Leistungsbeschreibung

IBM Managed Security Services (Cloud Computing) – Hosted Vulnerability Management

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 Managed Security Services (Cloud Computing) – Hosted Vulnerability Management (nachfolgend „VMS“ (Vulnerability Management Service) oder „Services“ genannt) ist die Erbringung eines Service für die Überprüfung auf Schwachstellen, der dem Kunden die notwendigen Tools zur Erfüllung verschiedener Anforderungen bereitstellt (z. B. zur Unterstützung der internen Prüfung und Risikobewertung des Kunden sowie der Einhaltung gesetzlicher und branchenspezifischer Bestimmungen). Der VMS beinhaltet ein umfangreiches Funktionsspektrum. Wenn der Kunde jedoch Berichte durch einen von der Payment Card Industry (PCI) zertifizierten Approved Scanning Vendor (ASV) wünscht, muss er ausdrücklich anfordern, dass eine entsprechende Umgebung für ihn konfiguriert wird.

IBM stellt den VMS als eine Lösung bereit, die vom Kunden betrieben wird. Das bedeutet, IBM stellt die Anwendung für die Schwachstellenüberprüfung und technische Unterstützung für die Anwendung bereit; für den Betrieb der Services und die aus den Services abgeleiteten Ergebnisse ist jedoch der Kunde verantwortlich.

Entscheidungen darüber, welche Schwachstellen durch den VMS erkannt werden sollen, liegen im alleinigen Ermessen von IBM. Diese Entscheidungen basieren darauf, wie gravierend und häufig eine Schwachstelle ist, ob der VMS die Schwachstelle sicher erkennen kann und wie hoch die Priorität der Schwachstelle im Vergleich zu anderen abgedeckten Sicherheitsbedrohungen ist.

Der VMS bietet zwei unterschiedliche Arten der Schwachstellenüberprüfung, die zusammen oder getrennt ausgeführt werden können:

- Extern – IBM hostet und betreibt Schwachstellenscanner im Internet. Diese können verwendet werden, um die öffentlich zugänglichen IP-Adressen und Webanwendungen des Kunden zu überprüfen. Sie sind für die Erkennung von Schwachstellen konzipiert, die das Unternehmen anfällig für Sicherheitsrisiken aus dem Internet machen.
- Intern – Der Kunde kann den Status von Sicherheitsschwachstellen in seinem Unternehmensnetzwerk mit einem von IBM betriebenen und am Kundenstandort installierten Gerät für die Schwachstellenüberprüfung (nachfolgend „Agent“ oder „Managed Agent“ genannt) analysieren. 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.

Approved Scanning Vendor (ASV) ist ein Anbieter einer Lösung für die Schwachstellenüberprüfung, der vom PCI SSI (Payment Card Industry Security Standards Council) anerkannt ist. ASVs erbringen

Services für Unternehmen, die sich an die Datensicherheitsstandards der Payment Card Industry (PCI) halten müssen.

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.

Externe Schwachstellenüberprüfung ist eine Suche nach Schwachstellen, die von einem IBM Schwachstellenscanner außerhalb der physischen Umgebung des Kunden durchgeführt wird. Externe Schwachstellenüberprüfungen simulieren die Sichtweise eines externen Angreifers (z. B. eines Hackers, der versucht, aus dem öffentlichen Internet auf die Umgebung des Kunden zuzugreifen).

Interne Schwachstellenüberprüfung ist eine Suche nach Schwachstellen, die von einem am Standort des Kunden installierten Gerät zur Schwachstellenüberprüfung durchgeführt wird. Interne Schwachstellenüberprüfungen können eine gründlichere Analyse von Zielmaschinen ermöglichen, da sie Störungen durch Firewalls und andere Sicherheitskomponenten während der Überprüfung vermeiden.

PCI SSC (Payment Card Industry Security Standards Council) ist die Organisation, die für die Festlegung der Datensicherheitsstandards für Unternehmen, die Kreditkartendaten verarbeiten, verantwortlich ist.

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-Level-Ziele
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
Alarmausgabe zum Status von Agenten	15 Minuten	SLA für die proaktive Systemüberwachung
Anzahl/Häufigkeit von externen/internen Schwachstellenüberprüfungen	unbegrenzt	nicht zutreffend
Durchführung einer Schwachstellenüberprüfung	Innerhalb +/- 1 Stunde	SLA für die Durchführung einer Schwachstellenüberprüfung
Servicemerkmale der PCI ASV Services	**Messgröße oder Anzahl**	**Service-Level-Agreements**
Anforderung einer Änderung des Umfangs von PCI-Überprüfungen	unbegrenzt	nicht zutreffend
Bestätigung der Anforderung einer Änderung des Umfangs von PCI-Überprüfungen	2 Stunden	SLA für die Bestätigung der Anforderung einer Änderung des Umfangs von PCI-Überprüfungen

Implementierung einer angeforderten Änderung des Umfangs von PCI-Überprüfungen	72 Stunden	SLA für die Implementierung einer angeforderten Änderung des Umfangs von PCI-Überprüfungen
Anforderung einer Prüfung von Ausnahmen von PCI-Schwachstellen	unbegrenzt	nicht zutreffend
Beantwortung der Anforderung einer Prüfung von Ausnahmen von PCI-Schwachstellen	72 Stunden	SLA für die Beantwortung der Anforderung einer Prüfung von Ausnahmen von PCI-Schwachstellen
Konformitätsbescheinigung durch den PCI ASV	eine pro Quartal	nicht zutreffend

3.1 Security Operations Centers

IBM Managed Security Services 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) Standardprüfvorlagen und -berichtsvorlagen;
   (2) Informationen über und Warnung bei Sicherheitsbedrohungen;
   (3) Informationen über 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 Prüfergebnisse;
   (8) Berechtigung zum Download von Daten; und
   (9) 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 und weiteren zu liefernden Materialien, z. B. Prüf- und Ergebnisberichten;

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. Zugriff auf das Portal bereitstellen, einschließlich folgender Möglichkeiten (sofern passend):
   (1) Übermittlung von Serviceanforderungen an die SOCs;
   (2) „Live Chat“ mit einem SOC-Analysten in Bezug auf bestimmte Vorfälle oder Tickets, die im Rahmen der Services erstellt wurden;
   (3) Erstellung interner Tickets im Zusammenhang mit den Services und Zuordnung dieser Tickets zu den Portalbenutzern;
   (4) Abfrage, Anzeige und Aktualisierung von Tickets im Zusammenhang mit den Services;
   (5) Erstellung und Änderung individuell angepasster Prüfvorlagen (ausgenommen PCI-Vorlagen);
   (6) Erstellung und Änderung individuell angepasster Berichtsvorlagen (ausgenommen PCI-Berichte);
   (7) Anforderung von Ausnahmen von Schwachstellen;
   (8) Prüfung und Genehmigung von Ausnahmen von Schwachstellen (ausgenommen PCI-Ausnahmen);
   (9) Festlegung von Sites für die Schwachstellenüberprüfung (IP-Adressen und Webdomänen, die in den Umfang der Überprüfung aufgenommen werden sollen) sowie der Benutzer und Richtlinien im Zusammenhang mit der Site (ausgenommen Umfang der PCI-Überprüfung);
   (10) Planung und Ausführung von Überprüfungen; und
   (11) Planung und Ausführung von Berichten;
b. Portalbenutzer mittels eines statischen Kennworts authentifizieren; und
c. 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 dieser Leistungsbeschreibung 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 die Services konfigurieren und, sofern zutreffend, Agenten für die interne Schwachstellenüberprüfung implementieren.

Anmerkung: Die Aktivitäten im Rahmen der Implementierung und Aktivierung werden einmal während der Erbringung der Leistungen durchgeführt. Wenn der Kunde seine/n Agenten während der Laufzeit des Servicevertrags austauscht, aufrüstet oder an einen anderen Standort verlegt, kann IBM verlangen, dass dieser Agent/diese Agenten erneut implementiert und aktiviert wird/werden (nachfolgend „erneute Implementierung“ genannt). Solche erneuten Implementierungen werden gegen Zahlung einer im Bestellschein 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, sofern zutreffend. IBM wird dem Kunden eine Begrüßungsmail zusenden und (sofern zutreffend) 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 – Hardwarevoraussetzungen für den Agenten für die interne Schwachstellenüberprüfung

Zweck dieser Aktivität ist die Festlegung der Voraussetzungen für das/die Gerät/e für die interne Schwachstellenüberprüfung, das/die am Kundenstandort installiert wird/werden.

IBM wird

a. dem Kunden das Dokument „Customer Premise (CPE) Vulnerability Scanner Setup Instructions“ übergeben, das Folgendes beschreibt:

   (1) Spezifikationen für die Hardware, die der Kunde bereitstellen muss; und

   (2) Schritte, die der Kunde durchführen muss, um die Geräte für die interne Schwachstellenüberprüfung, die im Rahmen der Services verwendet werden sollen, zu konfigurieren und zu installieren;

b. dem Kunden Zugriff auf das Software-Image, einschließlich Betriebssystem und Software für die Überprüfung, gewähren, das auf der vom Kunden bereitgestellten Hardware eingespielt wird.

Beendigung der Leistungen:

Die IBM Verpflichtungen im Rahmen dieser Aktivität sind erfüllt, wenn das Dokument „Customer Premise (CPE) Vulnerability Scanner Setup Instructions“ an den Beauftragten des Kunden übergeben wurde.

Zu liefernde Materialien:

- Dokument „Customer Premise (CPE) Vulnerability Scanner Setup Instructions“

Aktivität 3 – Voraussetzungen für den Netzwerkzugriff für die interne Schwachstellenüberprüfung

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 4 – Prüfung

Zweck dieser Aktivität ist die Durchführung einer Prüfung der aktuellen Umgebung sowie der geschäftlichen und technischen Ziele des Kunden und, sofern zutreffend, die Unterstützung des Kunden bei der Ausarbeitung der erforderlichen Sicherheitsstrategie für die Implementierung und Nutzung des/der Agenten für die interne Schwachstellenüberprüfung.

Aufgabe 1 – Erfassung von Daten

IBM wird

a. dem Beauftragten des Kunden ein Formular zur Datenerfassung übergeben, auf dem der Kunde beispielsweise folgende Informationen dokumentieren wird:
   (1) Namen, Kontaktinformationen, Aufgabenbereiche und Verantwortlichkeiten der Mitglieder des Projektteams;
   (2) Besondere länder- und standortspezifische Anforderungen;
   (3) Anzahl und Art der Endbenutzer;
   (4) Wichtige Einflussfaktoren und/oder Abhängigkeiten, die die Erbringung der Leistungen oder die vereinbarten Fristen beeinflussen könnten; und
   (5) IP-Adressen und Domänen, die Gegenstand der PCI-Überprüfung sein werden (sofern zutreffend).

Aufgabe 2 – Prüfung der Umgebung für die interne Schwachstellenüberprüfung

IBM wird

a. die im Formular zur Datenerfassung angegebenen Informationen verwenden, um die vorhandene Umgebung des Kunden zu prüfen;
b. die optimale Position des Agenten bestimmen; und
c. sofern zutreffend, Empfehlungen zur Anpassung der Anordnung des Netzwerks und der Sicherheitsrichtlinien abgeben, um die Überprüfung der gewünschten Ziele zu ermöglichen.

Beendigung der Leistungen:

Die IBM Verpflichtungen im Rahmen dieser Aktivität sind erfüllt, wenn IBM die Prüfung der Umgebung des Kunden abgeschlossen hat.

Zu liefernde Materialien:

- Keine

Aktivität 5 – Implementierung für die interne Schwachstellenüberprüfung

Zweck dieser Aktivität ist die Implementierung des/der Agenten.

Aufgabe 1 – Konfiguration des Agenten

IBM wird

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

b. Agentenhardware ermitteln, die nicht mit den aktuellen von IBM unterstützten Versionen übereinstimmt; und

c. den Kunden telefonisch beim Laden des Software-Image und bei der Konfiguration des Agenten mit einer öffentlichen IP-Adresse und zugehörigen Einstellungen unterstützen. Diese Unterstützung muss im Voraus geplant werden, um sicherzustellen, dass ein IBM Spezialist für die Implementierung zur Verfügung steht.

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); und

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

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 wurde.

Zu liefernde Materialien:

- Keine

Aktivität 6 – Test und Verifizierung

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

IBM wird

a. für jeden Agenten
   (1) die Verbindung des Agenten zu der IBM MSS-Infrastruktur verifizieren;
   (2) die Übermittlung von Prüfdaten von dem Agenten an die IBM MSS-Infrastruktur verifizieren;
   (3) die Verfügbarkeit und Funktionalität des Agenten im Portal verifizieren; und
   (4) Qualitätssicherungstests des Agenten durchführen;

b. abschließende Funktionstests der Services durchführen; und

c. 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 der Agenten übernehmen;

b. die Agenten auf „active“ einstellen; und

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

Beendigung der Leistungen:

Die IBM Verpflichtungen im Rahmen dieser Aktivität sind erfüllt, wenn die Services aktiviert und die Agenten auf „active“ eingestellt wurden.

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 – Hardwarevoraussetzungen für den Agenten für die interne Schwachstellenüberprüfung

Der Kunde wird

a. für jeden Standort, an dem eine interne Schwachstellenüberprüfung durchgeführt werden soll, Server-Hardware bereitstellen, die mit den im Dokument „Customer Premise (CPE) Vulnerability Scanner Setup Instructions“ angegebenen Systemvoraussetzungen konform ist;

b. bestätigen, dass jegliche vom Kunden bereitgestellte Hardware, die nicht mit den von IBM angegebenen Systemvoraussetzungen konform ist, zu einem Fehler bei der Installation des Softwarepakets oder einem Betriebsfehler führen kann;

c. die von IBM bereitgestellten Anweisungen für das Laden und die Konfiguration des Software-Image auf dem Gerät für die interne Schwachstellenüberprüfung befolgen; und

d. sicherstellen, dass für jede bereitgestellte Hardware ein gültiger Wartungsvertrag für die Dauer der Services vorliegt.

Aktivität 3 – Voraussetzungen für den Netzwerkzugriff für die interne Schwachstellenüberprüfung

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 4 – 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 für die interne Schwachstellenüberprüfung

Der Kunde wird

a. erforderliche Änderungen an der Anordnung seines Netzwerks und an Sicherheitsrichtlinien vornehmen, um die Überprüfung der gewünschten Ziele zu ermöglichen; und

b. die Agenten für die Schwachstellenüberprüfung so im Netzwerk des Kunden anordnen, dass sie die Zielgeräte erreichen können und dass Firewalls und andere Sicherheitskomponenten die Überprüfungen nicht stören.

Aktivität 5 – Implementierung für die interne Schwachstellenüberprüfung

Aufgabe 1 – Konfiguration des Agenten

Der Kunde wird

a. seine Hardware aktualisieren, um die IBM Spezifikationen zu erfüllen;

b. das von IBM bereitgestellte Software-Image herunterladen und auf dem Agenten installieren (d. h. Datenträger physisch laden, sofern zutreffend);

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

d. 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;

c. die von IBM angegebenen Anpassungen an der Anordnung des Netzwerks und den Sicherheitsrichtlinien durchführen, um die Überprüfung der gewünschten Ziele zu ermöglichen; und

d. die Agenten für die Schwachstellenüberprüfung so im Netzwerk des Kunden anordnen, dass sie die Zielgeräte erreichen können und dass Firewalls und andere Sicherheitskomponenten die Überprüfungen nicht stören.

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

Der Kunde bestätigt, dass

a. er die Services nutzen wird, um nur IP-Adressen und/oder Webdomänen auf Schwachstellen zu überprüfen, deren Eigentümer er ist oder zu deren Überprüfung er rechtlich befugt ist; und

b. vollständige und präzise Prüfergebnisse voraussetzen, dass er seine Netzwerktopologie und Sicherheitskomponenten so konfiguriert und wartet, dass sie ungefilterten Prüfdatenverkehr von seinen Geräten zur Schwachstellenüberprüfung an seine ausgewählten Ziele der Überprüfung passieren lassen.

3.6 Datenerfassung und -archivierung

IBM nutzt das X-Force Protection System, um die im Rahmen der Services erzeugten Prüfdaten und -berichte 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 Prüfprotokolle und -berichte, die in der Infrastruktur des X-Force Protection System erfasst und gespeichert werden.

3.6.1 Leistungsumfang

IBM wird

a. die von dem/den Agenten erzeugten Prüfdaten erfassen, sobald sie die IBM MSS-Infrastruktur erreichen;

b. Prüfdaten erfassen, die von der IBM Infrastruktur für die externe Schwachstellenüberprüfung erzeugt wurden;

c. temporäre Prüfprotokolle löschen, die von Agenten und externen Schwachstellenscannern erzeugt wurden, nachdem die Prüfergebnisse in die Datenbank des X-Force Protection System importiert wurden;

d. sofern zutreffend, Ergebnisse einzelner PCI-Überprüfungen für die Dauer von zwei Jahren zur Anzeige im Portal zur Verfügung stellen;

e. Ergebnisse einzelner Nicht-PCI-Überprüfungen für die Dauer von sechs Monaten zur Anzeige im Portal zur Verfügung stellen;

f. bei einzelnen Nicht-PCI-Überprüfungen nach Ablauf der ersten sechs Monate zusammengefasste Prüfergebnisse für die Dauer von 18 Monaten zur Verfügung stellen; und

g. Daten nach Ablauf der oben angegebenen Aufbewahrungsfristen löschen.

3.6.2 Verantwortlichkeiten des Kunden

Der Kunde wird

a. bestätigen, dass

(1) IBM temporäre Prüfprotokolle und einzelne Prüfergebnisse gemäß den in Ziffer 3.6.1 angegebenen Fristen löschen wird;

(2) IBM ungeachtet der in Ziffer 3.6.1 angegebenen Aufbewahrungsfristen seiner Verpflichtung zur Aufbewahrung der im Rahmen der Services erzeugten Daten des Kunden enthoben wird, wenn die Services aus irgendeinem Grund gekündigt oder beendet werden;

(3) alle Prüfdaten über das Internet an die SOCs übertragen werden;

(4) IBM nur Daten erfassen und überprüfen kann, die erfolgreich an die IBM MSS-Infrastruktur übertragen werden; und

(5) IBM nicht garantiert, dass die im Rahmen der Services erzeugten Daten 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;

b. das Portal verwenden, um Prüfergebnisse zu prüfen.

3.7 Überwachung des Status und der Verfügbarkeit der Managed Agents

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

Abhängig von der Anzahl an IP-Adressen, die durch einen gültigen VMS-Vertrag abgedeckt werden, wird IBM eine bestimmte Anzahl an Agenten überwachen, wie in der nachstehenden Tabelle angegeben.

IP-Adressen		Zulässige Anzahl an Agenten
Von	Bis	
1	199	2
200	999	6
1.000	2.999	12
3.000	29.999	16

30.000+	1 pro 2.000 IP-Adressen

Der Kunde bestätigt, dass für zusätzliche benötigte Agenten zusätzliche Gebühren für die Überwachung der Agenten fällig werden.

3.7.1 Leistungsumfang

Aktivität 1 – Überwachung

Zweck dieser Aktivität ist die Überwachung des Status und der Leistung der Agenten.

Agentenbasierte Überwachung

IBM wird auf den 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.

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.

3.7.2 Verantwortlichkeiten des Kunden

Aktivität 1 – Überwachung

Diese Aktivität erfordert keine weiteren Verantwortlichkeiten des Kunden.

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.

3.8 Management von Agenten

Anwendungs- und Sicherheitsupdates für Agenten sind äußerst wichtig für ein Unternehmen.

3.8.1 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.

3.8.2 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) die über das Internet übertragenen Daten mittels standardisierter Algorithmen für die starke Verschlüsselung verschlüsselt werden, wann immer möglich;

   (3) 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;

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

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

3.9 Erstellung von Serviceberichten

Über das Portal erhält der Kunde Zugriff auf Informationen zu den Services und auf Berichtsfunktionen mit individuell anpassbaren Anzeigen von Assets und Prüfergebnissen.

3.9.1 Leistungsumfang

IBM wird

a. dem Kunden Zugriff auf die Berichtsfunktionen im Portal gewähren, die Folgendes beinhalten:
   (1) Anzahl der aufgerufenen und eingehaltenen SLAs;
   (2) Anzahl, Art und Zusammenfassung von Serviceanforderungen/-tickets;
   (3) Details zu durchgeführten Überprüfungen in einer Vielzahl vordefinierter und individuell anpassbarer Formate;
b. dem Kunden die erzeugten Berichte (PDF, CSV, XML etc.) für die Dauer eines Jahres nach ihrer Erstellung (zwei Jahre bei PCI-Berichten) zum Download vom Portal bereitstellen.

3.9.2 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 Out-of-Band-Zugriff

Out-of-Band-Zugriff ist ein Feature, dessen Verwendung nachdrücklich empfohlen wird. Es unterstützt die SOCs, falls die Verbindung zu einem Agenten unterbrochen wird. Im Fall solcher Verbindungsprobleme kann sich der SOC-Analyst in das Modem einwählen, um zu verifizieren, dass der Agent korrekt funktioniert, und zur Bestimmung der Ursache des Ausfalls beitragen, bevor das Problem an den Kunden eskaliert wird.

4.1.1 Leistungsumfang

Auf Wunsch des Kunden und ohne Aufpreis wird IBM

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.

4.1.2 Verantwortlichkeiten des Kunden

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. 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.

4.2 PCI Approved Scanning Vendor Services

Auf Anforderung des Kunden wird IBM als PCI Approved Scanning Vendor (ASV) fungieren, um dem Kunden die Möglichkeit zu bieten, seinen Händlerbanken („Acquiring Banks“ oder „Acquirer“ genannt) oder Zahlungskartenunternehmen Prüfberichte vorzulegen, die durch einen ASV zertifiziert sind.

4.2.1 Leistungsumfang

Auf Wunsch des Kunden und ohne Aufpreis wird IBM

a. eine separate Umgebung innerhalb des VMS für die Durchführung von PCI-Überprüfungen einrichten;

b. mit Unterstützung des Kunden Sites innerhalb des VMS einrichten, die die Komponenten (IP-Adressen und/oder Domänen) definieren, die Gegenstand der PCI-Überprüfung sein werden;

c. nach einem vom Kunden festgelegten Zeitplan Schwachstellenüberprüfungen gemäß PCI DSS (Data Security Standard) Anforderung 11.2 durchführen;

d. Anforderungen einer Änderung des Umfangs von PCI-Überprüfungen (Ergänzungen oder Streichungen gegenüber dem zuvor genannten Umfang der PCI-Überprüfungen) beantworten. IBM wird

(1) eine unbegrenzte Anzahl an Anforderungen einer Änderung des Umfangs von PCI-Überprüfungen, die über das Portal eingereicht werden, akzeptieren;

(2) die über das Portal eingereichten Anforderungen einer Änderung des Umfangs von PCI-Überprüfungen innerhalb der Fristen bestätigen, die im Abschnitt „Service-Level-Agreements“, „Bestätigung der Anforderung einer Änderung des Umfangs von PCI-Überprüfungen“ dieser Leistungsbeschreibung angegeben sind;

(3) die eingereichten Anforderungen einer Änderung des Umfangs von PCI-Überprüfungen prüfen, um zu verifizieren, dass der Kunde die Änderung des Umfangs mittels einer ausreichenden Dokumentation begründet hat; und

(4) die angeforderten Änderungen des Umfangs von PCI-Überprüfungen innerhalb der Fristen implementieren, die im Abschnitt „Service-Level-Agreements“, „Implementierung einer angeforderten Änderung des Umfangs von PCI-Überprüfungen“ dieser Leistungsbeschreibung angegeben sind;

e. Anforderungen einer Ausnahme von Schwachstellen (z. B. mutmaßliche falsch positive Ergebnisse) beantworten. IBM wird

(1) eine unbegrenzte Anzahl an Anforderungen von Ausnahmen von Schwachstellen, die der Kunde über das Portal einreicht, akzeptieren;

(2) Anforderungen einer Ausnahme von Schwachstellen prüfen, um zu verifizieren, dass der Kunde die angeforderte Ausnahme mittels einer ausreichenden Dokumentation begründet hat; und

(3) nach alleinigem Ermessen Anforderungen einer Ausnahme von Schwachstellen innerhalb der Fristen annehmen oder ablehnen, die im Abschnitt „Service-Level-Agreements“,

„Beantwortung von Anforderungen einer Ausnahme von PCI-Schwachstellen“ dieser Leistungsbeschreibung angegeben sind;

f. das Deckblatt der Konformitätsbescheinigung durch den ASV (Attestation of Scan Compliance) und die Prüfberichte erstellen, die der Kunde Händlerbanken oder Zahlungskartenunternehmen vorlegen muss; und

g. die Prüfberichte und zugehörigen Arbeitsergebnisse zwei Jahre lang aufbewahren, wie in den Prüfanforderungen für ASVs (Validation Requirements for Approved Scanning Vendors) vorgeschrieben.

Anmerkung: Der Zugriff des Kunden auf die Berichte, die über das Portal bereitgestellt werden, und die Nutzung der Berichte durch den Kunden unterliegen den im Portal angegebenen Nutzungsbedingungen. Im Fall von Widersprüchen zwischen den im Portal angegebenen Nutzungsbedingungen und den Bedingungen dieser Leistungsbeschreibung oder eines zugehörigen Vertragsdokuments 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.

4.2.2 Verantwortlichkeiten des Kunden

Der Kunde wird

a. Portalbenutzer benennen, die berechtigt sind, die PCI-Umgebung innerhalb des VMS zu nutzen;

b. den Umfang der externen Schwachstellenüberprüfung festlegen. Der Kunde wird unter anderem

   (1) IBM die IP-Adressen und/oder Domänennamen aller aus dem Internet zugänglichen Systeme bereitstellen;

   (2) Änderungen am Umfang von PCI-Überprüfungen über das Portal anfordern und diese Änderungen umfassend und präzise begründen; und

   (3) die korrekte Netzwerksegmentierung für alle von außen zugänglichen IP-Adressen, die aus der Überprüfung ausgenommen werden sollen, implementieren;

c. sicherstellen, dass der Kunde rechtlich befugt ist, IP-Adressen und/oder Webdomänen zu überprüfen, die im Umfang der angeforderten PCI-Überprüfung enthalten sind;

d. bestätigen, dass er die alleinige Verantwortung für die Richtigkeit und Vollständigkeit des Umfangs von PCI-Überprüfungen (d. h. der IP-Adressen und/oder Webdomänen, die überprüft werden sollen) trägt;

e. sicherstellen, dass keine Geräte die Überprüfung durch den ASV stören. Der Kunde wird unter anderem

   (1) Intrusion-Detection-Systeme (IDS), Intrusion-Prevention-Systeme (IPS) und weitere Geräte so konfigurieren, dass sie die Überprüfung nicht stören (z. B. temporären ungefilterten Netzwerkzugriff auf Zielsysteme von den externen IBM Schwachstellenscannern zulassen); und

   (2) sich mit IBM abstimmen, falls der Kunde Lastverteiler einsetzt;

f. Folgendes bereitstellen, falls Lastverteiler eingesetzt werden:

   (1) eine dokumentierte Zusicherung, dass die Infrastruktur hinter dem/den Lastverteiler/n im Hinblick auf die Konfiguration synchronisiert ist; oder

   (2) eine dokumentierte Zusicherung, dass der IBM genannte Umfang der PCI-Überprüfung alle per Lastverteiler gesteuerten Geräte eindeutig identifiziert, sodass eine vollständige Überprüfung durchgeführt werden kann;

g. die Verantwortung für die Koordination mit dem Internet-Service-Provider (ISP) und/oder den Hosting-Providern des Kunden übernehmen, um völlig ungefilterten Netzdatenverkehr zwischen den externen IBM Schwachstellenscannern und dem/den Zielnetzwerk/en des Kunden zu ermöglichen;

h. sofern er Prüfergebnisse bezüglich einer bestimmten Schwachstelle anzweifelt,

   (1) über das Portal eine Ausnahme anfordern und IBM eine ausreichende Dokumentation bereitstellen, um IBM bei der Untersuchung der strittigen Ergebnisse (z. B. mutmaßliche

falsch positive Ergebnisse) und der Lösung des Konflikts zu unterstützen, sowie eine entsprechende Bescheinigung im Rahmen des VMS bereitstellen;

(2) systemgenerierte Nachweise wie z. B. Screenshots, Konfigurationsdateien, Systemversionen, Dateiversionen und eine Liste der installierten Patches bereitstellen. Diese systemgenerierten Nachweise müssen durch eine Beschreibung ergänzt werden, die angibt, wann, wo und wie sie erlangt wurden; und

(3) bestätigen, dass IBM möglicherweise (auf Kosten des Kunden) einen PCI Qualified Security Assessor (QSA) beauftragen muss, bevor bestimmte strittige Punkte akzeptiert werden (z. B. geplante andere Kontrollen);

i. das Portal verwenden, um eine Überprüfung zu initiieren;

j. den Prüfbericht prüfen und alle festgestellten Schwachstellen beseitigen, um PCI-Konformität zu erreichen;

k. über das Portal eine erneute Überprüfung von nicht konformen IP-Adressen initiieren, um die vierteljährliche Prüfung zu bestehen;

l. das Portal verwenden, um bei IBM die Erstellung der vierteljährlichen Konformitätsbescheinigung (Attestation of Scan Compliance) durch den PCI ASV anzufordern;

m. die fertigen ASV-Prüfberichte herunterladen und sie dem Acquirer oder den Zahlungskartenunternehmen des Kunden nach Anweisung der Zahlungskartenunternehmen vorlegen;

n. durch das Herunterladen und Vorlegen der ASV-Berichte für Acquirer oder Zahlungskartenunternehmen bescheinigen und bestätigen, dass

(1) der Kunde die systemgenerierten ASV-Berichte nicht auf irgendeine Weise geändert oder abgewandelt hat oder ändern oder abwandeln wird, bevor er sie seinen Acquirern oder Zahlungskartenunternehmen vorlegt;

(2) der Kunde für die korrekte Bestimmung des Umfangs der Überprüfungen verantwortlich ist und alle Komponenten in die Überprüfung einbezogen hat, die Gegenstand einer Überprüfung gemäß PCI DSS sein sollten;

(3) der Kunde die Netzwerksegmentierung implementiert hat, falls Komponenten aus dem Umfang der PCI DSS-Überprüfung ausgenommen werden sollen;

(4) der Kunde präzise und vollständige Nachweise im Fall von Kontroversen über Prüfergebnisse bereitgestellt hat; und

(5) die Prüfergebnisse nur angeben, ob die überprüften Systeme mit den Anforderungen an eine externe Schwachstellenüberprüfung (gemäß PCI DSS 11.2) konform sind, aber nicht bestätigen, dass sie mit jeglichen anderen PCI DSS-Anforderungen übereinstimmen.

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/die Agent/en (sofern zutreffend) auf „active“ eingestellt wurde/n und die Unterstützung und das Management des/der 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. 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.

b. Durchführung einer Schwachstellenüberprüfung – IBM wird innerhalb einer Stunde vor oder nach dem vom Kunden (oder von IBM für den Kunden) geplanten Termin mit einer geplanten Schwachstellenüberprüfung beginnen, und alle Überprüfungen werden abgeschlossen. Dieses SLA gilt nur unter der Voraussetzung, dass Anforderungen einer Überprüfung korrekt konfiguriert sind, die Agenten am Kundenstandort online und von der SOC-Infrastruktur aus zugänglich sind und der ausgewählte Schwachstellenscanner vollen Zugriff auf die Ziele der Überprüfung hat.

c. Bestätigung der Anforderung einer Änderung des Umfangs von PCI-Überprüfungen – IBM wird Anforderungen einer Änderung des Umfangs von PCI-Überprüfungen innerhalb von zwei Stunden, nachdem sie über das Portal eingereicht wurden, bestätigen.

d. Implementierung einer angeforderten Änderung des Umfangs von PCI-Überprüfungen – IBM wird angeforderte Änderungen des Umfangs von PCI-Überprüfungen innerhalb von 72 Stunden nach Erhalt einer ausreichend und akzeptabel dokumentierten Begründung der Änderung durch den Kunden implementieren.

e. Beantwortung der Anforderung einer Ausnahme von PCI-Schwachstellen – IBM wird eine angeforderte Ausnahme innerhalb von 72 Stunden nach Erhalt einer ausreichend und akzeptabel dokumentierten Begründung der Ausnahme durch den Kunden annehmen oder ablehnen.

   Anmerkung: Der Kunde kann eine unbegrenzte Anzahl an Ausnahmen von PCI-Schwachstellen anfordern, doch nur die ersten 15 Anforderungen, die pro Tag eingereicht werden, unterliegen diesem SLA. Alle nachfolgenden Anforderungen (die über die ersten 15 pro Tag hinausgehen) werden zwar angenommen, aber nicht mit Priorität behandelt, und unterliegen nicht diesem SLA.

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 % bieten, ausgenommen 1) während der im Abschnitt „Geplante und im Notfall durchgeführte Portalwartung“ in den Allgemeinen Bedingungen für IBM Managed Security Services angegebenen Zeiten und 2) während eines zusätzlichen Standardwartungszeitfensters am dritten Samstag jedes Monats von 8:00 Uhr bis 12:00 US Eastern Time.

5.2 SLA-Gutschriften

Service-Level-Gutschriften bei Nichteinhaltung folgender SLAs: proaktive Systemüberwachung, Durchführung einer Schwachstellenüberprüfung, Bestätigung der Anforderung einer Änderung des Umfangs von PCI-Überprüfungen, Implementierung einer angeforderten Änderung des Umfangs von PCI-Überprüfungen, Beantwortung der Anforderung einer Ausnahme von PCI-Schwachstellen – Falls IBM eines dieser SLAs nicht einhält, wird IBM dem Kunden eine Service-Level-Gutschrift in Höhe von 1/30 der monatlichen VMS-Gebühren 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
Proaktive Systemüberwachung	Service-Level-Gutschrift, 1/30 der monatlichen Servicegebühr
Durchführung einer Schwachstellenüberprüfung	
Bestätigung der Anforderung einer Änderung am Umfang von PCI-Überprüfungen	
Implementierung einer angeforderten Änderung am Umfang von PCI-Überprüfungen	
Beantwortung der Anforderung einer Ausnahme von	

PCI-Schwachstellen	

6. Ergänzende Bedingungen

6.1 Allgemeines

Der Kunde bestätigt und erklärt sich damit einverstanden, dass

a. sämtliche von IBM im Rahmen dieser Services bereitgestellte Software lizenziert, nicht verkauft wird und mit Ausnahme der ausdrücklich hierin gewährten Nutzungsrechte sämtliche Rechte, einschließlich des Eigentumsrechts, an der Software bei IBM oder den Lizenzgebern verbleiben;

b. er IBM mindestens 30 Tage vor Kündigung oder Beendigung der Services oder unverzüglich nach Kündigung der Lizenz für die Software durch IBM, gleich aus welchem Grund, schriftlich informieren wird, ob

   (1) er die von IBM bereitgestellte Software für die Schwachstellenüberprüfung entweder von IBM per Fernzugriff entfernen lassen oder mit Unterstützung durch IBM selbst entfernen wird; oder

   (2) er die von IBM bereitgestellte Software für die Schwachstellenüberprüfung behalten wird.

   Entscheidet sich der Kunde dafür, die Software entfernen zu lassen, wird er mit IBM zusammenarbeiten, indem er IBM den zum Entfernen der Software notwendigen Fernzugriff gewährt oder IBM beim Entfernen der Software unterstützt.

c. dem Kunden zusätzlich zu den oben aufgeführten Bedingungen bestimmte Lizenzbedingungen zur Prüfung und Annahme präsentiert werden, sowohl beim Herunterladen als auch bei der Installation der Software.

6.2 Autorisierung zur Durchführung von Tests

Im Rahmen der gesetzlichen Bestimmungen kann es verboten sein, unbefugt in Computersysteme einzudringen oder auf sie zuzugreifen. Der Kunde autorisiert IBM, die hierin beschriebenen Services zu erbringen, und bestätigt, dass IBM im Rahmen dieser Services berechtigt ist, sich Zugriff auf die Computersysteme des Kunden zu verschaffen. IBM kann diese Autorisierung an Dritte weitergeben, sofern IBM dies zur Erbringung der Services für notwendig erachtet.

Die von IBM erbrachten Leistungen sind mit bestimmten Risiken verbunden. Der Kunde erklärt sich damit einverstanden, alle Risiken im Zusammenhang mit den Services zu tragen, vorausgesetzt, dass dies die IBM Verpflichtung zur Erbringung der Services gemäß den Bedingungen dieser Leistungsbeschreibung nicht einschränkt. Der Kunde bestätigt daher ausdrücklich und erklärt sich damit einverstanden, dass

a. die Services zur Generierung einer großen Anzahl an Protokollnachrichten führen können und die Log-Datei dadurch sehr viel Plattenplatz belegen kann;

b. die Leistung und der Durchsatz der Systeme des Kunden sowie der zugehörigen Router und Firewalls vorübergehend beeinträchtigt werden können;

c. bestimmte Daten aufgrund der Überprüfung auf Schwachstellen vorübergehend verändert werden können;

d. die Services zu einem Hängen oder Absturz der Computersysteme des Kunden und einem vorübergehenden Systemausfall führen können;

e. die Rechte oder Ansprüche aus bestehenden Service-Level-Agreements während einer Überprüfung keine Gültigkeit haben;

f. bei einer Überprüfung Alarmnachrichten von den Systemen zur Erkennung unbefugter Zugriffe ausgelöst werden können;

g. bei bestimmten Aspekten der Services die über das überwachte Netzwerk übertragenen Daten zum Zweck der Erkennung bestimmter Aktivitäten abgefangen werden dürfen; und

h. ständig neue Sicherheitsbedrohungen entstehen und kein Service zum Schutz vor Sicherheitsbedrohungen in der Lage ist, Netzwerkressourcen gegenüber solchen Sicherheitsbedrohungen unangreifbar zu machen oder sicherzustellen, dass sämtliche Risiken, Sicherheitslücken und Schwachstellen aufgedeckt werden.

6.3 Systeme Dritter

Wenn sich die Systeme (die im Sinne dieser Bestimmung auch Anwendungen und IP-Adressen einschließen), die im Rahmen dieser Leistungsbeschreibung überprüft werden, nicht im Eigentum des Kunden befinden, wird der Kunde

a. bevor IBM mit der Überprüfung auf Systemen Dritter beginnt, eine schriftliche Bestätigung des jeweiligen Eigentümers jedes Systems vorlegen, wonach der Eigentümer IBM autorisiert, die Services auf dem betreffenden System durchzuführen, und sein Einverständnis mit den im Abschnitt „Autorisierung zur Durchführung von Tests“ genannten Bedingungen erklärt. Der Kunde wird IBM unverzüglich eine Kopie dieser Autorisierung aushändigen;

b. die alleinige Verantwortung dafür übernehmen, den Eigentümer eines Systems über die Risiken, Sicherheitslücken und Schwachstellen auf diesem System zu informieren, die bei der von IBM per Fernzugriff durchgeführten Überprüfung festgestellt wurden; und

c. den Informationsaustausch zwischen dem Eigentümer des Systems und IBM ermöglichen, sofern IBM dies für notwendig erachtet.

Des Weiteren wird der Kunde

a. IBM unverzüglich informieren, wenn ein Wechsel des Eigentümers eines Systems erfolgt, das Gegenstand der hierunter durchgeführten Tests ist;

b. die zu liefernden Materialien oder die Information über die Tatsache, dass IBM die Services erbracht hat, ohne vorherige schriftliche Zustimmung von IBM nicht an Dritte weitergeben; und

c. IBM in vollem Umfang für Verluste oder Haftungspflichten entschädigen, die IBM infolge von Ansprüchen Dritter aufgrund der Nichteinhaltung der in Ziffer 6.3 („Systeme Dritter“) aufgeführten Bedingungen durch den Kunden entstehen, und IBM oder die IBM Unterauftragnehmer oder deren Bevollmächtigte in Bezug auf alle Ansprüche oder Zwangsmaßnahmen Dritter schadlos halten, die sich aus (a) der Überprüfung der hierunter getesteten Systeme auf Sicherheitsrisiken, -lücken oder -schwachstellen, (b) der Bereitstellung der Ergebnisse dieser Überprüfungen für den Kunden oder (c) der Verwendung oder Offenlegung dieser Ergebnisse durch den Kunden ergeben.

6.4 Ausschlüsse

Der Kunde nimmt zur Kenntnis und erklärt sich damit einverstanden, dass

a. es in seinem alleinigen Ermessen liegt, die Informationen, die ihm im Rahmen der hierunter erbrachten Services bereitgestellt werden, zu verwenden oder auf ihre Verwendung zu verzichten. IBM kann nicht für Maßnahmen haftbar gemacht werden, die der Kunde auf der Basis der hierunter erbrachten Services und/oder bereitgestellten zu liefernden Materialien ergreift oder nicht ergreift;

b. IBM keine Rechtsberatung erteilt und nicht zusichert oder gewährleistet, dass die von IBM bereitgestellten oder für den Kunden beschafften Services oder Produkte die Einhaltung bestimmter Gesetze sicherstellen, insbesondere der Gesetze für Sicherheit oder Datenschutz; und

c. es dem Kunden obliegt, sich von kompetenter juristischer Stelle zu Inhalt und Einhaltung aller relevanten Gesetze beraten zu lassen, die sich auf seine Geschäftstätigkeit und alle Maßnahmen des Kunden auswirken können, die dieser im Hinblick auf die Einhaltung solcher Gesetze durchführen muss.

6.5 Vereinbarungen bezüglich der Zahlungskartenbranche

Der Kunde bestätigt, dass es sich bei IBM um einen ASV handelt, der über eine gültige Vereinbarung mit dem Payment Card Industry Security Standards Council (PCI SSC) verfügt. In Übereinstimmung mit den in einer solchen Vereinbarung enthaltenen Bedingungen werden die folgenden Bestimmungen in diese Leistungsbeschreibung aufgenommen.

a. Der Kunde bestätigt, dass er im Zusammenhang mit seiner Verpflichtung zur Einhaltung des PCI DSS (Payment Card Industry Data Security Standard), d. h. des Datensicherheitsstandards der Zahlungskartenbranche, bei IBM möglicherweise Services bestellt. Dem Kunden ist bewusst, dass die Handhabung des PCI DSS bezüglich Sicherheitsanalysen bei den bekannten Zahlungskartenunternehmen liegt, die das PCI SSC damit beauftragen. Der Kunde bestätigt, dass er IBM für die Erbringung von Services aus einer Liste genehmigter Anbieter ausgewählt hat, die vom PCI SSC veröffentlicht wurde („ASV-Liste“). Darüber hinaus bestätigt der Kunde, dass IBM als Voraussetzung für die Aufnahme in die ASV-Liste eine Vereinbarung mit dem PCI SSC (nachfolgend „ASV-Vereinbarung“ genannt) schließen muss (Beispiel unter

www.pcisecuritystandards.org, „Validation Requirements for Approved Scanning Vendors („ASVs“) Version 1.2“, „Appendix A PCI ASV Compliance Test Agreement“). Der Kunde bestätigt zudem, dass IBM aufgrund bestimmter Teile dieser Vereinbarung bestimmte Bedingungen in seine Verträge mit Kunden aufnehmen muss.

(1) Der Kunde erklärt sich damit einverstanden, dass die Aufnahme von IBM in die ASV-Liste weder eine stillschweigende oder ausdrückliche Billigung oder Empfehlung des PCI SSC noch eine Gewährleistung des PCI SSC oder eines seiner Mitglieder im Zusammenhang mit IBM, Services oder Produkten von IBM oder der Funktionalität, Qualität oder Leistung der Vorgenannten darstellt. Darüber hinaus bestätigt der Kunde, dass vonseiten des PCI SSC keine Verpflichtung zur Nutzung von IBM Produkten oder Services durch den Kunden besteht. Der Kunde erklärt sich außerdem damit einverstanden, dass bestimmte Begriffe in den Ziffern a. (2), (3), (4) und (5) im Rahmen dieses Abschnitts „Vereinbarungen bezüglich der Zahlungskartenbranche“ dieselbe Bedeutung wie in der ASV-Vereinbarung haben.

(2) Der Kunde erklärt sich damit einverstanden, dass (i) IBM Test- und Analyseergebnisse (mit Prüfberichten) und zugehörige Informationen gemäß Anforderung von PCI SSC und/oder seiner Mitglieder auf Anforderung des Kunden offenlegen kann, (ii) sofern ein Mitglied diese Informationen in Übereinstimmung mit der vorhergehenden Ziffer erhält, dieses Mitglied diese Informationen bei Bedarf gegenüber seinen Finanzinstituten und Kartenherausgebern („Issuer“) sowie gegenüber den zuständigen Behörden und Beamten offenlegen kann, und (iii) IBM diese Informationen offenlegen kann, um seinen Verpflichtungen und Anforderungen gemäß der ASV-Vereinbarung und der Beschreibung in Ziffer (4) unten gerecht zu werden. Der Kunde bestätigt, dass das PCI SSC oder dessen Händlerbanken („Acquirer“) vertrauliche Informationen, die das PCI SSC im Zusammenhang mit der ASV-Vereinbarung erhält, gegenüber Mitgliedern gemäß dieser Ziffer a. (2) offenlegen kann, die diese Informationen wiederum gegenüber ihren Finanzinstituten und anderen Mitgliedern offenlegen können. Der Kunde stimmt (i) einer solchen Offenlegung durch das PCI SSC und dessen Mitglieder sowie (ii) einer Offenlegung vertraulicher Informationen, einschließlich Test- und Analyseergebnissen (mit Prüfberichten) und zugehöriger Informationen, gemäß dieser Ziffer a. (2) zu. Sollte der Kunde über eine Geheimhaltungsvereinbarung mit IBM verfügen, werden die Bedingungen dieser Ziffer a. (2) durch diese Bezugnahme darauf in diese Vereinbarung aufgenommen.

(3) Dem Kunden ist bewusst, dass IBM sich in der ASV-Vereinbarung bereit erklärt hat, bestimmte Datenschutzvorkehrungen für personenbezogene Informationen, die IBM ggf. vom PCI SSC oder von einem Mitglied bzw. Kunden erhält, zu treffen. Ferner verpflichtet sich IBM dazu, dem PCI SSC und dessen Mitgliedern und/oder Acquirern/Issuern sachdienliche Analysen und Berichte zur Überwachung der Einhaltung dieser Datenschutzanforderungen durch IBM bereitzustellen. Der Kunde stimmt der Bereitstellung dieser Analysen und Berichte für PCI SSC und Mitglieder und/oder Acquirer/Issuer durch IBM zu und erklärt sich ferner damit einverstanden, dass er dem PCI SSC oder dessen Mitgliedern und/oder Acquirern/Issuern sachdienliche Analysen und Berichte zur Überwachung der Einhaltung dieser Datenschutzanforderungen durch IBM bereitstellt, die das PCI SSC oder dessen Mitglieder und/oder Acquirer/Issuer in angemessenem Umfang von Zeit zu Zeit anfordern.

(4) Dem Kunden ist bewusst, dass IBM in der ASV-Vereinbarung auf schriftliche Anforderung von PCI SSC oder einem Mitglied (nachfolgend jeweils „anfordernde Organisation“ genannt) eingewilligt hat, dieser anfordernden Organisation Test- und Analyseergebnisse (mit Prüfberichten) zur Verfügung zu stellen, die eine solche anfordernde Organisation in angemessenem Umfang anfordert und die sich auf Folgendes beziehen: (i) Wenn es sich bei der anfordernden Organisation um ein Mitglied handelt, auf einen Kunden eines Anbieters, für den IBM eine Analyse durchgeführt hat und bei dem es sich um Folgendes handelt: eine Finanzinstitution eines solchen Mitglieds, einen Issuer dieses Mitglieds, einen Händler, der berechtigt ist, die Zahlungskarten dieses Mitglieds zu akzeptieren, einen Acquirer von Accounts von Händlern, die berechtigt sind, die Zahlungskarten dieses Mitglieds zu akzeptieren, oder einen Kartenverarbeiter („Processor“), der Services für die Finanzinstitute, Issuer, Händler oder Acquirer dieses Mitglieds erbringt, oder (ii) wenn es sich bei der anfordernden Organisation um PCI SSC handelt, auf einen Kunden eines Anbieters, für den der ASV Tests oder Analysen durchgeführt hat. Der Kunde erklärt sich mit jeder derartigen Offenlegung von Test- und Analyseergebnissen (mit Prüfberichten) einverstanden und erteilt IBM alle erforderlichen Ermächtigungen, Lizenzen und sonstigen Berechtigungen, die

erforderlich sind, damit IBM seinen Verpflichtungen und Anforderungen gemäß der ASV-Vereinbarung nachkommen kann.

b. Haftungsfreistellung durch den Kunden im Zusammenhang mit Payment Card Industry Services

Soweit IBM Services als ASV bereitstellt, muss der Kunde IBM gegen alle Ansprüche, Verluste, Verbindlichkeiten, Schäden, Rechtsstreitigkeiten, Klagen, Verwaltungsverfahren, Steuern, Strafen oder Zinsen, zugehörige Prüf- und Rechtskosten sowie andere Kosten (angemessene Anwaltskosten und zugehörige Kosten uneingeschränkt eingeschlossen) verteidigen, schadlos halten und davon freistellen, die sich aus Ansprüchen des PCI Security Standards Council LLC und seiner Mitglieder, ihrer jeweiligen Tochtergesellschaften sowie aller verbundenen Unternehmen, Direktoren, Führungskräfte, Mitarbeiter, Beauftragten, Bevollmächtigten, unabhängigen Auftragnehmer, Anwälte, Nachfolger und Rechtsnachfolger der Vorgenannten gegen IBM oder verbundene Unternehmen von IBM im Zusammenhang mit den Services im Rahmen dieser Vereinbarung ergeben.