Condizioni di Utilizzo IBM (TOU) – Condizioni Specifiche dell'Offerta SaaS

IBM Application Security on Cloud

Le Condizioni di Utilizzo ("ToU") sono costituite dalle presenti Condizioni di Utilizzo IBM – Condizioni Specifiche dell'Offerta SaaS ("Condizioni Specifiche dell'Offerta SaaS") e dalle disposizioni contenute nel documento Condizioni di Utilizzo IBM - Condizioni Generali ("Condizioni Generali") disponibile alla seguente pagina web: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

In caso di discordanza, le presenti Condizioni Specifiche dell'Offerta SaaS prevalgono sulle Condizioni Generali. Ordinando, accedendo o utilizzando i servizi IBM SaaS, il Cliente accetta le Condizioni di Utilizzo (ToU).

Le presenti Condizioni di Utilizzo (ToU) sono disciplinate da IBM International Passport Advantage Agreement, IBM International Passport Advantage Express Agreement, o IBM International Agreement per l'offerta dei Servizi IBM SaaS selezionata, quando applicabili, e complessivamente costituiscono l'accordo completo tra le parti ("Accordo").

1. IBM SaaS

Le presenti Condizioni Specifiche dell'Offerta SaaS si applicano alle seguenti offerte IBM SaaS:

- IBM Application Security Analyzer

2. Calcolo dei Corrispettivi

I Servizi IBM SaaS sono venduti secondo il seguente calcolo dei corrispettivi come specificato nel Documento della Transazione:

a. **Istanza dell'Applicazione** – è un'unità di misura che consente di ottenere i servizi IBM SaaS. Per ciascuna istanza di un'Applicazione collegata ai servizi IBM SaaS è richiesta una titolarità Istanza dell'applicazione. Se un'Applicazione è composta da più componenti, ciascuno dei quali soddisfa uno scopo diverso e/o una base di utenti, e ciascuno dei quali può essere connesso a IBM SaaS o da questo monitorato, ognuno di tali componenti viene considerato come Applicazione separata. Inoltre gli ambienti di test, sviluppo, staging e produzione di un'Applicazione sono considerati come istanze separate dell'Applicazione e ciascuno di essi ha una propria titolarità. Più istanze dell'applicazione in un singolo ambiente sono tutte considerate Istanze separate dell'Applicazione e ciascuna deve avere una titolarità. È necessario ottenere titolarità sufficienti a coprire il numero di Istanze dell'applicazione connesse ai servizi IBM SaaS durante il periodo di misurazione specificato nella PoE (Proof o f Entitlement) del Cliente o nel Documento della Transazione.

b. **Accesso** – è un'unità di misura che consente di ottenere i servizi IBM SaaS. Un Accesso è il diritto di utilizzo di IBM SaaS. Il Cliente deve ottenere un'unica titolarità di Accesso al fine di utilizzare i servizi IBM SaaS durante il periodo di misurazione specificato nella PoE (Proof of Entitlement) del Cliente o nel Documento della Transazione.

3. Corrispettivi e Fatturazione

L'ammontare da pagare per i servizi IBM SaaS viene specificato nella Documentazione d'Ordine (Documento della Transazione).

3.1 Corrispettivi 'Pay per Use'

Le opzioni "Pay per Use" saranno fatturate nel mese successivo, quando il servizio viene utilizzato in base alla tariffa specificata nel Documento della Transazione.

3.2 Corrispettivo Mensile Parziale

Un Corrispettivo Mensile Parziale così come specificato nel Documento della Transazione può essere valutato proporzionalmente.

4. Supporto tecnico

Durante il Periodo di Abbonamento e dopo che IBM ha comunicato al Cliente che l'accesso ai servizi IBM SaaS è disponibile, il supporto tecnico viene fornito tramite i forum online e come supporto standard durante il periodo di tempo in cui il Cliente è soggetto ai corrispettivi 'Pay per Use'. Dall'interno dei servizi IBM SaaS, i Clienti possono inviare un ticket di assistenza o aprire una sessione di chat per assistenza.

IBM renderà disponibile la Guida al Supporto IBM Software as a Service che fornisce le informazioni di contatto e le procedure sul supporto tecnico.

Severità	Definizione di Severità	Obiettivi del Tempo di Risposta	Copertura del Tempo di Risposta
1	**inattività di servizio/impatto critico:** La funzionalità aziendale critica non è operativa oppure l'interfaccia critica non funziona. Ciò è di solito applicabile a un ambiente di produzione e indica l'impossibilità di accedere ai servizi determinando un impatto critico sulle operazioni. Questa condizione richiede una soluzione immediata.	Entro (1) un'ora	24x7
2	**Impatto aziendale significativo:** Una funzione dei servizi aziendali o una funzione del servizio è gravemente limitata nel suo utilizzo oppure il Cliente rischia di non rispettare le scadenze aziendali.	Entro due (2) ore lavorative	Ore lavorative L-V
3	**Impatto aziendale minore:** Indica che il servizio o la funzionalità è utilizzabile e non ha un impatto critico sulle operazioni.	Entro 4 ore lavorative	Ore lavorative L-V
4	**Impatto aziendale minimo:** Una domanda o una richiesta non tecnica	Entro 1 giorno lavorativo	Ore lavorative L-V

4.1 Accesso ai Dati del Cliente

IBM sarà in grado di accedere ai dati del Cliente allo scopo di eseguire una diagnosi dei problemi relativi al servizio e facilitare la scansione delle applicazioni del Cliente tramite il servizio. IBM accederà ai dati al solo scopo di correggere i difetti o per fornire supporto per i prodotti o servizi IBM.

5. Ulteriori Condizioni dell'Offerta IBM SaaS

Le Scansioni della sicurezza non possono individuare tutti i rischi della sicurezza di un'applicazione.

I servizi IBM SaaS possono essere utilizzati per aiutare il Cliente a rispettare gli obblighi di conformità, che possono essere basati su leggi, norme, standard o procedure. Qualsiasi indicazione, suggerimento sull'utilizzo o istruzione forniti dal Servizio non costituisce consiglio di tipo legale, contabile o di altro settore professionale e al Cliente viene consigliato di avvalersi della consulenza di un proprio legale o altro esperto professionale. Il Cliente è l'unico responsabile nel garantire che le sue attività, applicazioni e sistemi siano conformi con tutta la legislazione, la normativa, gli standard e le procedure applicabili. L'utilizzo di questo Servizio non garantisce l'osservanza di leggi, regole, consuetudini o procedure.

I servizi IBM SaaS eseguono test invasivi e non invasivi sul sito web e sulle applicazioni web o per dispositivi mobili che il Cliente decide di esaminare, tali test comportano dei rischi, compresi, a titolo esemplificativo, ma non esaustivo, i seguenti:

a. i sistemi computerizzati del Cliente, durante l'esecuzione delle applicazioni in fase di test, potrebbero bloccarsi o andare in crash, causando un temporaneo disservizio del sistema o la perdita di dati;

b. le prestazioni e il rendimento dei sistemi del Cliente, così come le prestazioni e il rendimento dei router e dei firewall associati, potrebbero diminuire temporaneamente;

c. è possibile che venga generata una quantità eccessiva di messaggi di log, comportando in tal modo un eccessivo consumo di spazio sul disco dedicato ai file di log;

d. alcuni dati potrebbero essere modificati o eliminati come risultato di alcune vulnerabilità del processo di "probing";

e. è possibile che scattino allarmi dei sistemi anti-Intrusione;

f. è possibile che le funzioni e-mail delle applicazioni web in fase di test inviino delle e-mail;

e

g. il servizio cloud potrebbe intercettare il traffico della rete monitorata allo scopo di cercare eventi.

Nel caso al Cliente venga richiesto di inserire le credenziali di accesso autenticate per l'applicazione sottoposta a test nel Servizio, il Cliente deve inserire solo le credenziali degli account di test e non quelle degli utenti dell'ambiente di produzione. L'utilizzo delle credenziali di accesso in un ambiente di produzione determinerebbe la trasmissione di dati personali attraverso il Servizio.

I servizi IBM SaaS possono essere configurati per la scansione delle applicazioni web di produzione. Quando il Cliente imposta il tipo di scansione come "produzione", il servizio è pensato per eseguire la scansione in modo da ridurre i rischi elencati sopra; tuttavia, in alcune situazioni il Servizio Cloud può portare a una riduzione delle prestazioni o all'instabilità all'interno dei siti e delle infrastrutture di produzione sottoposti a test. IBM non fornisce alcuna garanzia o dichiarazioni relative all'idoneità dell'utilizzo del Servizio Cloud per la scansione dei siti di produzione.

IL CLIENTE HA LA RESPONSABILITA' DI DETERMINARE SE IL SERVIZIO E' SICURO ED ADATTO AL SITO WEB, ALL'APPLICAZIONE WEB, ALL'APPLICAZIONE PER DISPOSITIVI MOBILI O ALL'AMBIENTE TECNICO DEL CLIENTE.

I servizi IBM SaaS sono progettati per identificare diversi potenziali problemi di sicurezza e conformità nelle applicazioni web e per dispositivi mobili e nei servizi web. Non verifica i rischi legati alle vulnerabilità ed alla conformità, e non funge da barriera contro gli attacchi alla sicurezza. Le minacce alla sicurezza, le normative e gli standard cambiano continuamente ed il Servizio potrebbe non riflettere tali cambiamenti. La sicurezza e la conformità delle applicazioni web del Cliente, dei suoi sistemi e dipendenti, e tutte le azioni correttive, sono di sola responsabilità del Cliente. È ad esclusiva discrezione del Cliente utilizzare o non utilizzare le informazioni fornite dal Servizio.

Il Cliente autorizza IBM ad eseguire i Servizi come descritti in questa sede e ciò anche al fine di evitare la violazione di leggi che proibiscono qualsiasi tentativo non autorizzato di penetrare o accedere ai sistemi computerizzati. IL CLIENTE DICHIARA E GARANTISCE CHE NON UTILIZZERÀ IL SERVIZIO PER MONITORARE I SITI WEB E/O LE APPLICAZIONI DIVERSE DAI SITI WEB E/O LE APPLICAZIONI DI SUA PROPRIETÀ O QUELLE DI CUI POSSIEDE IL TITOLO E L'AUTORIZZAZIONE PER PROCEDERE ALLA SCANSIONE.

5.2 Cookie

Il Cliente è consapevole ed accetta che IBM potrebbe, come parte della normale operatività e supporto dei servizi IBM SaaS, raccogliere dati personali del Cliente (dei dipendenti o dei contraenti) correlate all'utilizzo dei servizi IBM SaaS, mediante tracciamento ed altre tecnologie. IBM esegue tali attività allo scopo di raccogliere statistiche sull'utilizzo ed informazioni sull'efficacia dei servizi IBM SaaS in modo da migliorare l'esperienza dell'utente e/o personalizzare le interazioni con il Cliente. Il Cliente dichiara e garantisce di aver ottenuto o che sta per ottenere il consenso affinché IBM possa elaborare le informazioni personali, raccolte per gli scopi riportati in precedenza, all'interno di IBM, di altre società IBM e relativi subfornitori, ovunque IBM o i suoi subfornitori operino, in conformità alle leggi applicabili. IBM soddisferà le richieste di accesso, aggiornamento, correzione ed eliminazione di tali informazioni da parte di dipendenti e subfornitori.

5.3 Sedi beneficiarie dei servizi

Ove applicabili, le imposte sono calcolate in base alle sedi del Cliente beneficiarie dei servizi IBM SaaS. IBM applicherà le imposte in base all'indirizzo commerciale riportato come sede principale delle attività aziendali durante la compilazione dell'ordine di IBM SaaS, salvo diversamente indicato dal Cliente. Il Cliente è responsabile di mantenere tali informazioni aggiornate e di comunicare eventuali variazioni a IBM.

Appendice A

1. Descrizione Generale di IBM Application Security on Cloud

IBM Application Security on Cloud fornisce un'unica posizione per fornire assistenza al Cliente nella identificazione delle vulnerabilità della sicurezza (come, ad esempio, SQL Injection, Cross-Site Scripting e Data Leakage) per una varietà di applicazioni. Il servizio comprende vari tipi di tecnologie di scansione della sicurezza delle applicazioni, ciascuna delle quali identifica i problemi di sicurezza in tale applicazione.

IBM Application Security on Cloud fornisce le seguenti funzionalità:

- Applicazione per la scansione dei dispositivi mobili per la vulnerabilità della sicurezza. Tale operazione viene eseguita tramite tecnologie dinamiche di analisi della sicurezza (blackbox) e Interactive (glassbox).
- Scansione dei siti Web di produzione o pre-produzione per le vulnerabilità della sicurezza. Tale operazione viene eseguita tramite tecnologie dinamiche di analisi della sicurezza (blackbox).
- Scansione dei flussi di dati all'interno di applicazioni Web e Desktop per le vulnerabilità della sicurezza. Tale operazione viene eseguita tramite tecnologie di analisi della sicurezza statiche (whitebox).
- Report dettagliati delle vulnerabilità di sicurezza che includono sia riepiloghi di alto livello dei risultati che delle misure correttive che possono essere applicate dagli sviluppatori.
- Integrazione con diverse piattaforme DevOps come, ad esempio, Maven e IBM UrbanCode