Warunki Używania Produktów i Usług IBM — Warunki Specyficzne dla Oferty Usług SaaS

IBM Application Security on Cloud

Warunki Używania (zwane dalej „Warunkami Używania”) składają się z niniejszych „Warunków Używania Produktów i Usług IBM — Warunków Specyficznych dla Oferty Usług SaaS” (zwanych dalej „Warunkami Specyficznymi dla Oferty Usług SaaS”) oraz dokumentu pt. „Warunki Używania Produktów i Usług IBM — Warunki Ogólne” (zwanego dalej „Warunkami Ogólnymi”) dostępnego pod adresem: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

W przypadku sprzeczności Warunki Specyficzne dla Oferty Usług SaaS mają znaczenie rozstrzygające nad Warunkami Ogólnymi. Zamawiając usługę IBM SaaS, uzyskując do niej dostęp lub korzystając z niej, Klient wyraża zgodę na niniejsze Warunki Używania.

Niniejsze Warunki Używania podlegają Międzynarodowej Umowie IBM Passport Advantage, Międzynarodowej Umowie IBM Passport Advantage Express lub Międzynarodowej Umowie IBM dotyczącej Wybranych Ofert Usług IBM SaaS (zwanej dalej „Umową”), która razem z Warunkami Używania stanowi całość umowy.

1. Usługi IBM SaaS

Niniejsze Warunki Specyficzne dla Oferty Usług SaaS dotyczą następujących usług IBM SaaS:

- IBM Application Security Analyzer
- IBM Application Security Analyzer Per Scan
- IBM Application Security Analyzer Premium

2. Opłaty rozliczeniowe

Przy sprzedaży usługi IBM SaaS wysokość opłat rozliczeniowych jest ustalana na podstawie następujących miar określonych w Dokumencie Transakcyjnym:

a. Jednostką miary, według której można korzystać z usługi IBM SaaS, jest **Zadanie**. Pojęcie to oznacza obiekt w obrębie usługi IBM SaaS, który nie podlega dalszemu podziałowi i przedstawia proces przetwarzania wraz z jego wszystkimi podprocesami. Klient musi uzyskać odpowiednie uprawnienia umożliwiające obsługę łącznej liczby Zadań przetwarzanych lub zarządzanych w ramach usługi IBM SaaS w okresie pomiarowym określonym w dokumencie Proof of Entitlement lub w Dokumencie Transakcyjnym Klienta.

b. **Instancja Aplikacji** – jednostka miary, według której można korzystać z usługi IBM SaaS. Uprawnienie do Instancji Aplikacji jest wymagane dla każdej instancji Aplikacji połączonej z usługą IBM SaaS. Jeśli Aplikacja zawiera wiele komponentów, z których każdy służy do odrębnego celu i/lub obsługuje odrębną grupę użytkowników i każdy może być połączony z usługą IBM SaaS lub przez nią zarządzany, to każdy z takich komponentów jest uznawany za odrębną Aplikację. Ponadto Instancje Aplikacji w środowiskach testowych, programistycznych, produkcyjnych i środowiskach przemieszczania są uznawane za odrębne instancje Aplikacji, a każda z nich wymaga uprawnienia. Wiele Instancji Aplikacji w tym samym środowisku uznaje się za odrębne instancje Aplikacji, a każda z nich wymaga uprawnienia. Klient musi uzyskać odpowiednie uprawnienia umożliwiające obsługę stosownej liczby Instancji Aplikacji połączonych z usługą IBM SaaS w okresie pomiarowym określonym w dokumencie Proof of Entitlement (PoE) lub w Dokumencie Transakcyjnym Klienta.

c. Jednostką miary, według której można korzystać z usługi IBM SaaS, jest **Instancja**. Instancja oznacza dostęp do konkretnej konfiguracji usługi IBM SaaS. Dla każdej udostępnionej Instancji Klient musi uzyskać odpowiednie uprawnienia umożliwiające mu uzyskiwanie do niej dostępu i jej używanie w okresie pomiarowym określonym w dokumencie Proof of Entitlement (PoE) lub w Dokumencie Transakcyjnym.

   W przypadku poszczególnych uprawnień do Instancji nie obowiązuje limit liczby wykonywanych Zadań ani Instancji Aplikacji (podłączonych Aplikacji), jednakże z zastrzeżeniem że w danym momencie nie może być uruchomionych więcej niż 30 Zadań.

3. Opłaty i rozliczenia

Kwota należna do zapłaty za usługę IBM SaaS jest określona w Dokumencie Transakcyjnym.

3.1 Opłaty za używanie

Opłaty za używanie będą fakturowane w miesiącu następującym po miesiącu, w którym korzystano z usługi, według stawek określonych w Dokumencie Transakcyjnym.

3.2 Opłaty za niepełne miesiące

Opłata za niepełny miesiąc, zgodnie z treścią Dokumentu Transakcyjnego, może być naliczana w ujęciu proporcjonalnym.

4. Okres obowiązywania i możliwości odnowienia

Okres obowiązywania usługi IBM SaaS rozpoczyna się z datą powiadomienia Klienta przez IBM o udostępnieniu mu tej usługi zgodnie z dokumentem PoE. W dokumencie PoE zostanie określone, czy usługa IBM SaaS będzie odnawiana automatycznie, kontynuowana na zasadzie nieprzerwanego używania czy zakończona po upływie okresu jej obowiązywania.

W przypadku odnawiania automatycznego usługa IBM SaaS będzie automatycznie przedłużana na okres wskazany w dokumencie PoE, chyba że Klient złoży pisemny wniosek o jej nieprzedłużanie co najmniej 90 dni przed datą jej wygaśnięcia.

W przypadku kontynuacji na zasadzie nieprzerwanego używania dostępność usługi IBM SaaS będzie przedłużana z miesiąca na miesiąc, chyba że Klient wypowie ją pisemnie z wyprzedzeniem co najmniej 90 dni. Po zakończeniu takiego 90-dniowego okresu wypowiedzenia usługa IBM SaaS będzie dostępna do końca miesiąca kalendarzowego.

5. Wsparcie Techniczne

W Okresie Subskrypcji, po poinformowaniu Klienta przez IBM o dostępności usługi IBM SaaS, świadczone jest wsparcie techniczne za pośrednictwem forów internetowych oraz w ramach wsparcia standardowego w okresie, w którym Klientowi naliczane są opłaty za faktyczne wykorzystanie usługi (Pay per Use). W ramach usługi IBM SaaS Klient może wprowadzić zgłoszenie problemu lub rozpocząć sesję rozmowy sieciowej, aby uzyskać asystę. IBM udostępni „Podręcznik wsparcia do usługi IBM Software as a Service (SaaS)", który zawiera informacje kontaktowe działu wsparcia technicznego oraz inne informacje i procesy.

Poziom istotności	Definicja poziomu istotności	Docelowe czasy reakcji	Zakres czasu reakcji
1	**Krytyczne zakłócenie działalności / uniemożliwienie świadczenia usług:** Newralgiczne funkcje biznesowe nie działają lub nastąpiła awaria newralgicznego interfejsu. Zwykle dotyczy to środowiska produkcyjnego i uniemożliwia dostęp do usług, co powoduje krytyczne zakłócenia w działalności gospodarczej. Sytuacja taka wymaga natychmiastowego rozwiązania.	W 1 godzinę	24x7
2	**Istotne zakłócenie działalności:** Korzystanie z funkcji usługowych lub działanie usług zostało poważnie ograniczone lub istnieje ryzyko niedotrzymania ważnych terminów.	W 2 godziny robocze	W godzinach pracy od poniedziałku do piątku
3	**Niewielkie utrudnienie działalności:** Usługi lub funkcje mogą być używane, a problem nie powoduje krytycznego zakłócenia działalności.	W 4 godziny robocze	W godzinach pracy od poniedziałku do piątku
4	**Minimalne utrudnienie działalności:** Zapytanie lub prośba nietechniczna	W 1 dzień roboczy	W godzinach pracy od poniedziałku do piątku

5.1 Dostęp do danych Klienta

IBM będzie uzyskiwać dostęp do danych Klienta, aby diagnozować problemy z usługą i usprawniać skanowanie aplikacji przez usługę. Dostęp IBM do danych będzie ograniczony wyłącznie do celów związanych z usuwaniem defektów lub świadczeniem wsparcia do produktów lub usług IBM.

6. Warunki dodatkowe dla oferty usług IBM SaaS

Skanowanie bezpieczeństwa nie zawsze wykrywa wszystkie typy zagrożeń w aplikacji.

Usługa IBM SaaS może być wykorzystywana przez Klienta do wypełniania zobowiązań w zakresie zachowania zgodności z przepisami, normami lub procedurami. Wszelkie wskazówki, zalecenia dotyczące używania bądź porady udzielane w ramach usługi IBM SaaS nie stanowią porad prawnych bądź księgowych ani innych porad specjalistycznych, a Klientowi zaleca się uzyskanie we własnym zakresie fachowych porad radców prawnych lub innych specjalistów. Klient ponosi wyłączną odpowiedzialność za przestrzeganie wszelkich obowiązujących przepisów, norm i procedur oraz za zapewnienie zgodności swoich działań, aplikacji i systemów z takimi przepisami, normami i procedurami. Korzystanie z niniejszej Usługi nie gwarantuje osiągnięcia zgodności z jakimikolwiek przepisami, normami bądź procedurami.

Ta usługa IBM SaaS przeprowadza testy inwazyjne i nieinwazyjne serwisu WWW oraz aplikacji WWW lub aplikacji do urządzeń przenośnych wybranych przez Klienta do skanowania. Takie testowanie wiąże się z pewnymi zagrożeniami, w szczególności dotyczącymi następujących problemów:

a. Systemy komputerowe Klienta, które obsługują aplikację podlegającą testowaniu, mogą podczas testu ulec awarii lub zawiesić się, co może spowodować tymczasowy brak dostępności systemu lub utratę danych.

b. W trakcie testów może dojść do obniżenia wydajności i przepustowości systemów Klienta oraz powiązanych z nimi routerów i firewalli.

c. Testowanie może spowodować generowanie bardzo wielu komunikatów w dzienniku, a przez to prowadzić do nadmiernego wykorzystania miejsca na dysku przez pliki dziennika.

d. W wyniku sondowania słabych punktów zabezpieczeń może dojść do modyfikacji lub usunięcia danych.

e. Systemy wykrywania włamań mogą zgłaszać alarmy.

f. W wyniku testowania funkcja pocztowa testowanej aplikacji WWW może wysyłać wiadomości e-mail.

g. Usługa IBM SaaS może przejmować ruch w monitorowanej sieci w celu wyszukiwania zdarzeń.

Jeśli Klient wprowadza do Usługi uwierzytelnione dane logowania do testowanej aplikacji, powinien podawać je tylko dla kont testowych, nie użytkowników produkcyjnych. Użycie danych uwierzytelniających użytkownika produkcyjnego może spowodować udostępnianie lub przekazywanie danych osobowych za pośrednictwem Usługi.

Usługę IBM SaaS można skonfigurować tak, aby skanowała produkcyjne aplikacje WWW. Jeśli Klient wprowadzi dla typu wartość „produkcja”, to skanowanie w ramach usługi będzie przeprowadzane w sposób zmniejszający wymienione powyżej czynniki ryzyka. W niektórych sytuacjach usługa IBM SaaS może jednak spowodować zmniejszenie wydajności lub stabilności testowanych serwisów produkcyjnych i infrastruktur. IBM nie udziela żadnych gwarancji (rękojmia jest również wyłączona) ani zapewnień dotyczących przydatności usługi IBM SaaS do skanowania serwisów produkcyjnych.

ODPOWIEDZIALNOŚĆ ZA STWIERDZENIE, CZY NINIEJSZA USŁUGA JEST ODPOWIEDNIA LUB BEZPIECZNA DO UŻYTKU W POŁĄCZENIU Z SERWISEM WWW, APLIKACJĄ WWW, APLIKACJĄ DLA URZĄDZEŃ MOBILNYCH ALBO ŚRODOWISKIEM TECHNICZNYM KLIENTA, SPOCZYWA NA KLIENCIE.

Niniejsza usługa IBM SaaS służy do identyfikowania szeregu potencjalnych problemów z bezpieczeństwem i zgodnością z przepisami w aplikacjach WWW, aplikacjach dla urządzeń mobilnych i usługach WWW. Usługa nie testuje wszystkich słabych punktów i czynników ryzyka w zakresie zgodności z przepisami ani nie zapewnia ochrony przed atakami naruszającymi bezpieczeństwo. Zagrożenia, przepisy i standardy nieustannie się zmieniają, a niniejsza Usługa może nie uwzględniać wszystkich tych zmian. Klient ponosi wyłączną odpowiedzialność za bezpieczeństwo i zachowanie zgodności z przepisami w swoich aplikacjach WWW i systemach oraz przez swoich pracowników, a także za

podejmowanie ewentualnych działań naprawczych. Kwestia wykorzystania lub niewykorzystania informacji udostępnionych przez Usługę pozostaje całkowicie w gestii Klienta.

Niektóre systemy prawne zakazują nieautoryzowanych prób penetracji lub uzyskiwania dostępu do systemów komputerowych. KLIENT MA OBOWIĄZEK UPEWNIĆ SIĘ, ŻE NIE UŻYWA USŁUGI DO SKANOWANIA SERWISÓW I/LUB APLIKACJI WWW INNYCH NIŻ SWOJE WŁASNE SERWISY I APLIKACJE WWW LUB TAKIE SERWISY I APLIKACJE WWW, DO KTÓRYCH SKANOWANIA KLIENT JEST UPRAWNIONY.

6.1 Informacje cookie

Klient przyjmuje do wiadomości i uznaje, że w ramach normalnej obsługi i wsparcia usługi IBM SaaS IBM może gromadzić dane osobowe pochodzące od Klienta (dotyczące jego pracowników i wykonawców), które mają związek z używaniem usługi IBM SaaS, za pomocą mechanizmów śledzenia i innych technologii. IBM gromadzi w ten sposób dane statystyczne dotyczące używania usługi IBM SaaS i informacje na temat skuteczności jej działania, które służą do podnoszenia poziomu obsługi użytkowników i/lub dostosowywania interakcji z Klientem. Klient potwierdza, że uzyskał lub uzyska zgodę na to, aby zezwolić IBM na przetwarzanie zgromadzonych danych osobowych w powyższym celu w obrębie IBM, innych spółek IBM i przedsiębiorstw ich podwykonawców wszędzie tam, gdzie podmioty te prowadzą działalność, zgodnie z obowiązującym prawem. IBM na żądanie umożliwi pracownikom i wykonawcom Klienta dostęp do tych informacji kontaktowych oraz ich aktualizację, korygowanie i usuwanie.

6.2 Miejsce osiągania korzyści pochodnych

Podatki, o ile mają zastosowanie, są oparte na miejscu lub miejscach, które Klient określi jako miejsca osiągania korzyści z usługi IBM SaaS. IBM będzie stosować podatki na podstawie adresu działalności, który Klient poda podczas zamawiania usługi IBM SaaS jako główne miejsce osiągania korzyści, chyba że Klient dostarczy IBM dodatkowe informacje. Klient odpowiada za aktualizowanie tych informacji i informowanie IBM o każdej ich zmianie.

Dodatek A

1. IBM Application Security on Cloud General Description

Usługa IBM Application Security on Cloud pomaga w wykrywaniu słabych punktów zabezpieczeń różnych aplikacji pod kątem takich zagrożeń jak wstrzyknięcie SQL, ataki cross-site scripting i wycieki danych. Obejmuje ona różnego typu techniki skanowania bezpieczeństwa, z których każda wykrywa problemy w danej aplikacji.

IBM Application Security on Cloud udostępnia następujące funkcje:

- Scanning Mobile Applications (skanowanie aplikacji dla urządzeń mobilnych) — wykrywanie słabych punków zabezpieczeń za pomocą dynamicznych (blackbox) i interaktywnych (glassbox) technologii analizy bezpieczeństwa.
- Skanowanie produkcyjnych lub przedprodukcyjnych stron WWW, udostępnianych publicznie lub w sieci prywatnej, w celu wykrycia słabych punktów zabezpieczeń za pomocą dynamicznych (blackbox) technik analizy bezpieczeństwa.
- Skanowanie przepływów danych w aplikacjach WWW i aplikacjach komputerowych pod kątem słabych punktów zabezpieczeń za pomocą statycznych (whitebox) technik analizy bezpieczeństwa.
- Szczegółowe raporty dotyczące słabych punktów zabezpieczeń zawierające ogólne podsumowania wyników i środki zaradcze, które mogą zastosować programiści.
- Integracja z różnymi platformami DevOps.