**Servicebeschreibung**

**HCL AppScan on Cloud**

Diese Servicebeschreibung ("Servicebeschreibung") beschreibt den HCL AppScan on Cloud-Service ("HCL AppScan on Cloud" oder "Cloud-Service"). Zusätzliche Bedingungen für die Nutzung von HCL AppScan on Cloud sind in der HCL Cloud-Servicevereinbarung ("CSA") festgelegt, die unter <https://www.hcltechsw.com/wps/portal/resources/master-agreements> verfügbar ist. Diese Servicebeschreibung, alle zugehörigen Anlagen, Aufträge und die CSA (Cloud Services Agreement, Cloud-Servicevereinbarung) bilden die vollständige Vereinbarung in Bezug auf Transaktionen im Rahmen der CSA (zusammenfassend als "Vereinbarung" bezeichnet). Alle in dieser Servicebeschreibung verwendeten, aber nicht definierten großgeschriebenen Begriffe haben die in der CSA oder anderen geltenden Vertragsdokumenten angegebene Bedeutung.

**1. HCL AppScan on Cloud**

HCL AppScan on Cloud ermöglicht es dem Kunden, Sicherheitslücken (z. B. SQL-Injection, Cross-Site Scripting und Datenlecks) für eine Reihe von Anwendungen von einem zentralen Ort aus zu identifizieren. Der Service umfasst verschiedene Arten von Scantechniken für Anwendungssicherheit, die jeweils Sicherheitslücken in dieser Anwendung identifizieren.

HCL AppScan on Cloud bietet die folgenden Funktionen:

* Scannen mobiler Anwendungen auf Sicherheitslücken.
* Scannen von Websites und Webservices in der Produktion oder Vorproduktion, in öffentlichen oder privaten Netzwerken auf Sicherheitslücken mit Hilfe von Sicherheitstest mit dynamischer Analyse.
* Scannen des Codes in Web- und Desktop-Anwendungen auf Sicherheitslücken mit Hilfe von Sicherheitstests mit statischer Analyse.
* Analyse von Webanwendungen und Webservices während ihrer Ausführung zur Aufdeckung von Sicherheitslücken mit Hilfe von interaktiven Sicherheitstests für Anwendungen.
* Identifizieren anfälliger Open-Source-Pakete, die in einer Anwendung verwendet werden, mit Hilfe der Analyse der Softwarekomposition.
* Ausführliche Berichte über Sicherheitslücken, die sowohl Gesamtübersichten der Ergebnisse als auch Korrekturmaßnahmen enthalten, die von den Entwicklern Schritt für Schritt umgesetzt werden können.
* Integration in verschiedene DevOps-Plattformen.

**1.1 Angebote**

Der Kunde kann unter folgenden verfügbaren Angeboten wählen:

**1.1.1 HCL AppScan Analyzer**

HCL AppScan Analyzer kann entweder pro Anwendungsinstanz, pro Job (Scan), pro gleichzeitigem Ereignis (Scan) oder als Parallelinstanz bestellt werden und ermöglicht die Ausführung der folgenden Arten von Scans:

* Dynamic Analyzer - Testen von Websites in der Vorproduktion oder Produktion
* Mobile Analyzer - Testen von iOS- oder Android-Anwendungen
* Static Analyzer - Testen von Byte oder Quellcode der Anwendung

**1.1.2 HCL AppScan IAST Analyzer**

HCL AppScan IAST Analyzer identifiziert Sicherheitslücken bei der Ausführung von Webanwendungen und Webservices. Ein IAST-Agent instrumentiert die Anwendung, um ihr Verhalten passiv zu überwachen, während er mit ihr interagiert, und meldet die identifizierten Schwachstellen an HCL AppScan on Cloud. HCL AppScan IAST Analyzer kann pro Anwendungsinstanz oder pro gleichzeitigem Ereignis (Scan) bestellt werden.

**1.1.3 HCL AppScan Open Source Analyzer**

HCL AppScan Open Source Analyzer entdeckt und identifiziert Open-Source-Pakete, die im Anwendungscode verwendet werden. Der Open Source Analyzer überprüft diese Pakete auf Schwachstellen und liefert Korrekturvorschläge. HCL AppScan Open Source Analyzer kann pro Anwendungsinstanz, pro gleichzeitigem Ereignis (Scan) oder als Parallelinstanz bestellt werden.

**2. Gebührenmetriken**

Für diesen Cloud-Service gelten die folgenden Gebührenmetriken:

* **Anwendungsinstanz** ist eine Kopie eines eindeutig benannten Softwareanwendungsprogramms, das mit dem Cloud-Service verbunden ist oder von diesem verwaltet wird. Eine Anwendung in mehreren Umgebungen (z.B. Test-, Entwicklungs-, Staging- oder Produktionsumgebung) oder mehrere Instanzen einer Anwendung innerhalb einer einzigen Umgebung werden als separate Anwendungsinstanzen betrachtet.

Bei diesem Cloud-Service versteht man unter Anwendungsinstanzen aufeinanderfolgende Scans einer einzelnen Anwendung, die wie folgt definiert werden:

* Für dynamische Tests: eine Website oder ein Webservice, die / der über eine öffentliche oder private URL aufrufbar ist. Jede Anwendungsinstanz umfasst die Berechtigung für eine Website mit bis zu 5.000 Seiten in einer einzigen Domäne.
* Für statische Tests: eine Codeeinheit, die für eine einzelne ausführbare Umgebung erstellt wurde. Jede Anwendungsinstanz umfasst die Berechtigung zum Scannen von Codeeinheiten mit bis zu 1.000.000 Zeilen.
* Für mobile Tests: eine Binärcodeeinheit, die auf einem mobilen Gerät ausführbar ist. Jede Art von mobiler Plattform (z. B. iOS und Android) stellt eine eigene Anwendungsinstanz dar.
* Für Open-Source-Tests: eine Codeeinheit, die für eine einzelne ausführbare Umgebung erstellt wurde. Jede Anwendungsinstanz umfasst die Berechtigung zum Scannen von Codeeinheiten mit bis zu 1.000.000 Zeilen.
* Für interaktive Tests: eine Website oder ein Webservice, die / der über eine öffentliche oder private URL aufrufbar ist.
* **Unter gleichzeitigen Ereignissen** versteht man die Gesamtzahl der gleichzeitigen Vorkommnisse eines bestimmten Ereignisses, das durch den Cloud-Service verarbeitet wird oder sich auf die Nutzung des Cloud-Service bezieht.
* **Parallelinstanz** steht für jeden Zugriff auf eine bestimmte Konfiguration des Cloud-Service. Bei der einzelnen Parallelinstanz-Berechtigung besteht keine Beschränkung der Anzahl der ausgeführten Jobs oder Anwendungsinstanzen (verbundene Anwendungen), sofern die Anzahl der gleichzeitigen Ereignisse zu einem bestimmten Zeitpunkt nicht die Anzahl der gesamten gleichzeitigen Berechtigungen für die Parallelinstanz übersteigt.
* **Job** ist ein Objekt innerhalb des Cloud-Service, das nicht weiter unterteilt werden kann und einen Rechenprozess einschließlich all seiner Unterprozesse darstellt, die vom Cloud-Service verwaltet oder verarbeitet werden. Es müssen ausreichende Berechtigungen erworben werden, um die Gesamtzahl aller Jobs abzudecken, die vom Cloud-Service während des im Auftrag oder einer anderen zugehörigen Anlage angegebenen Messzeitraums verarbeitet oder verwaltet werden.

|  |  |
| --- | --- |
| **AppScan pro Scan** | |
| Abonnementtyp | Beschreibung |
| ASoC\_PerScan | Bietet einen einzelnen Scan (der als Job anzusehen ist) einer Anwendung, die eine dieser Scan-Technologien (Static Analyzer, Dynamic Analyzer oder Mobile Analyzer) verwendet.  Gekaufte Scans müssen innerhalb von zwölf (12) Monaten nach dem Kaufdatum verwendet werden; danach verfallen sie ohne Möglichkeit der Rückerstattung. Kein Zeitlimit pro Scan; die Scans werden bis zum Abschluss ausgeführt.  Die Anzahl der gleichzeitig ausgeführten Jobs ist auf drei (3) beschränkt. |
| **AppScan pro Anwendung** | |
| Abonnementtyp | Beschreibung |
| ASoC\_PerApplication | Jahresabonnement, das unbegrenztes Scannen einer Anwendung ("Anwendungsinstanz") mit einer dieser Scan-Technologien (Static Analyzer, Dynamic Analyzer oder Mobile Analyzer) ermöglicht, die je nach Anwendung einsetzbar sind.  Die Anzahl der gleichzeitig ausgeführten Jobs ist auf jeweils nur einen (1) beschränkt. |
| **AppScan – Unbegrenzte Preisoptionen** | |
| Abonnementtyp | Beschreibung |
| AsoC\_PerConcurrent | Jahresabonnement, das das Scannen jeder Anwendung mit einer dieser Scantechnologien (Static Analyzer, Dynamic Analyzer oder Mobile Analyzer) ermöglicht.  Die Anzahl der ausgeführten Jobs ist auf einen (1) pro gleichzeitiger Scan-Berechtigung beschränkt.  (Parallelinstanz von "1") |
| ASoC Premium | Jahresabonnement für bis zu zehn (10) gleichzeitige Scans einer beliebigen Anwendung mithilfe einer dieser Scantechnologien (Static Analyzer, Dynamic Analyzer oder Mobile Analyzer).  Die Anzahl der ausgeführten Jobs pro "Premium"-Berechtigung ist auf bis maximal zehn (10) beschränkt.  (Parallelinstanz von "10") |
| ASoC\_PerConcurrent(s) und ASoC\_Premium(s) lassen sich kombinieren, um die Anforderungen eines Kunden an die Gleichzeitigkeit zu erfüllen. | |
| **AppScan IAST Analyzer pro Anwendung** | |
| Abonnementtyp | Beschreibung |
| ASoC\_IAST\_PerApplication | Jahresabonnement für unbegrenztes IAST-Scannen einer (1) Anwendung ("Anwendungsinstanz").  Die Anzahl der gleichzeitig ausgeführten IAST-Jobs ist auf jeweils nur einen (1) beschränkt. |
| **AppScan IAST Analyzer – Unbegrenzte Preisoptionen** | |
| Abonnementtyp | Beschreibung |
| ASoC\_IAST\_PerConcurrent | Jahresabonnement, das das IAST-Scannen für jede Anwendung ermöglicht.  Die Anzahl der ausgeführten IAST-Jobs ist auf einen (1) pro gleichzeitiger Scan-Berechtigung beschränkt.  (Parallelinstanz von "1") |
|  |  |
| **AppScan Open Source Analyzer pro Anwendung** | |
| Abonnementtyp | Beschreibung |
| ASoC\_OSA\_PerApplication | Jahresabonnement für unbegrenztes Open Source-Scannen einer (1) Anwendung ("Anwendungsinstanz").  Die Anzahl der gleichzeitig ausgeführten Jobs ist auf jeweils nur einen (1) beschränkt. |
| **AppScan Open Source Analyzer – Unbegrenzte Preisoptionen** | |
| Abonnementtyp | Beschreibung |
| ASoC\_OSA\_PerConcurrent | Jahresabonnement, das das Open Source-Scannen für jede Anwendung ermöglicht.  Die Anzahl der ausgeführten Jobs ist auf einen (1) pro gleichzeitiger Scan-Berechtigung beschränkt.  (Parallelinstanz von "1") |
| ASoC\_OSA\_Premium | Jahresabonnement, das bis zu zehn (10) gleichzeitige Open-Source-Scans für jede Anwendung ermöglicht.  Die Anzahl der ausgeführten Jobs pro "Premium"-Berechtigung ist auf bis maximal zehn (10) beschränkt.  (Parallelinstanz von "10") |
|  | |

**3. Gebühren und Abrechnung**

Der für den HCL AppScan on Cloud zu zahlende Betrag wird in einer Bestellung angegeben.

**3.1 Gebühren für den angefangenen Monat**

Die in der Bestellung angegebenen Gebühren für den angefangenen Monat können anteilsmäßig berechnet werden.

**3.2 Abrechnungshäufigkeit**

Basierend auf der gewählten Abrechnungshäufigkeit stellt HCL dem Kunden die zu Beginn des Abrechnungszeitraums fälligen Gebühren in Rechnung, mit Ausnahme von Gebühren für Nutzungsüberschreitungen und spezifischen Nutzungsgebühren, die rückwirkend berechnet werden.

**3.3 Abgeleitete Leistungsorte**

Sofern zutreffend, basieren die Steuern auf dem / den Standort(en), den / die der Kunde als Empfangsort der Leistungen des Cloud-Service angibt. HCL berechnet die Steuern auf der Grundlage der Geschäftsadresse, die bei der Bestellung des Cloud-Service als primärer Leistungsort angegeben wird, es sei denn, der Kunde stellt HCL hierzu zusätzliche Informationen zur Verfügung. Der Kunde ist verpflichtet, diese Informationen auf dem neuesten Stand zu halten und HCL alle Änderungen diesbezüglich mitzuteilen.

**3.4 Bestätigung**

Der Kunde wird i) Aufzeichnungen und Systemtools pflegen und auf Anforderung zur Verfügung stellen, soweit dies für HCL und ihre beauftragten externen Prüfer erforderlich ist, um die Einhaltung der Vereinbarung durch den Kunden zu überprüfen, und ii) unverzüglich alle erforderlichen Berechtigungen bestellen und zu den zum jeweiligen Zeitpunkt gültigen Preisen von HCL bezahlen und andere Verbindlichkeiten, die sich aufgrund der Prüfung ergeben und in einer Rechnung von HCL angegeben sind, begleichen. Die Verpflichtungen im Rahmen dieses Abschnitts bleiben während der Laufzeit des Cloud-Service und eines Zeitraums von zwei Jahren danach in Kraft.

**4. Laufzeit und Verlängerungsoptionen**

Die Laufzeit des Cloud-Service beginnt an dem Datum, an dem HCL den Kunden über seinen Zugriff auf den Cloud-Service gemäß der Erklärung im Berechtigungsnachweis benachrichtigt. Im Berechtigungsnachweis wird festgelegt, ob sich der Cloud-Service automatisch verlängert oder am Ende der Laufzeit ausläuft.

Bei der automatischen Verlängerung erfolgt eine automatische Verlängerung für die im Berechtigungsnachweis angegebene Laufzeit, es sei denn, der Kunde teilt mindestens 30 Tage vor Ablauf der Laufzeit schriftlich mit, dass er keine Verlängerung wünscht.

**5. Technische Unterstützung**

Während des Abonnementzeitraums und nachdem HCL den Kunden darüber informiert hat, dass der Zugriff auf den Cloud-Service gewährt wurde, können technische Support-Informationen auf der zu diesem Zeitpunkt aktuellen HCL-Website, die dem Kunden von HCL zur Verfügung gestellt wurde, oder wie in der Vereinbarung festgelegt, abgerufen werden.

|  |  |  |  |
| --- | --- | --- | --- |
| **Schweregrad** | **Definition des Schweregrades** | **Antwortzeit – Ziele** | **Antwortzeit – Abdeckung** |
| 1 | Kritische Geschäftsauswirkungen/Service-Ausfall: Geschäftskritische Funktionen funktionieren nicht oder die kritische Schnittstelle ist ausgefallen. Dies trifft in der Regel auf eine Produktionsumgebung zu und deutet auf die fehlende Zugriffsmöglichkeit auf Services hin, wodurch die Betriebsabläufe erheblich beeinträchtigt werden. Dieser Zustand erfordert eine sofortige Lösung. | Innerhalb von 1 Stunde | 24/7 |
| 2 | Bedeutender Einfluss auf die Geschäftsabläufe. Ein Leistungsmerkmal oder die Funktion des Service ist in seiner Nutzung stark eingeschränkt oder es besteht die Gefahr, dass der Kunde seine geschäftlichen Fristen nicht einhalten kann. | Innerhalb von 2 Geschäftsstunden | M-F Geschäftsstunden |
| 3 | Geringer Einfluss auf Geschäftsabläufe: Zeigt an, dass der Service oder die Funktionalität nutzbar ist und keine kritischen Einflüsse auf die Betriebsabläufe bestehen. | Innerhalb von 4 Geschäftsstunden | M-F Geschäftsstunden |
| 4 | Minimaler Einfluss auf Geschäftsabläufe: Eine Frage oder eine nicht-technische Anfrage. | Innerhalb von 1 Werktag | M-F Geschäftsstunden |

**5.1 Zugriff auf Kundendaten**

HCL kann auf Kundendaten zugreifen, um Probleme mit dem Service zu diagnostizieren und das Scannen der Kundenanwendung durch den Service zu erleichtern. HCL greift auf die Daten nur zu Zwecken der Behebung von Mängeln oder zur Unterstützung von HCL-Produkten oder -Services zu.

**6. Service-Level-Agreement**

HCL stellt die folgende Verfügbarkeit des Service-Level-Agreements ("SLA") für den Cloud-Service bereit. Das SLA stellt keine Garantie dar und ist der einzige und ausschließliche Rechtsbehelf des Kunden. Das SLA steht nur dem Kunden zur Verfügung und gilt ausschließlich für die Verwendung in Produktionsumgebungen.

**6.1 Gutschriften für die Verfügbarkeit**

Der Kunde muss innerhalb von 24 Stunden, nachdem er zum ersten Mal festgestellt hat, dass ein Vorfall mit kritischen Auswirkungen auf den Geschäftsbetrieb aufgetreten und der Cloud-Service nicht verfügbar ist, ein Support-Ticket der Fehlerklasse 1 beim HCL-Help-Desk für technische Unterstützung öffnen. Der Kunde verpflichtet sich, HCL bei der Problemdiagnose und -lösung in angemessener Weise zu unterstützen.

Ein Anspruch auf ein Support-Ticket wegen Nichteinhaltung eines SLA muss innerhalb von 3 Werktagen nach Ende des vertraglich vereinbarten Monats eingereicht werden. Die Entschädigung für einen berechtigten SLA-Anspruch wird als Gutschrift auf eine zukünftige Rechnung für den Cloud-Service auf der Grundlage der Zeitdauer gewährt, während der die Produktionssystemverarbeitung für den Cloud-Service nicht verfügbar ist ("Ausfallzeit"). Die Ausfallzeit wird ab dem Zeitpunkt gemessen, an dem der Kunde das Ereignis meldet, bis zu dem Zeitpunkt, an dem der Cloud-Service wiederhergestellt ist, und umfasst nicht die Zeit im Zusammenhang mit einem geplanten oder angekündigten Wartungsausfall, Ursachen, die außerhalb der Kontrolle von HCL liegen, Problemen mit Inhalten oder Technologie, Designs oder Anweisungen des Kunden oder Dritter, nicht unterstützten Systemkonfigurationen und Plattformen oder anderen Kundenfehlern oder vom Kunden verursachten Sicherheitsvorfällen oder Sicherheitstests. HCL wendet die höchste anwendbare Entschädigung basierend auf der kumulativen Verfügbarkeit des Cloud-Service während jedes Vertragsmonats an, wie in der folgenden Tabelle dargestellt. Die Gesamtentschädigung für einen beliebigen Vertragsmonat wird zehn Prozent (%) von einem Zwölftel (1/12) der Jahresgebühr für den Cloud-Service nicht überschreiten.

**6.2 Service-Levels**

Verfügbarkeit des Cloud-Service in einem Vertragsmonat

|  |  |
| --- | --- |
| **Verfügbarkeit in einem Vertragsmonat** | **Entschädigung (in Prozent (%) der monatlichen Abonnementgebühr\* für den Vertragsmonat, der Gegenstand des Anspruchs ist)** |
| Unter 99,9 % | 2 % |
| Unter 99 % | 5 % |
| Unter 95 % | 10 % |

\* Wurde der Cloud-Service von einem HCL-Geschäftspartner erworben, wird die monatliche Abonnementgebühr auf den zu diesem Zeitpunkt gültigen Listenpreis für den Cloud-Service, der in dem Vertragsmonat wirksam war, der Gegenstand eines Anspruchs ist, mit einem Preisnachlass von 50 % berechnet. Eine eventuelle Rückvergütung wird von HCL dem Kunden direkt zur Verfügung gestellt. Die Verfügbarkeit, ausgedrückt in Prozent, wird wie folgt berechnet: Gesamtzahl der Minuten in einem Vertragsmonat abzüglich der Gesamtzahl der Ausfallminuten in einem Vertragsmonat, dividiert durch die Gesamtzahl der Minuten in einem Vertragsmonat.

**7. Technologievorschau-Code**

Der Technologievorschau-Code (Technology Preview Code, TPC) kann in dem Programm oder in dessen Updates enthalten oder damit verteilt werden, ist aber nicht Teil des Programms. Der TPC ist unter den gleichen Bestimmungen wie das Programm lizenziert, mit Ausnahme der folgenden Bestimmungen. Der TPC wird als solches in der Benachrichtigungsdatei (oder in einer aktualisierten Benachrichtigungsdatei, die den Updates beigefügt ist) gekennzeichnet. Einige oder alle der TPCs werden möglicherweise nicht allgemein von HCL als oder in einem Produkt zur Verfügung gestellt. Der Lizenznehmer darf den TPC nur für die interne Nutzung zu Evaluierungszwecken nutzen. UNABHÄNGIG VON ANDEREN ERKLÄRUNGEN, DIE BEIM ODER VOR DEM KAUF GEMACHT WURDEN, LIEGT ES IN DER VERANTWORTUNG DES LIZENZNEHMERS, ZU BESTIMMEN, OB DAS PROGRAMM FÜR DIE WEBSITE, DIE WEBANWENDUNG ODER DIE TECHNISCHE UMGEBUNG DES LIZENZNEHMERS GEEIGNET ODER SICHER IST. DER LIZENZNEHMER ERKENNT ALLE RISIKEN AN UND AKZEPTIERT ALLE RISIKEN, DIE IM ZUSAMMENHANG MIT DER NUTZUNG DES PROGRAMMS STEHEN. Die Benachrichtigungsdatei oder die Proof-of-Concept-Vereinbarung (POC) kann diese Evaluierungsnutzung auf einen Evaluierungszeitraum beschränken. Wenn ja, muss der Lizenznehmer nach Ablauf dieser Evaluierungsperiode die Nutzung und Deinstallation des TPC einstellen. HCL stellt den TPC ohne Supportpflicht und "WIE BESEHEN" zur Verfügung, OHNE GARANTIE JEDER ART, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND, EINSCHLIESSLICH, OHNE BESCHRÄNKUNG, DER GARANTIE VON RECHTSMÄNGELN, DER NICHTVERLETZUNG ODER NICHTINTERVENTION UND DEN STILLSCHWEIGENDEN GARANTIEN UND BEDINGUNGEN DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK.

Der Lizenznehmer darf den TPC nur als programmbegleitende Übertragung an Drittparteien übertragen. Der TPC kann ein Deaktivierungsgerät enthalten, das verhindert, dass er nach Ablauf des Testzeitraums genutzt wird. Der Lizenznehmer darf dieses Deaktivierungsgerät oder den TPC nicht manipulieren. Der Lizenznehmer sollte Vorkehrungen treffen, um Datenverluste zu vermeiden, die entstehen können, wenn der TPC nicht mehr genutzt werden kann.

**8. HCL AppScan on Cloud – Zusätzliche Bedingungen**

**8.1 Sicherheitsscans**

Durch Sicherheitsscans können möglicherweise nicht alle Sicherheitsrisiken in einer Anwendung identifiziert werden, noch sind sie für den Einsatz in gefährlichen Umgebungen, die einen ausfallsicheren Betrieb erfordern, ausgelegt oder vorgesehen, einschließlich, aber nicht beschränkt auf Flugzeugnavigation, Flugverkehrskontrollsysteme, Waffensysteme, Lebenserhaltungssysteme, Nuklearanlagen oder andere Anwendungen, bei denen die Nichterkennung von Sicherheitsrisiken zum Tod, zu Personen- oder Sachschäden führen könnte. Es gibt keine Garantie dafür, dass Sicherheitsscans ununterbrochen oder fehlerfrei funktionieren.

Der HCL AppScan on Cloud kann verwendet werden, um Kunden bei der Erfüllung von Compliance-Verpflichtungen zu unterstützen, die auf Gesetzen, Verordnungen, Normen oder Verfahren beruhen können. Die vom Cloud-Service bereitgestellten Anweisungen, empfohlenen Vorgehensweisen oder Anleitungen stellen keine rechtliche, betriebswirtschaftliche oder anderweitige fachliche Beratung dar und dem Kunden wird dringend geraten, sich von juristisch oder fachlich kompetenter Stelle beraten zu lassen. Der Kunde ist allein dafür verantwortlich, dass seine Aktivitäten, Anwendungen und Systeme mit allen geltenden Gesetzen, Vorschriften, Standards und Praktiken übereinstimmen. Durch die Verwendung dieses Cloud-Service ist die Einhaltung von Gesetzen, Verordnungen, Normen oder Verfahren nicht garantiert.

Der HCL AppScan on Cloud führt invasive und nicht-invasive Tests auf der Website und der Web- oder Mobilanwendung durch, die vom Kunden zum Scannen ausgewählt wurde. Das unbefugte Eindringen in oder Zugreifen auf Computersysteme ist durch bestimmte Gesetze verboten. Der Kunde autorisiert HCL zur Ausführung der hier beschriebenen Services und erkennt an, dass der Zugriff der Services auf die Computersysteme des Kunden berechtigt ist. HCL kann diese Autorisierung Dritten gegenüber offenlegen, wenn dies zur Ausführung der Services als notwendig erachtet wird. Die Tests bergen bestimmte Risiken, einschließlich der folgenden:

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

* Die Leistung und der Durchsatz der Systeme des Kunden sowie die Leistung und der Durchsatz der zugehörigen Router und Firewalls können während der Tests vorübergehend beeinträchtigt werden;
* Es werden möglicherweise übermäßige Mengen an Protokollmeldungen erzeugt, die zu einem übermäßigen Speicherplatzverbrauch der Protokolldatei führen;
* Durch das Testen auf Sicherheitslücken könnten Daten verändert oder gelöscht werden;
* Intrusion Detection Systems (Warnsysteme gegen Angriffe von außen) können einen Alarm auslösen;
* Von der E-Mail-Funktion der getesteten Webanwendung könnten E-Mails ausgelöst werden;
* HCL AppScan on Cloud kann den Datenverkehr des überwachten Netzwerks zum Zweck der Suche nach Ereignissen abfangen.

Die von HCL zur Verfügung gestellten Rechte oder Rechtsbehelfe für Service Level Agreements, die sich auf die Websites oder Anwendungen beziehen und Gegenstand der Tests sind, werden während der Testaktivitäten aufgehoben.

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

Die HCL AppScan on Cloud kann zum Scannen von produktiven Webanwendungen konfiguriert werden. Wenn der Kunde den Scan-Typ als "Produktion" festlegt, werden die Scans so ausgeführt, dass die oben aufgeführten Risiken reduziert werden; in bestimmten Situationen kann HCL AppScan on Cloud jedoch zu einer Leistungseinbuße oder Instabilität innerhalb der getesteten Produktionsstandorte und Infrastruktur führen. HCL übernimmt keinerlei Garantien oder Zusicherungen hinsichtlich der Eignung der Verwendung des HCL AppScan on Cloud zum Scannen von Produktionssites.

ES LIEGT IN DER VERANTWORTUNG DES KUNDEN, ZU BESTIMMEN, OB DER SERVICE FÜR DIE WEBSITE, WEB- ODER MOBILE ANWENDUNG ODER DIE TECHNISCHE UMGEBUNG DES KUNDEN ANGEMESSEN ODER SICHER IST.

HCL AppScan on Cloud wurde entwickelt, um eine Vielzahl potenzieller Sicherheits- und Compliance-Probleme bei Mobil- und Webanwendungen und Webservices zu identifizieren. Es testet nicht alle Schwachstellen oder Compliance-Risiken und fungiert auch nicht als Schutz vor Sicherheitsangriffen. Da sich Sicherheitsbedrohungen, Regelungen und Standards ständig ändern, kann der Cloud-Service nicht alle Änderungen berücksichtigen. Die Sicherheit und Compliance der Webanwendung des Kunden, seiner Systeme und Mitarbeiter sowie alle Abhilfemaßnahmen liegen in der alleinigen Verantwortung des Kunden. Der Kunde entscheidet alleine über die Nutzung der vom Cloud-Service bereitgestellten Informationen.

Das unbefugte Eindringen in oder Zugreifen auf Computersysteme ist durch bestimmte Gesetze verboten. DER KUNDE IST DAFÜR VERANTWORTLICH, SICHERZUSTELLEN, DASS MIT DEM CLOUD-SERVICE NUR SEINE EIGENEN WEBSITES UND ANWENDUNGEN ODER WEBSITES UND ANWENDUNGEN GESCANNT WERDEN, FÜR DIE ER ENTSPRECHEND BERECHTIGT IST.

Zum Zwecke der Verdeutlichung umfasst der im Abschnitt Datenschutz des CSA beschriebene Kundeninhalt auch Daten, auf die HCL während der Anwendungspenetrationstests zugreifen kann.

**8.2 Datennutzung & Cookies**

Bitte lesen Sie die Informationen zur HCL-Datenschutzerklärung unter diesem Link: <https://www.hcltech.com/privacy-statement>

Der Kunde nimmt zur Kenntnis und erklärt sich damit einverstanden, dass HCL im Rahmen des normalen Betriebs und Supports des HCL AppScan on Cloud persönliche Daten vom Kunden (Mitarbeiter und Auftragnehmer des Kunden) im Zusammenhang mit der Nutzung des HCL AppScan on Cloud durch Tracking und andere Technologien erfassen kann. HCL erhebt auf diese Weise Nutzungsstatistiken und Informationen über die Effektivität des HCL AppScan on Cloud, um die Benutzererfahrung zu verbessern und / oder die Interaktion mit dem Kunden anzupassen. Der Kunde bestätigt, dass er die Zustimmung einholen wird oder eingeholt hat, um HCL zu gestatten, die gesammelten persönlichen Daten für den oben genannten Zweck innerhalb von HCL, anderen HCL-Unternehmen und deren Unterauftragnehmern, wo immer HCL und diese Unterauftragnehmer geschäftlich tätig sind, in Übereinstimmung mit dem geltenden Recht zu verarbeiten. HCL kommt Anfragen von Mitarbeitern und Auftragnehmern des Kunden nach, um auf ihre erfassten personenbezogenen Daten zuzugreifen, diese zu aktualisieren, zu korrigieren oder zu löschen.

Im Rahmen des HCL AppScan on Cloud-Service, der auch Berichtsaktivitäten umfasst, wird HCL die aus HCL AppScan on Cloud gesammelten de-identifizierten und aggregierten Daten (genannt "Sicherheitsdaten") aufbereiten und pflegen. Die Sicherheitsdaten identifizieren weder den Kunden noch eine Person, außer wie hier angegeben. Der Kunde erklärt sich außerdem damit einverstanden, dass HCL die Sicherheitsdaten nur für die folgenden Zwecke nutzen und / oder kopieren darf:

* Veröffentlichung und / oder Verbreitung der Sicherheitsdaten (z. B. in Zusammenstellungen und / oder Analysen im Zusammenhang mit der Cybersicherheit);
* Entwicklung oder Verbesserung von Produkten oder Services;
* Durchführung von Forschungen intern oder mit Dritten; und
* rechtmäßige Freigabe von bestätigten Dritttäterdaten.

**8.3 Aktivierungssoftware**

Für den Cloud-Service ist möglicherweise Aktivierungssoftware erforderlich, die der Kunde auf seine Systeme herunterladen muss, um die Nutzung des Cloud-Service zu ermöglichen. Der Kunde darf die Aktivierungssoftware nur in Verbindung mit dem Cloud-Service nutzen. Die Aktivierungssoftware wird dem Kunden unter den folgenden Bedingungen bereitgestellt:

|  |  |
| --- | --- |
| **Aktivierungssoftware** | **Geltende Lizenzbedingungen (sofern vorhanden)** |
| Static Analyzer Client-Dienstprogramm (IRX-Generator) | Bereitstellung zur Nutzung WIE BESEHEN |
| AppScan GO! | Bereitstellung zur Nutzung WIE BESEHEN |
| AppScan Presence | Bereitstellung zur Nutzung WIE BESEHEN |
| AppScan IAST Agent | Bereitstellung zur Nutzung WIE BESEHEN |