Autorisierte Ansprechpartner für die Sicherheit	3 Benutzer	nicht zutreffend

Archivierung von Protokollen/Ereignissen	bis zu 7 Jahre (1 Jahr Standard)	nicht zutreffend
Alarmbenachrichtigung bei Sicherheitsverstößen	60 Minuten	SLA für die Alarmbenachrichtigung bei Sicherheitsverstößen
Anforderung einer Richtlinienänderung	Unbegrenzte Anzahl	nicht zutreffend
Bestätigung der Anforderung einer Richtlinienänderung	2 Stunden	SLA für die Bestätigung der Anforderung einer Richtlinienänderung
Implementierung einer angeforderten Richtlinienänderung	8 Stunden	SLA für die Implementierung einer angeforderten Richtlinienänderung
Anforderung einer Richtlinienänderung im Notfall	1 pro Monat	nicht zutreffend
Implementierung einer angeforderten Richtlinienänderung im Notfall	2 Stunden	SLA für die Implementierung einer angeforderten Richtlinienänderung im Notfall
Alarmausgabe zum Status von Agenten	15 Minuten	SLA für die Systemüberwachung

3.1 Security Operations Centers

IBM Managed Security Services (MSS) werden von einem Netz aus IBM Security Operations Centers (SOCs) aus erbracht, die während 24 Stunden pro Tag an 7 Tagen die Woche für den Kunden erreichbar sind.

3.2 Portal

Über das Portal erhält der Kunde Zugriff auf eine Umgebung (und zugehörige Tools) für die Überwachung und das Management seines Sicherheitsstatus. Das Portal vereint Technologie- und Servicedaten von mehreren Anbietern und aus mehreren Ländern in einer einheitlichen webbasierten Oberfläche.

Das Portal kann auch zur Bereitstellung des Schulungsmaterials verwendet werden. Sämtliches Schulungsmaterial wird lizenziert, nicht verkauft, und verbleibt ausschließlich im Eigentum von IBM. IBM erteilt dem Kunden ein Nutzungsrecht gemäß den im Portal aufgeführten Bedingungen. Das Schulungsmaterial wird „as is“, ohne jegliche Gewährleistung oder Haftung bereitgestellt, sei sie ausdrücklich oder stillschweigend, einschließlich, jedoch nicht beschränkt auf die Gewährleistung für die Handelsüblichkeit, die Verwendbarkeit für einen bestimmten Zweck und die Nichtverletzung von Eigentums- und Schutzrechten.

3.2.1 Leistungsumfang

IBM wird

a. dem Kunden während 24 Stunden pro Tag an 7 Tagen die Woche Zugriff auf das Portal gewähren. Das Portal bietet Folgendes:
   (1) Informationen über und Warnung bei Sicherheitsbedrohungen;
   (2) Details zur Agentenkonfiguration und -richtlinie;
   (3) Informationen über Sicherheitsverstöße und Servicetickets;
   (4) Möglichkeit der Initiierung und Aktualisierung von Tickets und Workflows;
   (5) Möglichkeit des Live-Chats und der Onlinezusammenarbeit mit einem SOC-Analysten;
   (6) Dashboard für die Erstellung von Berichten auf der Basis von Vorlagen;
   (7) Zugriff auf Echtzeit- und archivierte Agentenprotokolle und -ereignisse;
   (8) Berechtigung zum Download von Protokolldaten;
   (9) Differenzierte Abfragefunktionen für Sicherheitsereignisse und -protokolle; und
   (10) Zugriff auf das Schulungsmaterial gemäß den im Portal aufgeführten Bedingungen;
b. die Verfügbarkeit des Portals gemäß den Kennzahlen sicherstellen, die im Abschnitt „Service-Level-Agreements“, „Verfügbarkeit des Portals“ dieser Leistungsbeschreibung angegeben sind.

3.2.2 Verantwortlichkeiten des Kunden

Der Kunde wird

a. das Portal nutzen, um tägliche Aktivitäten im Rahmen des Betriebs durchzuführen;
b. sicherstellen, dass die Mitarbeiter des Kunden, die im Namen des Kunden auf das Portal zugreifen, die im Portal veröffentlichten Nutzungsbedingungen einhalten, einschließlich der Bedingungen im Zusammenhang mit dem Schulungsmaterial;

c. seine Zugangsdaten für die Anmeldung am Portal angemessen schützen (das bedeutet unter anderem, sie gegenüber Unbefugten nicht offenzulegen);

d. IBM umgehend benachrichtigen, wenn er den Verdacht hat, dass seine Zugangsdaten kompromittiert wurden; und

e. IBM in Bezug auf alle Verluste entschädigen und schadlos halten, die IBM durch den Kunden oder Dritte dadurch entstehen, dass der Kunde seine Zugangsdaten nicht angemessen schützt.

3.3 Ansprechpartner für die Services

Der Kunde kann zwischen mehreren Ebenen des Zugriffs auf das SOC und das Portal wählen. Dadurch kann er verschiedenen Rollen in seinem Unternehmen unterschiedliche Zugriffsrechte zuweisen.

Autorisierte Ansprechpartner für die Sicherheit

Ein autorisierter Ansprechpartner für die Sicherheit ist ein Entscheidungsträger, der für alle betrieblichen Aspekte im Zusammenhang mit den IBM Managed Security Services verantwortlich ist.

Benannte Ansprechpartner für die Services

Ein benannter Ansprechpartner für die Services ist ein Entscheidungsträger, der für bestimmte betriebliche Aspekte im Zusammenhang mit den IBM Managed Security Services, einem Agenten oder einer Gruppe von Agenten verantwortlich ist. IBM wird sich mit einem benannten Ansprechpartner für die Services nur über die betrieblichen Aktivitäten austauschen, die in dessen Zuständigkeitsbereich fallen (z. B. über den Ausfall eines Agenten mit dem dafür benannten Ansprechpartner).

Portalbenutzer

IBM bietet mehrere Ebenen des Zugriffs für Portalbenutzer an. Diese Zugriffsebenen können auf einen IBM Managed Security Service, einen Agenten oder eine Gruppe von Agenten angewandt werden. Die Portalbenutzer werden mittels eines statischen Kennworts oder einer vom Kunden bereitgestellten Technologie für die Verschlüsselung mit öffentlichem Schlüssel (z. B. RSA SecureID-Token) auf der Basis der Anforderungen des Kunden authentifiziert.

3.3.1 Leistungsumfang

Autorisierte Ansprechpartner für die Sicherheit

IBM wird

a. dem Kunden die Erstellung von bis zu drei autorisierten Ansprechpartnern für die Sicherheit ermöglichen;

b. jedem autorisierten Ansprechpartner für die Sicherheit Folgendes bereitstellen:

   (1) administrative Portalberechtigungen für die Agenten des Kunden;

   (2) die Berechtigung zur Erstellung einer unbegrenzten Anzahl an benannten Ansprechpartnern für die Services und Portalbenutzern; und

   (3) die Berechtigung zur Delegation der Verantwortung an die benannten Ansprechpartner für die Services;

c. sich mit den autorisierten Ansprechpartnern für die Sicherheit über Aspekte bezüglich der Unterstützung und Benachrichtigung im Zusammenhang mit den Services austauschen; und

d. die Identität der autorisierten Ansprechpartner für die Sicherheit mittels einer Authentifizierungsmethode überprüfen, die ein vorab ausgetauschtes Abfragekennwort oder eine vorab ausgetauschte Abfragekennziffer verwendet.

Benannte Ansprechpartner für die Services

IBM wird

a. die Identität der benannten Ansprechpartner für die Services mittels einer Authentifizierungsmethode überprüfen, die ein vorab ausgetauschtes Abfragekennwort verwendet; und

b. sich mit den benannten Ansprechpartnern für die Services nur über die betrieblichen Aspekte austauschen, für die sie verantwortlich sind.

Portalbenutzer

IBM wird

a. mehrere Ebenen des Zugriffs auf das Portal bereitstellen:

   (1) Funktionen für administrative Benutzer, einschließlich folgender Möglichkeiten:

(a) Erstellung von Portalbenutzern;

(b) Erstellung und Bearbeitung von kundenspezifischen Agentengruppen;

(c) Übermittlung von Anforderungen einer Richtlinienänderung für einen Managed Agent oder eine Gruppe von Agenten an die SOCs;

(d) Übermittlung von Serviceanforderungen an die SOCs;

(e) „Live Chat“ mit einem SOC-Analysten in Bezug auf bestimmte Vorfälle oder Tickets, die im Rahmen der Services erstellt wurden;

(f) Erstellung interner Tickets im Zusammenhang mit den Services und Zuordnung dieser Tickets zu den Portalbenutzern;

(g) Abfrage, Anzeige und Aktualisierung von Tickets im Zusammenhang mit den Services;

(h) Anzeige und Bearbeitung von Agentendetails;

(i) Anzeige von Agentenrichtlinien;

(j) Erstellung und Bearbeitung von Beobachtungslisten (Watch Lists) zu Schwachstellen;

(k) Überwachung von Protokollen und Ereignissen;

(l) Abfrage von Sicherheitsereignis- und Protokolldaten;

(m) Planung von Downloads von Sicherheitsereignis- und Protokolldaten; und

(n) Planung und Ausführung von Berichten;

(2) Funktionen für reguläre Benutzer, einschließlich aller Rechte eines administrativen Benutzers für die Agenten, für die der Benutzer zuständig ist, mit Ausnahme der Möglichkeit zur Erstellung von Portalbenutzern; und

(3) Funktionen für eingeschränkte Benutzer, einschließlich aller Rechte eines regulären Benutzers für die Agenten, für die der Benutzer zuständig ist, mit Ausnahme folgender Möglichkeiten:

(a) Erstellung und Übermittlung von Anforderungen einer Richtlinienänderung;

(b) Aktualisierung von Tickets; und

(c) Bearbeitung von Agentendetails;

b. dem Kunden die Berechtigung erteilen, Zugriffsebenen auf einen Agenten oder auf Gruppen von Agenten anzuwenden;

c. Portalbenutzer mittels eines statischen Kennworts authentifizieren; und

d. Portalbenutzer mittels einer vom Kunden bereitgestellten Technologie für die Verschlüsselung mit öffentlichem Schlüssel (z. B. RSA SecureID-Token) auf der Basis der Kundenanforderungen authentifizieren.

3.3.2 Verantwortlichkeiten des Kunden

Autorisierte Ansprechpartner für die Sicherheit

Der Kunde wird

a. IBM Kontaktinformationen zu jedem autorisierten Ansprechpartner für die Sicherheit bereitstellen. Die autorisierten Ansprechpartner für die Sicherheit sind für Folgendes verantwortlich:

(1) Erstellung der benannten Ansprechpartner für die Services und Delegation von Verantwortlichkeiten und Rechten an diese Ansprechpartner, sofern angebracht;

(2) Erstellung von Portalbenutzern;

(3) Authentifizierung bei den SOCs mittels eines vorab ausgetauschten Abfragekennworts; und

(4) Pflege von Informationen zur Benachrichtigungsreihenfolge und von Kontaktinformationen zu Ansprechpartnern des Kunden sowie Übergabe dieser Informationen an IBM;

b. sicherstellen, dass mindestens ein autorisierter Ansprechpartner für die Sicherheit während 24 Stunden pro Tag an 7 Tagen die Woche erreichbar ist;

c. IBM innerhalb von drei Kalendertagen über Änderungen an den Kontaktinformationen zu Ansprechpartnern des Kunden informieren; und

d. bestätigen, dass nicht mehr als drei autorisierte Ansprechpartner für die Sicherheit erlaubt sind, unabhängig von der vereinbarten Anzahl an IBM Services oder Agenten.

Benannte Ansprechpartner für die Services

Der Kunde wird

a. IBM Kontaktinformationen zu jedem benannten Ansprechpartner für die Services und Informationen zu dessen Zuständigkeit bereitstellen. Die benannten Ansprechpartner für die Services sind für die Authentifizierung bei den SOCs mittels einer Kennphrase verantwortlich; und

b. bestätigen, dass ein benannter Ansprechpartner für die Services möglicherweise während 24 Stunden pro Tag an 7 Tagen die Woche erreichbar sein muss, abhängig von seinem Zuständigkeitsbereich (z. B. wenn der Ausfall eines Agenten in seinen Zuständigkeitsbereich fällt).

Portalbenutzer

Der Kunde wird

a. zustimmen, dass die Portalbenutzer das Portal zur Durchführung täglicher Aktivitäten im Rahmen des Betriebs nutzen werden;

b. die Verantwortung für die Bereitstellung der von IBM unterstützten RSA SecureID-Tokens übernehmen (sofern zutreffend); und

c. bestätigen, dass die SOCs nur mit den autorisierten Ansprechpartnern für die Sicherheit und den benannten Ansprechpartnern für die Services kommunizieren werden.

3.4 Security Intelligence

Informationen zu Sicherheitsbedrohungen werden vom IBM X-Force® Threat Analysis Center bereitgestellt, das eine Risikostufe („AlertCon“ genannt) zu Sicherheitsbedrohungen aus dem Internet veröffentlicht. Der AlertCon-Level beschreibt die progressiven Alarmstufen aktueller Gefahren aus dem Internet. Falls dieser Level auf AlertCon 3 angehoben wird – diese Stufe steht für gezielte Angriffe, die unverzügliche Abwehrmaßnahmen erfordern –, wird IBM dem Kunden Echtzeitzugriff auf IBM Informationen oder Anweisungen zur globalen Lage bereitstellen. Als Benutzer des Portals hat der Kunde Zugang zum X-Force Hosted Threat Analysis Service, der Zugriff auf den IBM X-Force Threat Insight Quarterly (Threat IQ) Report beinhaltet.

Über das Portal kann der Kunde eine Beobachtungsliste (Watch List) zu Schwachstellen mit individuell angepassten Informationen zu Sicherheitsbedrohungen erstellen. Darüber hinaus kann jeder Portalbenutzer auf Anforderung pro Arbeitstag eine Bewertung der Internetsicherheit per E-Mail erhalten. Diese Bewertung enthält eine Analyse der aktuellen bekannten Sicherheitsbedrohungen aus dem Internet, Echtzeitmessdaten zu Internet-Ports sowie individuell angepasste Warnungen, Empfehlungen und Sicherheitsnachrichten.

Anmerkung: Der Zugriff des Kunden auf die Informationen zu Sicherheitsbedrohungen, die über das Portal bereitgestellt werden, und die Nutzung dieser Informationen durch den Kunden (einschließlich des Threat IQ Report und der täglichen Bewertung der Internetsicherheit per E-Mail) unterliegen den im Portal angegebenen Nutzungsbedingungen. Im Fall von Widersprüchen zwischen den im Portal angegebenen Nutzungsbedingungen und den Bedingungen des Vertrags haben die im Portal angegebenen Nutzungsbedingungen Vorrang. Zusätzlich zu den im Portal angegebenen Nutzungsbedingungen gelten für die Nutzung von Informationen in Links oder Webseiten und Ressourcen Dritter durch den Kunden die in diesen Links oder Webseiten und Ressourcen Dritter veröffentlichten Nutzungsbedingungen.

3.4.1 Leistungsumfang

IBM wird

a. dem Kunden Zugriff auf den X-Force Hosted Threat Analysis Service gewähren;

b. dem Kunden einen Benutzernamen, ein Kennwort, eine URL und entsprechende Berechtigungen für den Zugriff auf das Portal bereitstellen;

c. Informationen über die Sicherheit im Portal anzeigen, sobald sie verfügbar sind;

d. über das Portal Informationen zu Sicherheitsbedrohungen bereitstellen, die auf eine vom Kunden definierte Beobachtungsliste zu Schwachstellen abgestimmt sind, sofern vom Kunden entsprechend konfiguriert;

e. an jedem Arbeitstag eine Bewertung der Internetsicherheit per E-Mail bereitstellen, sofern vom Kunden entsprechend konfiguriert;

f. einen AlertCon-Level zu Sicherheitsbedrohungen aus dem Internet über das Portal veröffentlichen;

g. einen Internet-Notfall ausrufen, wenn der tägliche AlertCon-Level AlertCon 3 erreicht. In diesem Fall wird IBM dem Kunden Echtzeitzugriff auf IBM Informationen oder Anweisungen zur globalen Lage bereitstellen;

h. dem Kunden Portalfunktionen zur Erstellung und Pflege einer Beobachtungsliste zu Schwachstellen bereitstellen;

i. zusätzliche Informationen über Warnungen, Empfehlungen oder weitere wichtige Sicherheitsaspekte bereitstellen, sofern IBM dies für notwendig hält; und

j. dem Kunden Zugriff auf den Threat IQ Report über das Portal bereitstellen.

3.4.2 Verantwortlichkeiten des Kunden

Der Kunde wird das Portal verwenden, um

a. die tägliche Bewertung der Internetsicherheit per E-Mail zu abonnieren, sofern gewünscht;

b. eine Beobachtungsliste zu Schwachstellen zu erstellen, sofern gewünscht;

c. auf den Threat IQ Report zuzugreifen; und

d. die Lizenzvereinbarung einzuhalten und die im Rahmen des Service erhaltenen Informationen nicht an Personen ohne gültige Lizenz weiterzugeben.

3.5 Implementierung und Aktivierung

Während der Implementierung und Aktivierung wird IBM in Zusammenarbeit mit dem Kunden einen neuen Agenten implementieren oder mit dem Management eines vorhandenen Agenten beginnen.

Anmerkung: Die Aktivitäten im Rahmen der Implementierung und Aktivierung werden einmal während der Erbringung der Leistungen durchgeführt. Wenn der Kunde seinen Agenten während der Laufzeit des Servicevertrags austauscht, aufrüstet oder an einen anderen Standort verlegt, kann IBM verlangen, dass dieser Agent erneut implementiert und aktiviert wird (nachfolgend „erneute Implementierung“ genannt). Solche erneuten Implementierungen werden gegen Zahlung einer im jeweils geltenden Bestellschein (nachfolgend „Bestellschein“ genannt) angegebenen zusätzlichen Gebühr durchgeführt. Die Gebühren für eine erneute Implementierung sind nur für einen Austausch, ein Upgrade oder eine Verlegung von Hardware an einen anderen Standort, initiiert vom Kunden, fällig. Sie sind nicht auf Defekte von Agenten anwendbar, die zu einer Rücksendung der Agenten führen.

3.5.1 Leistungsumfang

Aktivität 1 – Projektauftakt

Zweck dieser Aktivität ist die Durchführung einer Besprechung zum Projektauftakt. IBM wird dem Kunden eine Begrüßungsmail zusenden und eine maximal einstündige Besprechung zum Projektauftakt mit bis zu drei Mitarbeitern des Kunden durchführen, um

a. den Beauftragten des Kunden dem für die Implementierung zuständigen IBM Spezialisten vorzustellen;

b. die Verantwortlichkeiten jeder Vertragspartei zu prüfen;

c. die Erwartungen an den Zeitplan festzulegen; und

d. mit der Analyse der Anforderungen und der Umgebung des Kunden zu beginnen.

Beendigung der Leistungen:

Die IBM Verpflichtungen im Rahmen dieser Aktivität sind erfüllt, wenn die Besprechung zum Projektauftakt durchgeführt wurde.

Zu liefernde Materialien:

- Keine

Aktivität 2 – Voraussetzungen für den Netzwerkzugriff

Zweck dieser Aktivität ist die Festlegung der Voraussetzungen für den Netzwerkzugriff.

IBM wird

a. dem Kunden ein Dokument zu den Voraussetzungen für den Netzwerkzugriff („Network Access Requirements“ genannt) übergeben, das detailliert beschreibt,

   (1) wie IBM eine Remote-Verbindung zum Netzwerk des Kunden herstellen wird; und

   (2) welche technischen Voraussetzungen für diese Remote-Verbindung erforderlich sind;

Anmerkung: IBM kann das Dokument „Network Access Requirements“ während der Erbringung der Services ändern, sofern IBM dies für angebracht hält.

b. eine Verbindung zum Netzwerk des Kunden über das Internet mittels IBM Standardzugriffsmethoden herstellen; und

c. sofern angebracht, ein Site-to-Site-VPN für die Verbindung zum Netzwerk des Kunden einsetzen. Dieses VPN kann von IBM gegen Zahlung einer im Bestellschein angegebenen zusätzlichen Gebühr bereitgestellt werden.

Beendigung der Leistungen:

Die IBM Verpflichtungen im Rahmen dieser Aktivität sind erfüllt, wenn das Dokument „Network Access Requirements“ an den Beauftragten des Kunden übergeben wurde.

Zu liefernde Materialien:

- Dokument „Network Access Requirements“

Aktivität 3 – Prüfung

Zweck dieser Aktivität ist die Durchführung einer Prüfung der aktuellen Umgebung sowie der geschäftlichen und technischen Ziele des Kunden, um den Kunden bei der Ausarbeitung der erforderlichen Sicherheitsstrategie für den Agenten zu unterstützen.

Aufgabe 1 – Erfassung von Daten

IBM wird

a. dem Beauftragten des Kunden ein Formular zur Datenerfassung übergeben, auf dem der Kunde folgende Informationen dokumentieren wird:

   (1) Namen, Kontaktinformationen, Aufgabenbereiche und Verantwortlichkeiten der Mitglieder des Projektteams;

   (2) Besondere länder- und standortspezifische Anforderungen;

   (3) Vorhandene Netzwerkinfrastruktur des Kunden;

   (4) Kritische Server;

   (5) Anzahl und Art der Endbenutzer; und

   (6) Wichtige Einflussfaktoren und/oder Abhängigkeiten, die die Erbringung der Leistungen oder die vereinbarten Fristen beeinflussen könnten.

Aufgabe 2 – Prüfung der Umgebung

IBM wird

a. die im Formular zur Datenerfassung angegebenen Informationen verwenden, um die vorhandene Umgebung des Kunden zu prüfen;

b. eine optimale Agentenkonfiguration bestimmen; und

c. sofern zutreffend, Empfehlungen zur Anpassung der Richtlinie eines Agenten oder der Anordnung des Netzwerks abgeben, um die Sicherheit zu verbessern.

Aufgabe 3 – Prüfung des vorhandenen Agenten

IBM wird

a. den Agenten per Fernanalyse prüfen, um zu verifizieren, dass er den IBM Spezifikationen entspricht;

b. Anwendungs- und Benutzeraccounts ermitteln, die gelöscht oder hinzugefügt werden sollen, sofern zutreffend; und

c. bei Agenten, die den IBM Spezifikationen nicht entsprechen,

   (1) die Agentensoftware ermitteln, die ein Upgrade erfordert, und/oder

   (2) die Agentenhardware ermitteln, die ein Upgrade erfordert, damit sie den Kompatibilitätslisten der jeweiligen Hersteller entspricht.

Beendigung der Leistungen:

Die IBM Verpflichtungen im Rahmen dieser Aktivität sind erfüllt, wenn IBM die Umgebung des Kunden und den vorhandenen Agenten des Kunden (sofern zutreffend) geprüft hat.

Zu liefernde Materialien:

- Keine

Aktivität 4 – Out-of-Band-Zugriff

Out-of-Band-Zugriff ist erforderlich, um die SOCs zu unterstützen, falls die Verbindung zu einem Agenten unterbrochen wird. Im Fall solcher Verbindungsprobleme kann sich der SOC-Analyst in das Out-of-Band-Gerät einwählen, um zu verifizieren, dass der Agent korrekt funktioniert, und versuchen, die Ursache des Ausfalls zu bestimmen, bevor das Problem an den Kunden eskaliert wird.

IBM wird

a. den Kunden per Telefon und E-Mail dabei unterstützen, Dokumente des jeweiligen Herstellers zu finden, die eine genaue Beschreibung der Verfahren für die physische Installation und der Verkabelung enthalten;

b. das Out-of-Band-Gerät für den Zugriff auf die Managed Agents konfigurieren; oder

c. mit dem Kunden zusammenarbeiten, um eine von IBM genehmigte vorhandene Out-of-Band-Lösung zu nutzen.

Anmerkung: Zum Zweck der Klarstellung wird darauf hingewiesen, dass IBM auf den erforderlichen Out-of-Band-Zugriff verzichten kann, falls die interne Sicherheitsrichtlinie des Kunden die Verwendung eines Out-of-Band-Geräts verbietet. Dies kann jedoch die Fähigkeit von IBM zur effektiven Erbringung der Services deutlich beeinträchtigen.

Beendigung der Leistungen:

Die IBM Verpflichtungen im Rahmen dieser Aktivität sind erfüllt, wenn eine der folgenden Bedingungen zuerst eintritt:

- IBM hat das Out-of-Band-Gerät für den Zugriff auf den Managed Agent konfiguriert.

  oder

- IBM hat sich auf Wunsch des Kunden damit einverstanden erklärt, auf den erforderlichen Out-of-Band-Zugriff zu verzichten.

Zu liefernde Materialien:

- Keine

Aktivität 5 – Implementierung

Zweck dieser Aktivität ist die Implementierung des Agenten.

Aufgabe 1 – Konfiguration des Agenten

IBM wird

a. den Agenten per Fernanalyse prüfen, um zu verifizieren, dass er den IBM Spezifikationen entspricht;

b. Agentensoftware, -hardware und/oder -inhalte ermitteln, die nicht mit den aktuellen von IBM unterstützten Versionen übereinstimmen;

c. sofern angebracht, Hardware-Upgrades ermitteln, die erforderlich sind, um die Kompatibilitätslisten der jeweiligen Hersteller zu unterstützen;

d. den Agenten per Fernzugriff konfigurieren. Dies schließt die Festlegung der Richtlinie, die Absicherung des Betriebssystems und die Registrierung des Agenten in der IBM MSS-Infrastruktur ein;

e. telefonische Unterstützung bereitstellen und den Kunden darüber informieren, wo Dokumente des Herstellers zu finden sind, um den Kunden bei der Konfiguration des Agenten mit einer öffentlichen IP-Adresse und zugehörigen Einstellungen zu unterstützen. Diese Unterstützung muss im Voraus geplant werden, um sicherzustellen, dass ein IBM Spezialist für die Implementierung zur Verfügung steht;

f. die Agentenrichtlinie anpassen, um die Zahl von Fehlalarmen zu reduzieren (sofern zutreffend); und

g. auf Wunsch des Kunden die Konfiguration und Richtlinie auf dem vorhandenen Agenten ausführen.

Aufgabe 2 – Installation des Agenten

IBM wird

a. den Kunden per Telefon und/oder E-Mail dabei unterstützen, Dokumente des jeweiligen Herstellers zu finden, die eine genaue Beschreibung der Verfahren für die physische Installation und der Verkabelung enthalten. Diese Unterstützung muss im Voraus geplant werden, um sicherzustellen, dass ein IBM Spezialist für die Implementierung zur Verfügung steht;

b. Empfehlungen zur Anpassung der Anordnung des Netzwerks zur Verbesserung der Sicherheit abgeben (sofern zutreffend);

c. den Agenten per Fernzugriff konfigurieren. Dies schließt die Registrierung des Agenten in der IBM MSS-Infrastruktur ein; und

d. die Agentenrichtlinie anpassen, um die Zahl von Fehlalarmen zu reduzieren (sofern zutreffend).

Anmerkung: Der Kunde kann Leistungen für die physische Installation im Rahmen eines gesonderten Vertrags bei IBM beauftragen.

Beendigung der Leistungen:

Die IBM Verpflichtungen im Rahmen dieser Aktivität sind erfüllt, wenn der Agent in der IBM MSS-Infrastruktur registriert ist.

Zu liefernde Materialien:

- Keine

Aktivität 6 – Test und Verifizierung

Zweck dieser Aktivität ist der Test und die Verifizierung der Services.

IBM wird

a. die Verbindung des Agenten zu der IBM MSS-Infrastruktur verifizieren;

b. abschließende Funktionstests der Services durchführen;

c. die Übermittlung von Protokolldaten von dem Agenten an die IBM MSS-Infrastruktur verifizieren;

d. die Verfügbarkeit und Funktionalität des Agenten im Portal verifizieren;

e. Qualitätssicherungstests des Agenten durchführen; und

f. bis zu zehn Mitarbeitern des Kunden die wichtigsten Funktionen des Portals im Rahmen einer maximal einstündigen Remote-Demonstration vorstellen.

Beendigung der Leistungen:

Die IBM Verpflichtungen im Rahmen dieser Aktivität sind erfüllt, wenn IBM die Verfügbarkeit und Funktionalität des Agenten im Portal verifiziert hat.

Zu liefernde Materialien:

- Keine

Aktivität 7 – Aktivierung der Services

Zweck dieser Aktivität ist die Aktivierung der Services.

IBM wird

a. das Management und die Unterstützung des Agenten übernehmen;

b. den Agenten auf „active“ einstellen; und

c. die Verantwortung für das fortlaufende Management und die kontinuierliche Unterstützung des Agenten an die SOCs übertragen.

Beendigung der Leistungen:

Die IBM Verpflichtungen im Rahmen dieser Aktivität sind erfüllt, wenn der Agent auf „active“ eingestellt wurde.

Zu liefernde Materialien:

- Keine

3.5.2 Verantwortlichkeiten des Kunden

Aktivität 1 – Projektauftakt

Der Kunde wird

a. an der Besprechung zum Projektauftakt teilnehmen; und

b. die Verantwortlichkeiten jeder Vertragspartei prüfen.

Aktivität 2 – Voraussetzungen für den Netzwerkzugriff

Der Kunde wird

a. das IBM Dokument „Network Access Requirements“ prüfen und während der Implementierung und der gesamten Vertragslaufzeit befolgen; und

b. die alleinige Verantwortung für alle Gebühren übernehmen, die dadurch entstehen, dass IBM ein Site-to-Site-VPN für die Verbindung zum Netzwerk des Kunden nutzt.

Aktivität 3 – Prüfung

Aufgabe 1 – Erfassung von Daten

Der Kunde wird

a. alle Fragebogen und/oder Formulare zur Datenerfassung ausfüllen und innerhalb von fünf Tagen nach Erhalt an IBM zurückgeben;

b. Informationen, Daten, Zustimmungen, Entscheidungen und Genehmigungen, die IBM zur Implementierung der Services benötigt, innerhalb von zwei Arbeitstagen nach Anforderung durch IBM beschaffen und bereitstellen;

c. mit IBM zusammenarbeiten, um die Netzwerkumgebung des Kunden sorgfältig zu prüfen;

d. für den Fall, dass IBM Kontakt zum Kunden aufnehmen muss, Ansprechpartner im Unternehmen des Kunden nennen und eine Benachrichtigungsreihenfolge in seinem Unternehmen angeben; und

e. IBM innerhalb von drei Kalendertagen über Änderungen an den Kontaktinformationen zu den Ansprechpartnern des Kunden informieren.

Aufgabe 2 – Prüfung der Umgebung

Der Kunde wird

a. sicherstellen, dass gültige Lizenz-, Support- und Wartungsverträge für die Agenten vorliegen; und

b. alle von IBM angeforderten Änderungen an der Anordnung des Netzwerks des Kunden zur Verbesserung der Sicherheit durchführen.

Aufgabe 3 – Prüfung des vorhandenen Agenten

Der Kunde wird

a. sicherstellen, dass der vorhandene Agent den IBM Spezifikationen entspricht;

b. die von IBM angegebenen Anwendungen und Benutzeraccounts entfernen oder hinzufügen; und

c. auf Anforderung von IBM

   (1) die von IBM angegebene Agentensoftware aufrüsten; und

   (2) die von IBM angegebene Agentenhardware aufrüsten.

Aktivität 4 – Out-of-Band-Zugriff

Der Kunde wird

a. beim Einsatz neuer Out-of-Band-Lösungen

   (1) ein von IBM unterstütztes Out-of-Band-Gerät erwerben;

   (2) das Out-of-Band-Gerät physisch installieren und mit dem Agenten verbinden;

   (3) eine dedizierte analoge Telefonleitung für den Zugriff bereitstellen;

   (4) das Out-of-Band-Gerät physisch an die dedizierte Telefonleitung anschließen und die Verbindung aufrechterhalten;

   (5) die Verantwortung für alle Gebühren im Zusammenhang mit dem Out-of-Band-Gerät und der Telefonleitung übernehmen; und

   (6) die Verantwortung für alle Gebühren im Zusammenhang mit dem fortlaufenden Management der Out-of-Band-Lösung übernehmen;

b. beim Einsatz vorhandener Out-of-Band-Lösungen

   (1) sicherstellen, dass die Lösung IBM keinen Zugriff auf nicht von IBM betriebene Geräte ermöglicht;

   (2) sicherstellen, dass die Lösung keine Installation spezifischer Software erfordert;

   (3) IBM detaillierte Anweisungen für den Zugriff auf die Managed Agents bereitstellen; und

   (4) die Verantwortung für alle Aspekte im Zusammenhang mit dem Management der Out-of-Band-Lösung übernehmen;

c. bestätigen, dass vorhandene Out-of-Band-Lösungen von IBM genehmigt werden müssen;

d. sicherstellen, dass gültige Support- und Wartungsverträge für das Out-of-Band-Gerät vorliegen (sofern erforderlich); und

e. bestätigen – falls der Kunde sich für eine Nutzung der Services ohne den erforderlichen Out-of-Band-Zugriff entscheidet oder der Out-of-Band-Zugriff IBM aus irgendeinem Grund nicht zur Verfügung steht –, dass

   (1) IBM der Verpflichtungen im Rahmen aller SLAs enthoben wird, die direkt von der Verfügbarkeit dieses Zugriffs beeinflusst werden;

   (2) IBM möglicherweise mehr Zeit für die Fehlersuche/-behebung und/oder Wartung der Geräte des Kunden benötigt; und

   (3) der Kunde verpflichtet ist, IBM vor Ort bei der Konfiguration, Problemlösung, Geräteaktualisierung, Fehlersuche/-behebung und/oder jeder anderen Aufgabe zu unterstützen, die üblicherweise mittels Out-of-Band-Zugriff durchgeführt wird.

Aktivität 5 – Implementierung

Aufgabe 1 – Konfiguration des Agenten

Der Kunde wird

a. ein Update der Agentensoftware oder -inhalte auf die neueste von IBM unterstützte Version durchführen (d. h. Datenträger physisch laden, sofern zutreffend);

b. ein Update der Hardware durchführen, um die Kompatibilitätslisten der jeweiligen Hersteller zu unterstützen (sofern zutreffend);

c. die Agentenrichtlinie anpassen, wie von IBM angefordert;

d. den Agenten mit einer öffentlichen IP-Adresse und zugehörigen Einstellungen konfigurieren; und

e. IBM bei der Ausführung der Konfiguration und Richtlinie des vorhandenen Agenten unterstützen (sofern zutreffend).

Aufgabe 2 – Installation des Agenten

Der Kunde wird

a. in Zusammenarbeit mit IBM Dokumente der Hersteller suchen, die eine genaue Beschreibung der Verfahren für die physische Installation und der Verkabelung enthalten. Der Kunde wird diese Unterstützung im Voraus planen, um sicherzustellen, dass ein IBM Spezialist für die Implementierung zur Verfügung steht;

b. die Verantwortung für die physische Verkabelung und Installation des/der Agenten übernehmen; und

c. die von IBM angegebenen Anpassungen an der Anordnung des Netzwerks zur Verbesserung der Sicherheit durchführen.

Aktivität 6 – Test und Verifizierung

Der Kunde wird

a. die Verantwortung für die Erarbeitung aller spezifischen Testpläne der abschließenden Funktionstests des Kunden übernehmen;

b. die Verantwortung für die Durchführung der abschließenden Funktionstests der Anwendungen und Netzwerkverbindungen des Kunden übernehmen; und

c. bestätigen, dass zusätzliche abschließende Funktionstests, die der Kunde durchführt oder nicht durchführt, IBM nicht daran hindern, den Agenten in den SOCs auf „active“ einzustellen, um die kontinuierliche Unterstützung und das fortlaufende Management durch die SOCs zu aktivieren.

Aktivität 7 – Aktivierung der Services

Diese Aktivität erfordert keine weiteren Verantwortlichkeiten des Kunden.

3.6 Datenerfassung und -archivierung

IBM nutzt das X-Force Protection System, um Sicherheitsereignis- und Protokolldaten zu erfassen, zu organisieren, zu archivieren und abzurufen. Über das Portal erhält der Kunde während 24 Stunden pro Tag an 7 Tagen die Woche Einblick in die Services, einschließlich des Onlinezugriffs auf Rohprotokolle, die in der Infrastruktur des X-Force Protection System erfasst und gespeichert werden. Sicherheitsereignis- und Protokolldaten können im Portal für die Dauer eines Jahres online angezeigt werden. Nach Ablauf dieser Frist werden die Daten auf Offlinespeicher ausgelagert (sofern zutreffend).

3.6.1 Leistungsumfang

IBM wird

a. die von dem Managed Agent erzeugten Protokoll- und Ereignisdaten erfassen, sobald sie die IBM MSS-Infrastruktur erreichen;

b. die von dem Managed Agent erzeugten Protokoll- und Ereignisdatenströme drosseln, wenn diese Datenströme 100 Ereignisse pro Sekunde überschreiten;

c. die erfassten Protokoll- und Ereignisdaten eindeutig identifizieren;

d. die erfassten Daten im X-Force Protection System archivieren;

e. die Protokoll- und Ereignisdaten ein Jahr lang aufbewahren, sofern nicht vom Kunden anders angegeben;

f. die erfassten Protokoll- und Ereignisdaten ein Jahr lang im Portal anzeigen;

g. sofern unterstützt, die Protokoll- und Ereignisdaten normalisieren, damit sie besser im Portal präsentiert werden können;

h. mit dem Löschen der erfassten Protokoll- und Ereignisdaten beginnen, wobei die FIFO-Methode (First In, First Out) angewandt wird,

   (1) wenn die Standardaufbewahrungsdauer (ein Jahr) oder die vom Kunden festgelegten Aufbewahrungsfristen (sofern zutreffend) abgelaufen ist bzw. sind; oder

   (2) wenn die Protokoll- und Ereignisdaten das Alter von sieben Jahren überschreiten;

   Anmerkung: Ungeachtet der vom Kunden festgelegten Aufbewahrungsfristen wird IBM Protokoll- und Ereignisdaten nicht länger als sieben Jahre aufbewahren. Überschreitet der Kunde die Aufbewahrungsdauer von sieben Jahren an irgendeinem Zeitpunkt während der Vertragslaufzeit, wird IBM damit beginnen, die erfassten Protokoll- und Ereignisdaten mittels der FIFO-Methode zu löschen.

i. sofern IBM dies für angebracht hält, ein Site-to-Site-VPN empfehlen, das zur Verschlüsselung des Datenverkehrs verwendet wird, der nicht nativ durch den Agenten verschlüsselt wird.

   Anmerkung: Die über das Internet übertragenen Daten werden nur dann mittels der nativ vom Agenten bereitgestellten standardisierten Verschlüsselungsalgorithmen verschlüsselt, wenn der (vom Kunden bereitgestellte) Agent mit der entsprechenden Funktionalität ausgestattet ist.

3.6.2 Verantwortlichkeiten des Kunden

Der Kunde wird

a. IBM die Aufbewahrungsfristen für Sicherheitsereignis- und Protokolldaten mitteilen, sofern diese nicht sieben Jahre überschreiten bzw. überschritten haben;

b. das Portal verwenden, um Sicherheitsereignis- und Protokolldaten zu prüfen und abzufragen;

c. das Portal verwenden, um sich eigenverantwortlich über den verfügbaren Speicherplatz für Protokoll- und Ereignisdaten zu informieren;

d. sicherstellen, dass ein gültiger Vertrag über Firewall Management – Premium für jede einzelne Sicherheitsereignis- und Protokolldatenquelle vorliegt;

   Anmerkung: Wenn die Services aus irgendeinem Grund gekündigt werden, wird IBM seiner Verpflichtung enthoben, die Sicherheitsereignis- und Protokolldaten des Kunden aufzubewahren.

e. bestätigen, dass

   (1) IBM die erfassten Protokoll- und Ereignisdaten für die Dauer eines Kalenderjahres aufbewahren wird, sofern nicht vom Kunden schriftlich anders angegeben;

   (2) alle Protokoll- und Ereignisdaten über das Internet an die SOCs übertragen werden;

   (3) unverschlüsselte Daten, die über das Internet übertragen werden, nicht verschlüsselt werden, falls der Kunde kein von IBM empfohlenes Site-to-Site-VPN für Agenten nutzt, die keine nativen Verschlüsselungsalgorithmen bereitstellen;

   (4) IBM nur Protokoll- und Ereignisdaten erfassen und archivieren kann, die erfolgreich an die IBM MSS-Infrastruktur übertragen werden;

   (5) IBM nicht garantiert, dass die Sicherheitsereignis- oder Protokolldaten in einem nationalen oder internationalen Rechtssystem als Beweis verwendet werden können. Die Zulässigkeit von Beweisen basiert auf den beteiligten Technologien und der Fähigkeit des Kunden, die korrekte Datenverarbeitung und Beweiskette für jeden präsentierten Datensatz nachzuweisen;

(6) IBM das Recht hat, die von dem Agenten erzeugten Ereignisströme zu drosseln, sofern diese 100 Ereignisse pro Sekunde übersteigen (sofern erforderlich);

(7) IBM Protokoll- und Ereignisdaten nicht länger als sieben Jahre aufbewahren wird; und

(8) die vom Kunden festgelegten Aufbewahrungsfristen sieben Jahre nicht überschreiten werden. IBM wird damit beginnen, Daten mittels der FIFO-Methode zu löschen, wenn die erfassten Protokoll- und Ereignisdaten die Aufbewahrungsdauer von sieben Jahren überschreiten, ungeachtet der vom Kunden angegebenen Aufbewahrungsfristen.

3.7 Automatisierte Analyse

IBM hat eine proprietäre AI-Analyse-Engine (AI = Automated Intelligence) entwickelt, die Teil des X-Force Protection System ist. Die von den Agenten erfassten Ereignisse und Protokolle werden zur Korrelation und Identifikation an die AI-Analyse-Engine übermittelt. Diese überprüft die Protokolldaten im Hinblick auf statistische Abweichungen, Unregelmäßigkeiten und verdächtige Aktivitäten.

Die AI-Analyse-Engine führt die folgenden Basisfunktionen aus:

- Korrelation von Echtzeit- und Langzeitdaten;
- Nutzung statistischer und regelbasierter Analyseverfahren;
- Nutzung unformatierter, normalisierter und konsolidierter Daten; und
- Bearbeitung der von Anwendungen und Betriebssystemen erzeugten Alarmmeldungen.

Die AI-Alarmbenachrichtigungen des X-Force Protection System werden dem Kunden über das Portal zur Verfügung gestellt. IBM wird dem Kunden eine stündliche Alarmbenachrichtigung des X-Force Protection System per E-Mail zusenden, in der die AI-Alarmbenachrichtigungen zusammengefasst sind, sofern der Kunde diese Option im Portal ausgewählt hat.

Die automatisierte Analyse und die anschließend vom X-Force Protection System erzeugten AI-Alarmbenachrichtigungen sind nur auf den von IBM angegebenen Plattformen verfügbar.

3.7.1 Leistungsumfang

IBM wird

a. die erfassten Ereignisdaten an die AI-Analyse-Engine des X-Force Protection System zur Korrelation und Identifikation übertragen;

b. die von der AI-Analyse-Engine des X-Force Protection System erzeugten maßgeblichen Alarmbenachrichtigungen im Portal anzeigen, sobald sie verfügbar sind; und

c. sofern vom Kunden entsprechend konfiguriert, die Alarmbenachrichtigung des X-Force Protection System innerhalb der Fristen bereitstellen, die im Abschnitt „Service-Level-Agreements“, „Alarmbenachrichtigung bei Sicherheitsverstößen“ dieser Leistungsbeschreibung angegeben sind.

3.7.2 Verantwortlichkeiten des Kunden

Der Kunde wird

a. die Verantwortung dafür übernehmen, die maßgeblichen Regeln der AI-Engine über das Portal zu aktivieren/zu deaktivieren;

b. die Verantwortung dafür übernehmen, die Alarmbenachrichtigung des X-Force Protection System über das Portal auszuwählen; und

c. bestätigen, dass

(1) das Portal zur Überwachung und Prüfung der von der AI-Analyse-Engine des X-Force Protection System erzeugten Alarmbenachrichtigungen verwendet werden kann; und

(2) eine automatisierte Analyse nur auf den von IBM angegebenen Plattformen verfügbar ist.

3.8 Richtlinienmanagement

IBM definiert eine einzelne Änderung der regelbasierten Agentenrichtlinie/-konfiguration als autorisierte Anforderung zum Hinzufügen oder Ändern einer einzigen Regel in einem einzigen Kontext mit höchstens fünf Objekten pro Anforderung. Eine Änderungsanforderung, die das Hinzufügen von sechs oder mehr Objekten oder die Bearbeitung von zwei oder mehr Regeln erfordert, wird als zwei oder mehr Anforderungen gewertet. Bezieht sich die Änderungsanforderung auf Änderungen außerhalb der regelbasierten Agentenrichtlinie, wird jede eingereichte Anforderung als einzelne Änderung betrachtet.

Der Kunde kann den Managed Agent mit einer einzigen globalen Richtlinie konfigurieren, die für alle Ports gilt.

3.8.1 Leistungsumfang

IBM wird

a. eine unbegrenzte Anzahl an Anforderungen einer Richtlinienänderung pro Monat akzeptieren, die von autorisierten Ansprechpartnern für die Sicherheit oder benannten Ansprechpartnern für die Services über das Portal eingereicht wurden;

b. die über das Portal eingereichten Anforderungen einer Richtlinienänderung innerhalb der Fristen bestätigen, die im Abschnitt „Service-Level-Agreements“, „Bestätigung der Anforderung einer Richtlinienänderung“ dieser Leistungsbeschreibung angegeben sind;

c. die eingereichten Anforderungen einer Richtlinienänderung prüfen, um zu verifizieren, dass der Kunde darin alle erforderlichen Informationen angegeben hat;

d. sofern notwendig, den Antragsteller darüber informieren, dass zusätzliche Informationen benötigt werden. Solange diese Informationen nicht zur Verfügung stehen, werden die SLA-Timer angehalten;

e. die Konfiguration der Richtlinienänderung, wie vom Kunden angefordert, vorbereiten und prüfen;

f. angeforderte Richtlinienänderungen innerhalb der Fristen implementieren, die im Abschnitt „Service-Level-Agreements“, „Implementierung einer angeforderten Richtlinienänderung“ dieser Leistungsbeschreibung angegeben sind;

g. eine einzelne Anforderung einer Richtlinienänderung im Notfall pro Monat akzeptieren, die von einem autorisierten Ansprechpartner für die Sicherheit mittels der vereinbarten Verfahren eingereicht wurde;

h. Details der Anforderung einer Richtlinienänderung im IBM MSS-Ticketsystem dokumentieren;

i. den Kunden unverzüglich (telefonisch, per E-Mail oder über das Portal) über die Implementierung einer angeforderten Richtlinienänderung im Notfall informieren;

j. angeforderte Richtlinienänderungen im Notfall innerhalb der Fristen implementieren, die im Abschnitt „Service-Level-Agreements“, „Implementierung einer angeforderten Richtlinienänderung im Notfall“ dieser Leistungsbeschreibung angegeben sind;

k. Tickets zu Anforderungen einer Richtlinienänderung im Portal anzeigen;

l. auf Wunsch des Kunden und gegen Zahlung einer zusätzlichen Gebühr (und abhängig von der Verfügbarkeit von IBM Ressourcen) zusätzliche Richtlinienänderungen durchführen;

m. die Konfiguration des Managed Agent täglich sichern;

n. 14 Konfigurationssicherungen aufbewahren;

o. die aktuelle Konfiguration des Agenten im Portal anzeigen; und

p. auf vierteljährlicher Basis nach schriftlicher Anforderung durch den Kunden

   (1) die Richtlinieneinstellungen des Kunden prüfen, um ihre Richtigkeit zu verifizieren; und

   (2) in Zusammenarbeit mit dem Kunden die von IBM betriebenen Agenten prüfen und Änderungen an der Strategie zum Schutz des Netzwerks empfehlen.

3.8.2 Verantwortlichkeiten des Kunden

Der Kunde wird

a. sicherstellen, dass alle Anforderungen einer Richtlinienänderung von einem autorisierten Ansprechpartner für die Sicherheit oder einem benannten Ansprechpartner für die Services über das Portal gemäß den oben angegebenen Verfahren eingereicht werden;

b. die Anforderung einer Richtlinienänderung eindeutig als Notfall identifizieren, wenn sie im Portal eingereicht wird;

c. das SOC telefonisch kontaktieren, nachdem eine Anforderung einer Richtlinienänderung im Notfall über das Portal eingereicht wurde, um die Anforderung in den Status eines Notfalls hochzustufen;

d. die Verantwortung für die Bereitstellung ausreichender Informationen zu jeder angeforderten Richtlinienänderung übernehmen, um IBM die erfolgreiche Durchführung dieser Änderung zu ermöglichen;

e. die Verantwortung dafür übernehmen, IBM zu benachrichtigen, wenn der Kunde die Durchführung einer vierteljährlichen Richtlinienüberprüfung durch IBM wünscht;

f. die alleinige Verantwortung für die Sicherheitsstrategie des Kunden übernehmen, einschließlich der Verfahren für die Reaktion auf Sicherheitsverstöße; und

g. bestätigen, dass

(1) alle Richtlinienänderungen von IBM und nicht vom Kunden durchgeführt werden;

(2) die Implementierung von Richtlinienänderungen, die nach Ermessen von IBM nachteilige Auswirkungen auf die Fähigkeit der Agenten zum Schutz der Netzwerkumgebung haben, zu einer Aussetzung der anwendbaren SLAs führen wird; und

(3) nicht in Anspruch genommene Änderungen zum Ende eines Kalendermonats verfallen.

3.9 VPN-Unterstützung (Virtual Private Network)

IBM wird mittels einer der folgenden Methoden die vom Kunden gewünschten VPN-Features des Managed Agent aktivieren:

a. Site-to-Site-VPNs zwischen zwei von IBM betriebenen VPN-fähigen Agenten oder zwischen einem von IBM betriebenen Agenten und einem nicht von IBM betriebenen VPN-fähigen Gerät;

b. Client-to-Site-VPNs durch ein Modell, bei dem IBM die Konfiguration festlegt und dem Kunden die Administration der Client-to-Site-VPN-Benutzer ermöglicht; oder

c. SSL-VPNs (Secure Sockets Layer) durch ein Modell, bei dem IBM die Konfiguration festlegt und dem Kunden die Administration der SSL-VPN-Benutzer ermöglicht.

Die Unterstützung für Client-to-Site- und SSL-VPNs ist nur auf den von IBM angegebenen Plattformen verfügbar.

3.9.1 Leistungsumfang

IBM wird

a. bis zu zwei Site-to-Site-VPNs während der Implementierung und Aktivierung jedes Agenten konfigurieren;

b. Unterstützung für statische und dynamische Authentifizierungsmethoden der VPN-Konfiguration bereitstellen;

c. Client-to-Site-VPNs konfigurieren und bis zu fünf Client-to-Site-VPN-Benutzer erstellen und autorisieren;

d. SSL-VPNs konfigurieren und bis zu fünf SSL-VPN-Benutzer erstellen und autorisieren;

e. dem Kunden entsprechende Zugriffsrechte für die Administration seiner Client-to-Site- oder SSL-VPN-Benutzer bereitstellen; und

f. eine Demonstration der Administration von Client-to-Site- oder SSL-VPN-Benutzern für den Kunden durchführen (sofern zutreffend).

3.9.2 Verantwortlichkeiten des Kunden

Der Kunde wird

a. IBM alle erforderlichen Informationen für die Aktivierung der vom Kunden gewünschten VPN-Features bereitstellen;

b. die alleinige Verantwortung für die Erstellung und Administration aller Client-to-Site- und SSL-VPN-Benutzer nach der anfänglichen Aktivierung durch IBM übernehmen; und

c. bestätigen, dass

(1) jedes Site-to-Site-VPN, das der Kunde nach der Implementierung und Aktivierung des Agenten anfordert, zum Kontingent der Richtlinienänderungen des laufenden Monats gerechnet wird;

(2) der Kunde die alleinige Verantwortung für die Beschaffung aller erforderlichen Anwendungen für die Client-to-Site- oder SSL-VPN-Administration beim Hersteller des Agenten und für alle damit verbundenen Kosten trägt;

(3) der Kunde die alleinige Verantwortung für die Unterstützung und Wartung aller erforderlichen Anwendungen für die Client-to-Site- oder SSL-VPN-Administration, die beim Hersteller des Agenten beauftragt werden, und für alle damit verbundenen Kosten trägt;

(4) Client-to-Site-VPN-Lösungen von IBM genehmigt werden müssen; und

(5) die zertifikatbasierte Authentifizierung derzeit im Rahmen der VPN-Konfiguration nicht unterstützt wird.

3.10 Überwachung des Status und der Verfügbarkeit der Managed Agents

IBM wird den Status und die Verfügbarkeit der Managed Agents überwachen. Diese Überwachung soll dazu beitragen, die Verfügbarkeit und Betriebszeiten der Agenten zu erhöhen.

3.10.1 Leistungsumfang

Aktivität 1 – Überwachung

Zweck dieser Aktivität ist die Überwachung des Status und der Leistung der Agenten. IBM MSS wird zur Durchführung dieser Aufgabe entweder die agentenbasierte oder die agentenlose Überwachung einsetzen.

Agentenbasierte Überwachung

Sofern technisch machbar, wird IBM auf in Frage kommenden Agenten Software installieren, um den Systemstatus und die Systemleistung zu überwachen und Messdaten an die SOCs zu melden.

IBM wird

a. bei in Frage kommenden Plattformen Überwachungssoftware auf den Agenten installieren;

b. wichtige Kennzahlen analysieren und entsprechend reagieren. Dazu zählen:

   (1) Festplattenkapazität;

   (2) CPU-Auslastung;

   (3) Speicherauslastung; und

   (4) Prozessverfügbarkeit;

c. auf die von der Überwachungssoftware erzeugten Alarmbenachrichtigungen reagieren.

Agentenlose Überwachung

Wenn die Installation der Überwachungssoftware technisch nicht durchführbar ist, wird IBM den Datenstrom von den Agenten überwachen und/oder administrative Schnittstellen auf den Agenten abfragen.

IBM wird

a. die administrativen Schnittstellen der Agenten überwachen; und/oder

b. den von den Agenten erzeugten Ereignisstrom überwachen; und

c. zusätzliche zeitbasierte Prüfungen initiieren, wenn ein Managed Agent nicht mehr erreichbar ist.

Aktivität 2 – Fehlersuche/-behebung

Zweck dieser Aktivität ist die Durchführung von Recherchen und Untersuchungen, falls die Agenten nicht die erwartete Leistung erbringen oder ein potenzielles Problem mit dem ordnungsgemäßen Betrieb der Agenten festgestellt wird.

IBM wird

a. im Fall eines Problems mit der Leistung eines Agenten oder eines potenziellen Problems mit dem ordnungsgemäßen Betrieb eines Agenten ein Trouble-Ticket erstellen;

b. mit der Recherche und Untersuchung des dokumentierten Problems beginnen;

c. die Konfiguration und Funktionalität des Agenten im Hinblick auf potenzielle Probleme untersuchen, falls der Agent als mögliche Ursache eines netzwerkbezogenen Problems identifiziert wird; und

d. den Agentenstatus und Ausfalltickets im Portal anzeigen.

Aktivität 3 – Benachrichtigung

Zweck dieser Aktivität ist die Benachrichtigung des Kunden, wenn der Agent über In-Band-Standardmethoden nicht mehr erreichbar ist.

IBM wird

a. den Kunden benachrichtigen, wenn der Agent über In-Band-Standardmethoden nicht mehr erreichbar ist. Diese Benachrichtigung erfolgt telefonisch über ein zuvor festgelegtes Verfahren und innerhalb der Frist, die im Abschnitt „Service-Level-Agreements“, „Proaktive Systemüberwachung“ dieser Leistungsbeschreibung angegeben ist;

b. nach Initiierung der telefonischen Benachrichtigung mit der Untersuchung von Problemen im Zusammenhang mit der Konfiguration oder Funktionalität des Agenten beginnen; und

c. den Agentenstatus und Ausfalltickets im Portal anzeigen.

3.10.2 Verantwortlichkeiten des Kunden

Aktivität 1 – Überwachung

Der Kunde wird

a. IBM die Installation der Überwachungssoftware auf allen Managed Agents erlauben, sofern IBM diese Installation für technisch machbar hält; oder

b. IBM die Überwachung der administrativen Schnittstellen und des Ereignisstroms der Managed Agents erlauben, wenn die Installation der Überwachungssoftware auf diesen Agenten technisch nicht machbar ist.

Aktivität 2 – Fehlersuche/-behebung

Der Kunde wird

a. an Besprechungen zur Fehlersuche/-behebung mit IBM teilnehmen (sofern erforderlich);

b. die Verantwortung für die gesamte Remote-Konfiguration und Fehlersuche/-behebung übernehmen, falls der Kunde sich gegen die Implementierung einer Out-of-Band-Lösung entschieden hat oder die Out-of-Band-Lösung aus irgendeinem Grund nicht verfügbar ist; und

c. bestätigen, dass IBM keine weitere Fehlersuche/-behebung durchführen wird, wenn der Managed Agent als Ursache eines gegebenen Problems ausgeschlossen wurde.

Aktivität 3 – Benachrichtigung

Der Kunde wird

a. IBM Informationen zu seiner Benachrichtigungsreihenfolge und Kontaktinformationen zu seinen Ansprechpartnern bereitstellen;

b. IBM innerhalb von drei Kalendertagen über Änderungen an den Kontaktinformationen zu den Ansprechpartnern des Kunden informieren; und

c. sicherstellen, dass ein autorisierter Ansprechpartner für die Sicherheit oder ein für Agentenausfälle zuständiger benannter Ansprechpartner für die Services während 24 Stunden pro Tag an 7 Tagen die Woche erreichbar ist.

3.11 Management von Agenten

Anwendungs- und Sicherheitsupdates für Agenten sind äußerst wichtig für ein Unternehmen. IBM nutzt einen herstellerunabhängigen Ansatz für das Management von Agenten.

3.11.1 Leistungsumfang

IBM wird

a. als alleiniger Anbieter des Softwaremanagements für die Agenten fungieren;

b. den Systemstatus beobachten;

c. Patches und Software-Updates installieren, um die Leistung zu verbessern, zusätzliche Funktionalität zu ermöglichen oder ein Anwendungsproblem zu lösen. IBM übernimmt keine Verantwortung und gibt keine Gewährleistung für Patches, Updates oder Sicherheitsinhalte, die vom jeweiligen Hersteller bereitgestellt werden;

d. vor Updates von Agenten, die möglicherweise Plattformausfallzeiten oder Unterstützung durch den Kunden erfordern, ein Wartungszeitfenster ankündigen; und

e. in der Mitteilung zu diesem Wartungszeitfenster die voraussichtlichen Folgen einer planmäßigen Wartung und die spezifischen Anforderungen des Kunden eindeutig angeben.

3.11.2 Verantwortlichkeiten des Kunden

Der Kunde wird

a. die von IBM angegebenen Hardware-Upgrades durchführen, um die aktuelle Software und Firmware zu unterstützen;

b. Updates von Agenten in Zusammenarbeit mit IBM durchführen (sofern erforderlich);

c. die Verantwortung für alle Gebühren im Zusammenhang mit Hardware-Upgrades übernehmen;

d. sicherstellen, dass gültige Lizenz-, Support- und Wartungsverträge vorliegen;

e. sicherstellen, dass entsprechende Zustimmungen der vom Kunden gewählten Anbieter vorliegen, die es IBM ermöglichen, Support und Wartung im Rahmen bestehender Verträge im Namen des Kunden zu nutzen. Wenn diese Vereinbarungen nicht vorliegen, ist IBM nicht in der Lage, den Anbieter direkt zu kontaktieren, um Supportprobleme zu lösen; und

f. bestätigen, dass

(1) alle Updates per Internet übertragen und eingespielt werden;

(2) Leistungen und/oder SLAs von IBM ausgesetzt werden können, wenn die Zustimmung der Anbieter zu irgendeinem Zeitpunkt während der Vertragslaufzeit nicht eingeholt oder zurückgezogen wird;

(3) die Nichtdurchführung der von IBM geforderten Software-Upgrades zu einer Aussetzung der Serviceerbringung und/oder der SLAs führen kann; und

(4) die Nichtdurchführung der von IBM geforderten Hardware-Upgrades zu einer Aussetzung der Serviceerbringung und/oder der SLAs führen kann.

3.12 Externe Lösungen für die Content-Sicherheit

Der Agent kann dafür konfiguriert werden, eine externe Lösung für die Content-Sicherheit (z. B. eine Webfilter- oder Antivirus-Lösung) auf bestimmten von IBM angegebenen Plattformen zu unterstützen. Die Services unterstützen keine internen Lösungen für die Content-Sicherheit und unterstützen die Kommunikation zwischen der externen Lösung für die Content-Sicherheit und dem Agenten nur in vertretbarem Umfang.

3.12.1 Leistungsumfang

Auf Wunsch des Kunden und ohne Aufpreis wird IBM

a. den Agenten dafür konfigurieren, die Kommunikation zur Unterstützung einer externen Lösung für die Content-Sicherheit auf einer von IBM angegebenen Plattform zu ermöglichen; und

b. gemeinsam mit dem Kunden die Fehlersuche/-behebung bei Problemen im Zusammenhang mit der Kommunikation zwischen dem Agenten und der externen Lösung für die Content-Sicherheit übernehmen.

3.12.2 Verantwortlichkeiten des Kunden

Der Kunde wird

a. IBM ausreichende Informationen zur Herstellung der Kommunikation zwischen dem Agenten und der externen Lösung für die Content-Sicherheit bereitstellen;

b. gemeinsam mit IBM die Fehlersuche/-behebung bei Problemen im Zusammenhang mit der Kommunikation zwischen dem Agenten und der externen Lösung für die Content-Sicherheit übernehmen; und

c. bestätigen dass, der Kunde für die Beschaffung, Unterstützung und Wartung der externen Lösung für die Content-Sicherheit und für alle damit verbundenen Gebühren verantwortlich ist.

3.13 Erstellung von Sicherheitsberichten

Über das Portal erhält der Kunde Zugriff auf Informationen zu den Services und auf Berichtsfunktionen mit individuell anpassbaren Anzeigen der Aktivität auf Unternehmens-, Arbeitsgruppen- und Agentenebene. Das Portal bietet dem Kunden zudem die Möglichkeit, die Erstellung individuell angepasster Berichte zu planen.

3.13.1 Leistungsumfang

IBM wird dem Kunden Zugriff auf die Berichtsfunktionen im Portal gewähren, die Folgendes beinhalten:

a. Anzahl der aufgerufenen und eingehaltenen SLAs;

b. Anzahl, Art und Zusammenfassung von Serviceanforderungen/-tickets; und

c. Firewall-Berichte, die eine Zusammenfassung, eine Datenverkehrsanalyse, die Protokollnutzung, die Ziel-IP und die Nutzung von Regeln dokumentieren.

3.13.2 Verantwortlichkeiten des Kunden

Der Kunde wird

a. Berichte zu den Services über das Portal erstellen; und

b. die Verantwortung für die Planung von Berichten übernehmen (sofern zutreffend).

4. Optionale Services

Die vom Kunden ausgewählten optionalen Services und die dafür anfallenden zusätzlichen Gebühren werden im Bestellschein angegeben.

4.1 Cold Standby

Cold Standby ist eine Disaster-Recovery-Methode, bei der ein zusätzlicher Agent als Ersatz für den Fall eines Hardware- und/oder Softwareausfalls beim primären Agenten zur Verfügung steht. Cold-Standby-Agenten sind nicht eingeschaltet oder betriebsbereit und enthalten keine aktive Konfiguration, Richtlinie oder Content-Updates.

4.1.1 Leistungsumfang

Auf Wunsch des Kunden und ohne Aufpreis wird IBM

a. bei einem Ausfall des primären Agenten den Cold-Standby-Agenten in Zusammenarbeit mit dem Kunden in den Produktionsbetrieb überführen und auf „active“ einstellen;

b. bei einem Ausfall des primären Agenten die erforderlichen Content-Updates auf dem Cold-Standby-Agenten einspielen; und

c. bei einem Ausfall des primären Agenten die aktive aktuelle Konfiguration auf dem Cold-Standby-Agenten einspielen.

4.1.2 Verantwortlichkeiten des Kunden

Der Kunde wird

a. einen sekundären Agenten bereitstellen, der als Cold-Standby-Agent fungieren wird;

b. sicherstellen, dass gültige Lizenz-, Support- und Wartungsverträge für den Cold-Standby-Agenten vorliegen;

c. bei einem Ausfall des primären Agenten den Cold-Standby-Agenten in Zusammenarbeit mit IBM in den Produktionsbetrieb überführen und auf „active“ einstellen; und

d. bestätigen, dass

(1) Cold-Standby-Agenten nicht von IBM betrieben und gewartet werden, es sei denn, ihr Status wird in „active“ geändert;

(2) Konfigurationsänderungen an Cold-Standby-Agenten vorgenommen werden müssen, um deren Status in „active“ zu ändern; und

(3) Cold-Standby-Agenten keinen Datenverkehr zu den SOCs erzeugen dürfen, es sei denn, der primäre Agent ist ausgefallen und der Cold-Standby-Agent wurde in den Produktionsbetrieb überführt und auf „active“ eingestellt.

4.2 Warm Standby

Warm Standby ist eine Methode der Redundanz, die Ausfallzeiten aufgrund von Hardware- und/oder Softwareausfällen bei Agenten reduzieren kann. Im Rahmen der Option „Warm Standby“ wird IBM einen einzelnen Ersatzagenten für den Kunden betreiben und auf dem aktuellen Stand halten. Bei einem Ausfall des primären Agenten des Kunden steht der Ersatz- bzw. Warm-Standby-Agent zur Verfügung, um die Services schneller wiederherzustellen. Ein Standby-Agent darf keinen Datenverkehr zu den SOCs erzeugen, es sei denn, er wird in den Produktionsbetrieb überführt und auf „active“ eingestellt.

IBM empfiehlt nachdrücklich die Verwendung des Out-of-Band-Zugriffs auf den Warm-Standby-Agenten, wie im Abschnitt „Out-of-Band-Zugriff“ dieser Leistungsbeschreibung beschrieben.

4.2.1 Leistungsumfang

Auf Wunsch des Kunden und gegen Zahlung einer im Bestellschein angegebenen zusätzlichen Gebühr wird IBM

a. den ordnungsgemäßen Betrieb und die Verfügbarkeit des Warm-Standby-Agenten sicherstellen, wie im Abschnitt „Überwachung des Status und der Verfügbarkeit der Managed Agents“ dieser Leistungsbeschreibung beschrieben;

b. Content-Updates auf dem Warm-Standby-Agenten einspielen, wie im Abschnitt „Management von Agenten“ dieser Leistungsbeschreibung beschrieben; und

c. bei einem Ausfall des primären Agenten den Status des Warm-Standby-Agenten in „active“ ändern.

4.2.2 Verantwortlichkeiten des Kunden

Der Kunde wird

a. sicherstellen, dass gültige Lizenz-, Support- und Wartungsverträge für alle Warm-Standby-Plattformen vorliegen;

b. die Verantwortung für alle Gebühren im Zusammenhang mit dem fortlaufenden Management des Warm-Standby-Agenten übernehmen;

c. sekundäre IP-Adressen bereitstellen;

d. die Verantwortlichkeiten des Kunden erfüllen, die im Abschnitt „Überwachung des Status und der Verfügbarkeit der Managed Agents“ dieser Leistungsbeschreibung beschrieben sind;

e. die Verantwortlichkeiten des Kunden erfüllen, die im Abschnitt „Management von Agenten“ dieser Leistungsbeschreibung definiert sind;

f. bestätigen, dass

(1) Richtlinienänderungen, die am primären Agenten vorgenommen wurden, nicht auf dem Warm-Standby-Agenten widergespiegelt werden; und

(2) Standby-Agenten keinen Datenverkehr zu den SOCs erzeugen dürfen, es sei denn, sie wurden in den Produktionsbetrieb überführt und auf „active“ eingestellt;

g. die Verantwortung für die gesamte Remote-Konfiguration und Fehlersuche/-behebung übernehmen, falls sich der Kunde gegen die Implementierung einer Out-of-Band-Lösung entscheidet oder die Out-of-Band-Lösung aus irgendeinem Grund nicht verfügbar ist.

4.3 Hochverfügbarkeit

Um Schutz vor Hardware- und/oder Softwareausfällen und hohe Verfügbarkeit zu erreichen, können zwei Managed Agents konfiguriert und implementiert werden, von denen einer voll einsatzfähig ist und der andere als Ersatz bereitgehalten wird und erst bei einem Ausfall des ersten Agenten zum Einsatz kommt. Einige Agenten können auch in einem Cluster konfiguriert werden, in dem mehrere Agenten die Netzlast gemeinsam verarbeiten.

Aktiv/Passiv-Implementierungen

In dieser Konfiguration wird ein zweiter Agent konfiguriert, der bereit für den Einsatz im Netzwerk ist, falls es bei dem primären Agenten zu einem kritischen Hardware- oder Softwareausfall kommt. Die Verarbeitung wird in diesem Szenario automatisch und sofort an den zweiten Agenten übertragen.

Aktiv/Aktiv-Implementierungen

In einem Aktiv/Aktiv-Cluster werden zwei oder mehr Agenten zur gleichzeitigen Verarbeitung des Datenverkehrs im Netzwerk eingesetzt. In dieser Konfiguration verarbeitet jeder Agent einen Teil der Netzwerkpakete, gesteuert von einem Algorithmus für den Lastausgleich. Beim Ausfall eines Agenten wird der gesamte Datenverkehr von dem/den übrigen Agenten übernommen, bis der ausgefallene Agent wiederhergestellt ist.

IBM empfiehlt nachdrücklich die Verwendung des Out-of-Band-Zugriffs auf alle Agenten in der Hochverfügbarkeitskonfiguration, wie im Abschnitt „Out-of-Band-Zugriff“ dieser Leistungsbeschreibung beschrieben.

4.3.1 Leistungsumfang

Auf Wunsch des Kunden und gegen Zahlung einer im Bestellschein angegebenen zusätzlichen Gebühr wird IBM

a. einen sekundären Agenten konfigurieren, entweder in einer Aktiv/Passiv- oder Aktiv/Aktiv-Konfiguration, wie vom Kunden angegeben;

b. Aktiv/Aktiv-Konfigurationen konfigurieren, die drei oder mehr Agenten (Cluster) im Unicast-Modus verwenden (Unicast-Modus bedeutet, dass ein einzelner Absender und ein einzelner Empfänger über ein Netzwerk miteinander kommunizieren);

Anmerkung: IBM unterstützt keine Aktiv/Aktiv-Konfigurationen im Multicast-Modus.

c. die Hochverfügbarkeitslösung betreiben und überwachen;

d. den ordnungsgemäßen Betrieb und die Verfügbarkeit des sekundären Agenten sicherstellen, wie im Abschnitt „Überwachung des Status und der Verfügbarkeit der Managed Agents“ dieser Leistungsbeschreibung beschrieben;

e. Content-Updates auf dem/den sekundären Agenten einspielen, wie im Abschnitt „Management von Agenten“ dieser Leistungsbeschreibung beschrieben; und

f. die Richtlinie des sekundären Agenten aktualisieren, wie im Abschnitt „Richtlinienmanagement“ dieser Leistungsbeschreibung beschrieben.

4.3.2 Verantwortlichkeiten des Kunden

Der Kunde wird

a. einen sekundären Agenten bereitstellen;

b. alle erforderlichen Änderungen an der Softwarelizenzierung vornehmen;

c. sekundäre IP-Adressen bereitstellen;

d. die Verantwortung für alle Gebühren im Zusammenhang mit dem fortlaufenden Management des sekundären Agenten übernehmen;

e. die Verantwortlichkeiten des Kunden erfüllen, die in den folgenden Abschnitten dieser Leistungsbeschreibung definiert sind:

(1) „Überwachung des Status und der Verfügbarkeit der Managed Agents“;

(2) „Management von Agenten“;

(3) „Richtlinienmanagement“;

f. die Verantwortung für die gesamte Remote-Konfiguration und Fehlersuche/-behebung übernehmen, falls sich der Kunde gegen die Implementierung einer Out-of-Band-Lösung auf dem primären und sekundären Agenten entscheidet oder die Out-of-Band-Lösung aus irgendeinem Grund nicht verfügbar ist; und

g. bestätigen, dass

(1) die Services keine nicht integrierten Hochverfügbarkeitslösungen unterstützen; und

(2) IBM Aktiv/Aktiv-Konfigurationen, die drei oder mehr Agenten nutzen, nur im Unicast-Modus unterstützt.

4.4 Aggregator am Kundenstandort

Der Aggregator am Kundenstandort (nachfolgend „Onsite Aggregator“ oder „OA“ genannt) ist ein vom Kunden bereitgestelltes Gerät, das am Kundenstandort implementiert wird. Der Zweck des OA besteht darin, die Erfassung von Protokoll- und Sicherheitsereignisdaten zu zentralisieren, wenn der Kunde die IBM Managed Security Services für mehrere Agenten nutzt, und diese Daten sicher an die IBM MSS-Infrastruktur zu übertragen, in der sie weiter verarbeitet und langfristig aufbewahrt werden.

Die Basisfunktionen des OA sind nachstehend beschrieben:

a. Kompilierung oder anderweitige Zusammenfassung der Sicherheitsereignisse und Protokolldaten;

b. Komprimierung der Sicherheitsereignisse und Protokolldaten;

c. Verschlüsselung der Sicherheitsereignisse und Protokolldaten; und

d. Übertragung der Sicherheitsereignisse und Protokolldaten an die IBM MSS-Infrastruktur.

Die Kernfunktionen des OA sind nachstehend beschrieben:

a. Durchführung des lokalen Spoolings, indem die Ereignisse lokal in die Warteschlange gestellt werden, wenn keine Verbindung zur IBM MSS-Infrastruktur verfügbar ist;

b. Durchführung der unidirektionalen Protokollübertragung. Die OA-Kommunikation wird über abgehende SSL/TCP-443-Verbindungen ausgeführt;

c. Durchführung der Nachrichtendrosselung bei entsprechender Konfiguration. Dadurch wird die Zahl der vom OA zur IBM MSS-Infrastruktur übertragenen Nachrichten pro Sekunde eingeschränkt, um Bandbreite zu sparen; und

d. Bereitstellung von Übertragungszeitfenstern bei entsprechender Konfiguration. Die Übertragungszeitfenster aktivieren/deaktivieren die Ereignisübertragung an die IBM MSS-Infrastruktur während des vom Kunden im Portal angegebenen Zeitrahmens.

IBM empfiehlt nachdrücklich die Verwendung des Out-of-Band-Zugriffs auf den OA, wie im Abschnitt „Out-of-Band-Zugriff“ dieser Leistungsbeschreibung beschrieben.

4.4.1 Leistungsumfang

Auf Wunsch des Kunden und gegen Zahlung einer im Bestellschein angegebenen zusätzlichen Gebühr wird IBM die im Folgenden beschriebenen Leistungen erbringen.

Aktivität 1 – Konfiguration

Zweck dieser Aktivität ist die Konfiguration des OA.

IBM wird

a. den Kunden per Telefon und E-Mail dabei unterstützen, Dokumente des jeweiligen Herstellers zu finden, die eine genaue Beschreibung der Installations- und Konfigurationsverfahren für das OA-Betriebssystem und die von IBM bereitgestellte OA-Software enthalten. Diese Unterstützung muss im Voraus geplant werden, um sicherzustellen, dass ein IBM Spezialist für die Implementierung zur Verfügung steht;

b. dem Kunden Hardwarespezifikationen für die OA-Plattform bereitstellen;

c. dem Kunden OA-Software und Konfigurationseinstellungen bereitstellen;

d. den Kunden per Telefon und E-Mail bei der Installation der von IBM bereitgestellten OA-Software auf der vom Kunden bereitgestellten Hardwareplattform unterstützen. Diese Unterstützung muss im Voraus geplant werden, um sicherzustellen, dass ein IBM Spezialist für die Implementierung zur Verfügung steht;

e. auf Wunsch des Kunden und gegen Zahlung einer im Bestellschein angegebenen zusätzlichen Gebühr Leistungen für die Softwareinstallation erbringen; und

f. beim Einsatz vorhandener Plattformen

(1) vorhandene Hardwarekonfigurationen prüfen, um sicherzustellen, dass sie den IBM Spezifikationen entsprechen; und

(2) erforderliche Hardware-Upgrades ermitteln, die vom Kunden bereitzustellen und zu installieren sind.

Aktivität 2 – Installation

Zweck dieser Aktivität ist die Installation des OA.

IBM wird

a. den Kunden per Telefon und E-Mail dabei unterstützen, Dokumente des jeweiligen Herstellers zu finden, die eine genaue Beschreibung der Verfahren für die physische Installation und der Verkabelung des OA enthalten. Diese Unterstützung muss im Voraus geplant werden, um sicherzustellen, dass ein IBM Spezialist für die Implementierung zur Verfügung steht;

Anmerkung: Der Kunde kann Leistungen für die physische Verkabelung und Installation im Rahmen eines gesonderten Vertrags bei IBM beauftragen.

b. den OA per Fernzugriff konfigurieren. Dabei wird IBM den OA in der IBM MSS-Infrastruktur registrieren und den Prozess für die Übernahme der Implementierung und des Managements des OA initiieren; und

c. bestätigen, dass die IBM MSS-Infrastruktur Daten vom OA empfängt.

Aktivität 3 – Fortlaufendes Management und kontinuierliche Unterstützung

Zweck dieser Aktivität ist das fortlaufende Management und die kontinuierliche Unterstützung des OA.

IBM wird

a. den OA in den SOCs auf „active“ einstellen, um die kontinuierliche Unterstützung und das fortlaufende Management durch die SOCs zu aktivieren;

b. den ordnungsgemäßen Betrieb und die Verfügbarkeit des OA sicherstellen, wie im Abschnitt „Überwachung des Status und der Verfügbarkeit der Managed Agents“ dieser Leistungsbeschreibung beschrieben;

c. Software-Updates auf dem OA einspielen, wie im Abschnitt „Management von Agenten“ dieser Leistungsbeschreibung beschrieben; und

d. die Verantwortung für das Management und die Überwachung des OA für die Dauer der Vertragslaufzeit und jeder Verlängerungslaufzeit übernehmen.

4.4.2 Verantwortlichkeiten des Kunden

Aktivität 1 – Konfiguration

Der Kunde wird

a. IBM eine externe IP-Adresse für den OA bereitstellen;

b. die Hardware für die OA-Plattform bereitstellen, basierend auf den Empfehlungen und Anforderungen von IBM;

c. die von IBM bereitgestellte OA-Software nach Anleitung von IBM auf der vom Kunden bereitgestellten Hardware installieren;

d. eine externe IP-Adresse und die zugehörige Einstellung auf dem OA konfigurieren;

e. IBM die IP-Adresse des OA, den Hostnamen, die Maschinenplattform, die Anwendungsversion und die Zeitzone des Agenten bereitstellen; und

f. beim Einsatz vorhandener Plattformen die von IBM geforderten Hardware-Upgrades beschaffen und installieren.

Aktivität 2 – Installation

Der Kunde wird

a. die Verantwortung für die physische Installation und Verkabelung des OA übernehmen; und

b. die Unterstützung mit einem IBM Spezialisten für die Implementierung planen.

Aktivität 3 – Fortlaufendes Management und kontinuierliche Unterstützung

Der Kunde wird

a. die Verantwortung für die Beschaffung und Installation der erforderlichen Hardware-Upgrades für die OA-Plattform für die Dauer der Vertragslaufzeit übernehmen;

b. die Verantwortlichkeiten des Kunden erfüllen, die im Abschnitt „Überwachung des Status und der Verfügbarkeit der Managed Agents“ dieser Leistungsbeschreibung beschrieben sind; und

c. die Verantwortlichkeiten des Kunden erfüllen, die im Abschnitt „Management von Agenten“ dieser Leistungsbeschreibung beschrieben sind.

4.5 Integration des Ticketsystems

Wenn der Kunde ein vorhandenes Trouble-Ticket- und Incident-Management-System nutzen möchte, um seine Investitionen zu schützen, wird IBM eine Anwendungsprogrammierschnittstelle (API) bereitstellen, die die individuell angepasste Integration mit externen Ticketsystemen erlaubt.

4.5.1 Leistungsumfang

Auf Wunsch des Kunden und gegen Zahlung einer im Bestellschein angegebenen zusätzlichen Gebühr wird IBM eine API bereitstellen, um die individuell angepasste Integration mit externen Ticketsystemen zu ermöglichen.

4.5.2 Verantwortlichkeiten des Kunden

Der Kunde wird

a. die Verantwortung für alle zusätzlichen Gebühren im Zusammenhang mit der API für die Ticketintegration übernehmen;

b. das Portal-API-Paket nutzen, um die Ticketintegration zu ermöglichen;

c. die Verantwortung für alle technischen und entwicklungsspezifischen Probleme im Zusammenhang mit der Ticketintegration übernehmen; und

d. bestätigen, dass IBM keine Unterstützung oder Beratung für die Integration des Ticketsystems des Kunden bereitstellen wird.

4.6 Bereitstellung von Sicherheitsereignissen und -protokollen

Auf Wunsch des Kunden wird IBM Protokoll- und Ereignisdaten aus der IBM MSS-Infrastruktur abrufen und zum Download von einem sicheren IBM Server bereitstellen. In Fällen, in denen die Menge der Protokoll- und Ereignisdaten nach Ermessen von IBM zu groß ist, um per Download bereitgestellt zu werden, wird IBM die Daten auf verschlüsselten Datenträgern speichern und an einen vom Kunden angegebenen Standort liefern. IBM wird von Fall zu Fall entscheiden, ob die Bereitstellung per Download machbar ist oder nicht.

4.6.1 Leistungsumfang

Auf Wunsch des Kunden und gegen Zahlung einer im Bestellschein angegebenen zusätzlichen Gebühr wird IBM

a. die angegebenen Daten aus der IBM MSS-Infrastruktur abrufen und dem Kunden zum Download auf einem sicheren IBM Server bereitstellen, sofern vom Kunden über das Portal angefordert; und

b. den Kunden über zusätzliche Gebühren für sämtlichen Zeit- und Materialaufwand informieren, der für das Abrufen und Vorbereiten der Daten anfällt.

4.6.2 Verantwortlichkeiten des Kunden

Der Kunde wird

a. die Bereitstellung von Sicherheitsereignis- und Protokolldaten über das Portal anfordern;

b. die gewünschten Daten von einem sicheren IBM Server downloaden;

c. bestätigen, dass die Daten möglicherweise auf verschlüsselten Datenträgern gespeichert und an einen vom Kunden angegebenen Standort geliefert werden müssen, wenn die Menge der angeforderten Daten zu groß für einen Download ist; und

d. die Verantwortung für alle Gebühren auf Zeit- und Materialbasis und alle Versandkosten (sofern zutreffend) im Zusammenhang mit der Bereitstellung von Protokolldaten übernehmen.

5. Service-Level-Agreements

IBM Service-Level-Agreements (SLAs) legen Reaktionszeiten und Gegenmaßnahmen bei bestimmten Ereignissen, die sich aus den Services ergeben, fest. Die SLAs werden wirksam, wenn der Implementierungsprozess abgeschlossen ist, der Agent auf „active“ eingestellt wurde und die

Unterstützung und das Management des Agenten erfolgreich an die SOCs übertragen wurden. SLA-Gutschriften sind unter der Voraussetzung verfügbar, dass der Kunde seine in dieser Leistungsbeschreibung und allen zugehörigen Vertragsdokumenten definierten Verpflichtungen erfüllt.

5.1 SLA-Verfügbarkeit

Die im Folgenden beschriebenen SLA-Standardwerte beinhalten die erfassten Kennzahlen für die Erbringung der Services. Sofern nicht nachstehend ausdrücklich anders angegeben, gelten keinerlei Gewährleistungen für die im Rahmen dieser Leistungsbeschreibung erbrachten Services. Der einzige Anspruch des Kunden auf Kompensation bei Nichteinhaltung der vereinbarten SLA-Standardwerte ist im Abschnitt „SLA-Gutschriften“ dieser Leistungsbeschreibung angegeben.

a. Alarmbenachrichtigung bei Sicherheitsverstößen – Hat der Kunde die Alarmbenachrichtigung des X-Force Protection System im Portal konfiguriert und wurde ein Alarm erzeugt, wird IBM dem benannten Ansprechpartner für die Services eine stündliche Benachrichtigung per E-Mail zusenden, in der AI-Alarmbenachrichtigungen des X-Force Protection System zusammengefasst sind. Dieses SLA gilt nur für das erste Senden der Alarmbenachrichtigung des X-Force Protection System, nicht für die bestätigte Übermittlung an den/die Endempfänger.

   Zum Zweck der Klarstellung wird darauf hingewiesen, dass nur dann eine E-Mail-Benachrichtigung gesendet wird, wenn ein Alarm während der vorhergehenden Stunde erzeugt wurde.

b. Bestätigung der Anforderung einer Richtlinienänderung – IBM wird den Erhalt einer vom Kunden übermittelten Anforderung einer Richtlinienänderung innerhalb von zwei Stunden nach Eingang bestätigen. Dieses SLA ist nur für Anforderungen einer Richtlinienänderung verfügbar, die durch einen autorisierten Ansprechpartner für die Sicherheit oder einen benannten Ansprechpartner für die Services gemäß den im Portal dokumentierten Verfahren eingereicht wurden.

c. Implementierung einer angeforderten Richtlinienänderung – IBM wird eine vom Kunden angeforderte Richtlinienänderung innerhalb von 8 Stunden nach Eingang der Änderungsanforderung implementieren, es sei denn, die Anforderung wurde in den Status „hold“ versetzt, da die vom Kunden bereitgestellten Informationen für die Implementierung der angeforderten Richtlinienänderung nicht ausreichen. Dieses SLA ist nur für Anforderungen einer Richtlinienänderung verfügbar, die durch einen autorisierten Ansprechpartner für die Sicherheit oder einen benannten Ansprechpartner für die Services gemäß den im Portal dokumentierten Verfahren eingereicht wurden.

d. Implementierung einer angeforderten Richtlinienänderung im Notfall – IBM wird eine vom Kunden angeforderte Richtlinienänderung im Notfall innerhalb von zwei Stunden implementieren, nachdem der Kunde sie telefonisch als Notfall deklariert hat, nachdem die Änderungsanforderung über das Portal eingereicht wurde. Dieses SLA ist nur für Anforderungen einer Richtlinienänderung verfügbar, die durch einen autorisierten Ansprechpartner für die Sicherheit oder einen benannten Ansprechpartner für die Services gemäß den im Portal dokumentierten Verfahren eingereicht wurden.

e. Proaktive Systemüberwachung – IBM wird den Kunden innerhalb von 15 Minuten benachrichtigen, nachdem IBM festgestellt hat, dass der Agent des Kunden über In-Band-Standardverbindungen nicht erreichbar ist.

Nachfolgend genannte Service-Level-Ziele werden lediglich angestrebt. Im Falle des Nichterreichens dieser Service-Level-Ziele wird IBM in Abstimmung mit dem Kunden Maßnahmen zur Verbesserung der Verfügbarkeit der Services bzw. der Erreichbarkeit des Portals einleiten. Ein Anspruch auf Erteilung einer Service-Level-Gutschrift besteht nicht.

a. Verfügbarkeit der Services – IBM wird eine angestrebte Serviceverfügbarkeit von 100 % für die SOCs bieten.

b. Verfügbarkeit des Portals – IBM wird eine angestrebte Erreichbarkeit des Portals von 99,9 % außerhalb der im Abschnitt „Geplante und im Notfall durchgeführte Portalwartung“ in den Allgemeinen Bedingungen für IBM Managed Security Services angegebenen Zeiten bieten.

5.2 SLA-Gutschriften

a. Service-Level-Gutschriften bei Nichteinhaltung folgender SLAs: Alarmbenachrichtigung bei Sicherheitsverstößen, Bestätigung der Anforderung einer Richtlinienänderung, Implementierung einer angeforderten Richtlinienänderung, Implementierung einer angeforderten Richtlinienänderung im Notfall, proaktive Systemüberwachung – Falls IBM eines dieser SLAs nicht einhält, wird IBM dem Kunden eine Service-Level-Gutschrift in Höhe von 1/30 der monatlichen Überwachungsgebühr für den betroffenen Agenten, bei dem das jeweilige SLA nicht erfüllt wurde, als pauschalierten Schadensersatz gutschreiben. Mit Zahlung bzw.

Verrechnung der Service-Level-Gutschrift sind alle Ansprüche aus der Nichteinhaltung vereinbarter SLAs abschließend abgegolten.

Zusammenfassung der SLAs und SLA-Gutschriften

Service-Level-Agreements	SLA-Gutschriften
Alarmbenachrichtigung bei Sicherheitsverstößen	Service-Level-Gutschrift, 1/30 der monatlichen Überwachungsgebühr für den betroffenen Agenten
Bestätigung der Anforderung einer Richtlinienänderung	
Implementierung einer angeforderten Richtlinienänderung	
Implementierung einer angeforderten Richtlinienänderung im Notfall	
Proaktive Systemüberwachung	