IBM Application Security on Cloud

Niniejszy opis dotyczy Usługi Przetwarzania w Chmurze, którą IBM oferuje Klientowi. „Klient” oznacza tu przedsiębiorstwo wraz z jego autoryzowanymi użytkownikami i odbiorcami Usługi Przetwarzania w Chmurze. Odpowiednia Oferta Cenowa i dokument Proof of Entitlement (PoE) są dostarczane jako odrębne Dokumenty Transakcyjne.

1. Usługa Przetwarzania w Chmurze

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 interaktywnych (glassbox) technik 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.

1.1 IBM Application Analyzer

Rozwiązanie IBM Application Analyzer można zamówić w wariancie rozliczanym według Instancji Aplikacji lub według Zadania (skanowania) bądź jako Instancję pełną. Umożliwia ono następujące rodzaje skanowania:

- Dynamic Analyzer – testowanie serwisów WWW w środowisku przedprodukcyjnym lub produkcyjnym za pomocą techniki DAST,
- Mobile Analyzer – testowanie plików binarnych w systemach operacyjnych iOS lub Android za pomocą techniki IAST,
- Static Analyzer – testowanie przepływu danych kodu bajtowego lub kodu źródłowego za pomocą techniki SAST.

1.2 Usługa konfigurowania

IBM Application Security on Cloud Consulting Services to oferowana w postaci produktu usługa konfigurowania rozwiązania Application Analyzer. W ramach tej Usługi konsultanci IBM udzielają asysty i poradnictwa z zakresu testów i zarządzania ryzykiem bezpieczeństwa aplikacji. Usługi IBM Application Security on Cloud Consulting Services są nabywane w postaci bloków Przedsięwzięć, których ilości określone poniżej można przeznaczać na zamawianie i używanie następujących usług:

a. **Fast Start** [wykorzystanie 1 (jednej) jednostki Przedsięwzięcia]

Usługa Fast Start obejmuje udostępnienie wiedzy specjalistycznej i poradnictwa na temat używania funkcji testowania i zarządzania ryzykiem w ramach usługi Application Security on Cloud. Gdy Klient potwierdzi pomyślne zalogowanie w portalu usługi Application Security on Cloud, IBM przeprowadzi konferencję WWW trwającą maksymalnie 2 (dwie) godziny dla maksymalnie 2 (dwóch) aktywnych uczestników, aby przeszkolić ich z zakresu podstawowych konfiguracji i funkcji usługi AppSec on Cloud, w tym rodzajów skanowania, uruchamiania procesów skanowania, przeglądania raportów oraz instalowania powiązanych narzędzi i wtyczek. Świadczenie usługi Fast Start kończy się po (a) przeprowadzeniu webinarium szkoleniowego dla Klienta, (b) zainstalowaniu odpowiednich narzędzi i wtyczek oraz (c) udzieleniu Klientowi asysty przy konfigurowaniu i uruchamianiu pierwszego skanowania.

b. **Assessment Review** [wykorzystanie 2 (dwóch) jednostek Przedsięwzięcia]

Usługa Assessment Review polega na zapewnieniu asysty podczas przeglądania wyników testu, co obejmuje analizę i ustalanie priorytetów czynności naprawczych dotyczących słabych punktów zabezpieczeń w aplikacji. IBM przeprowadzi konferencję WWW trwającą maksymalnie 1 (jedną) godzinę dla maksymalnie 2 (dwóch) aktywnych uczestników, w ramach której dokona przeglądu wykrytych słabych punktów zabezpieczeń oraz ogólnych zagrożeń bezpieczeństwa w aplikacji. Konferencja będzie obejmować również szczegółowe omówienie wykrytych słabych punktów zabezpieczeń aplikacji, w tym (1) sposobu testowania słabego punktu zabezpieczeń, (2) sposobu wykrycia słabego punktu zabezpieczeń, (3) ryzyka związanego z poszczególnymi słabymi punktami zabezpieczeń oraz (4) ogólnych rekomendacji dotyczących naprawy, które ułatwią usunięcie danego słabego punktu zabezpieczeń. Przegląd będzie oparty wyłącznie na wynikach testu i nie będzie dotyczył samego kodu źródłowego. Klient dokona przeglądu wyników testu i przed konferencją WWW wskaże IBM wynik testu, który ma być poddany przeglądowi. Świadczenie usługi Assessment Review kończy się po zakończeniu konferencji WWW.

c. **Scan for Me** [wykorzystanie 4 (czterech) jednostek Przedsięwzięcia]

Usługa Scan for Me polega na udostępnieniu specjalisty IBM ds. bezpieczeństwa aplikacji, który skonfiguruje i uruchomi skanowanie, sprawdzi poprawność wyników i przeprowadzi briefing poświęcony raportowi, aby przejrzeć ustalenia. Klient zezwoli konsultantowi IBM na dostęp do swojego środowiska ASoC w celu skonfigurowania i uruchomienia skanowania, sprawdzenia poprawności wyników, przekazania rekomendacji w sprawie wyznaczenia priorytetów działań naprawczych oraz przeprowadzenia briefingu poświęconego raportowi z wyników. IBM przeprowadzi konferencję WWW trwającą maksymalnie 1 (jedną) godzinę dla maksymalnie 2 (dwóch) aktywnych uczestników, w ramach której dokona przeglądu wykrytych słabych punktów zabezpieczeń oraz ogólnych zagrożeń bezpieczeństwa w aplikacji. Konferencja będzie obejmować również szczegółowe omówienie wykrytych słabych punktów zabezpieczeń aplikacji, w tym (1) sposobu testowania słabego punktu zabezpieczeń, (2) sposobu wykrycia słabego punktu zabezpieczeń, (3) ryzyka związanego z poszczególnymi słabymi punktami zabezpieczeń oraz (4) ogólnych rekomendacji dotyczących naprawy, które ułatwią usunięcie danego słabego punktu zabezpieczeń. Na żądanie przedstawione najpóźniej 30 dni po skanowaniu początkowym IBM ponownie przeprowadzi skanowanie przy użyciu początkowej konfiguracji, wyłącznie w celu sprawdzenia poprawki zabezpieczeń, sprawdzenia poprawności wyników i dostarczenia raportu Klientowi (a nie w celu testowania nowej funkcjonalności). Świadczenie usługi Scan for Me kończy się po zakończeniu konferencji WWW poświęconej przeglądowi wyników skanowania początkowego lub ewentualnie po zakończeniu ponownego skanowania na żądanie Klienta i po dostarczeniu Klientowi raportu na ten temat.

d. **Advisor on Demand** [wykorzystanie 7 (siedmiu) jednostek Przedsięwzięcia]

Usługa Advisor on Demand obejmuje maksymalnie 20 (dwadzieścia) godzin czasu konsultanta IBM, który można przeznaczyć na czynności związane z Usługą Przetwarzania w Chmurze. Konsultant IBM zapewni asystę w zakresie tematów związanych z bezpieczeństwem aplikacji, a w szczególności kwestii zarządzania programami, ustalania priorytetów dla testowania bezpieczeństwa, strategii działań naprawczych oraz analizy i naprawy kodu źródłowego. IBM podejmie współpracę z Klientem w celu utworzenia i przeanalizowania harmonogramu projektu z uwzględnieniem konkretnych wymagań Klienta, w tym celów projektów, odpowiednich technologii, pożądanych ram czasowych, oczekiwanych materiałów oraz szacunkowej liczby przedsięwzięć przeznaczonych na usługę Advisor on Demand. Klient musi zapewnić dostęp do niezbędnych aplikacji, systemów i dokumentacji w zakresie wymaganym do wykonania usług. Świadczenie usługi Advisor on Demand kończy się po dwudziestu godzinach przekazywania wiedzy specjalistycznej dotyczącej bezpieczeństwa i/lub po dostarczeniu Klientowi harmonogramu projektu i/lub udokumentowanych materiałów, które zostały sprecyzowane w harmonogramie projektu.

e. **Testy Penetracyjne Aplikacji**

Trzy opcje:

(1) **Podstawowy Test Penetracyjny Aplikacji / Test Penetracyjny Aplikacji pod kątem zgodności** – usługa obejmująca maksymalnie 40 (czterdzieści) godzin czasu Konsultanta, przy czym tematyka konsultacji jest skoncentrowana na błędach logiki w procesach jednostopniowych oraz prostszych wersjach mechanizmów do wstrzyknięcia błędów. Wykorzystuje ona 15 (piętnaście) jednostek Przedsięwzięcia.

(2) **Standardowy Test Penetracyjny Aplikacji** – usługa obejmująca maksymalnie 60 (sześćdziesiąt) godzin czasu Konsultanta, przy czym tematyka konsultacji jest rozszerzona o błędy logiki w wielostopniowych przepływach pracy, złożone wersje mechanizmów do wstrzyknięcia błędów oraz analizę złożonych typów danych. Wykorzystuje ona 21 (dwadzieścia jeden) jednostek Przedsięwzięcia.

(3) **Zaawansowany Test Penetracyjny Aplikacji**

Usługa obejmująca maksymalnie 80 (osiemdziesiąt) godzin czasu Konsultanta, przy czym tematyka konsultacji jest rozszerzona o odtwarzanie kodu źródłowego skompilowanych plików wykonywalnych, rozbiór niestandardowych protokołów sieciowych na elementy składowe oraz skrupulatną analizę publicznie dostępnych bibliotek i środowisk. Wykorzystuje ona 27 (dwadzieścia siedem) jednostek Przedsięwzięcia.

W ramach usługi Testów Penetracyjnych Aplikacji pracownik IBM przeprowadza testy aplikacji i eksploatuje ją, dostarcza raport z testów oraz wyjaśnia ustalone fakty i powiązane z nimi czynniki ryzyka podczas briefingu poświęconego raportowi.

IBM zorganizuje na rozpoczęcie projektu rozmowę telefoniczną trwającą maksymalnie 1 (jedną) godzinę dla maksymalnie 2 (dwóch) aktywnych uczestników, której celem będzie przegląd środowiska i organizacji Klienta, w tym platformy aplikacji, architektury, środowisk programistycznych, infrastruktury pomocniczej, znanych problemów dotyczących bezpieczeństwa i zagrożeń związanych z aplikacją, wstępnego harmonogramu testów oraz planu kontaktów awaryjnych.

IBM przeprowadzi Testy Penetracyjne Aplikacji obejmujące w szczególności: zidentyfikowanie powszechnie spotykanych słabych punktów zabezpieczeń, takich jak podatność na wstrzyknięcie SQL i ataki cross-site scripting, ocenę silnych i słabych stron istniejących mechanizmów zabezpieczeń, takich jak sprawdzanie poprawności danych wejściowych, uwierzytelnianie, upoważnianie, sprawdzanie prawidłowego egzekwowania logiki biznesowej, sprawdzanie poprawności używania bezpiecznych protokołów, identyfikowanie błędów w obsłudze sesji, sprawdzanie prawidłowości mechanizmów zabezpieczeń dotyczących logowania, odzyskiwania hasła, strategii haseł oraz innych funkcji do zarządzania użytkownikami. Ustalenia zostaną udokumentowanie w raporcie z Testów Penetracyjnych Aplikacji. IBM przeprowadzi briefing poświęcony raportowi podczas konferencji WWW trwającej maksymalnie 1 (jedną) godzinę. Świadczenie usługi Testów Penetracyjnych Aplikacji kończy się po wykorzystaniu przydzielonego czasu na konsultacje, przeprowadzeniu konferencji WWW i dostarczeniu Klientowi ostatecznego raportu z Testów Penetracyjnych Aplikacji.

1.2.1 Obowiązki Stron w ramach usług konfigurowania

IBM zobowiązuje się:

- świadczyć Usługi Konfigurowania z wykorzystaniem jednostek Przedsięwzięcia nabytych przez Klienta oraz zgodnie z warunkami zamówienia Klienta;
- zakończyć świadczenie Usługi Konfigurowania w momencie spełnienia kryteriów zakończenia opisanych w paragrafie 1.2.

Klient zobowiązuje się:

- ponosić odpowiedzialność za wszystkie opłaty związane z wnioskami dotyczącymi Przedsięwzięcia składanymi przez Klienta w okresie obowiązywania;
- ponadto Klient potwierdza, że nabyte jednostki Przedsięwzięcia muszą zostać wykorzystane w początkowym okresie obowiązywania, gdyż w przeciwnym razie utracą ważność;
- złożyć formalny wniosek o wykonanie wszystkich Usług Konfigurowania na przynajmniej 30 dni przed datą zakończenia subskrypcji.

Podczas wykonywania jakiejkolwiek Usługi Konfigurowania IBM może zażądać od Klienta informacji i współpracy w uzasadnionym zakresie. Niedostarczenie żądanych informacji lub niepodjęcie współpracy przez Klienta w odpowiednim czasie może skutkować nałożeniem określonych przez IBM opłat za jednostki Przedsięwzięcia, zależnie od wymagań wynikających z usług lub z opóźnienia w wykonaniu odpowiedniej usługi.

Aby IBM mógł przeprowadzić testy w sposób dokładny, Klient zobowiązuje się przestrzegać wydanych przez IBM instrukcji dotyczących przygotowywania i konserwowania środowiska w okresie testów.

2. Opis zabezpieczeń

W odniesieniu do niniejszej Usługi Przetwarzania w Chmurze stosowane są zasady ochrony danych i prywatności dla usług IBM SaaS, dostępne pod adresem http://www.ibm.com/cloud/data-security, a także ewentualne dodatkowe zasady określone w niniejszym paragrafie. Żadna zmiana zasad ochrony danych i prywatności IBM nie zmniejszy bezpieczeństwa Usługi Przetwarzania w Chmurze.

Niniejsza Usługa Przetwarzania w Chmurze nie została zaprojektowana z myślą o spełnieniu konkretnych wymagań w zakresie bezpieczeństwa dla zawartości podlegającej regulacjom, takiej jak dane osobowe oraz dane osobowe objęte szczególną ochroną. Klient ponosi odpowiedzialność za stwierdzenie, czy Usługa Przetwarzania w Chmurze spełnia jego wymagania w zakresie typu zawartości, której Klient będzie używać w połączeniu z tą Usługą.

IBM nie występuje jako dostawca usług regulowanych przez Federalną Komisję Łączności („FCC") lub urzędy państwowe („Regulatorzy Państwowi") i nie zamierza świadczyć żadnych usług podlegających takim regulacjom. Jeśli FCC lub Regulator Państwowy nałoży wymagania lub obowiązki prawne na jakiekolwiek usługi świadczone przez IBM na mocy niniejszych Warunków, IBM może: (a) zmodyfikować lub zastąpić odpowiednie produkty na koszt Klienta i/lub (b) zmienić sposób świadczenia tych usług na rzecz Klienta, tak aby uniknąć stosowania takich wymagań lub obowiązków wobec IBM (na przykład IBM może wystąpić jako agent Klienta nabywający dane usługi od operatora publicznego będącego osobą trzecią).

3. Wsparcie techniczne

W okresie subskrypcji, po poinformowaniu Klienta przez IBM o dostępności Usługi Przetwarzania w Chmurze, 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 Przetwarzania w Chmurze Klient może wprowadzić zgłoszenie problemu lub rozpocząć sesję rozmowy sieciowej, aby uzyskać asystę. IBM udostępni „Podręcznik wsparcia dla 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 zgłoszenie nietechniczne.	W 1 dzień roboczy	W godzinach pracy od poniedziałku do piątku

3.1 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.

4. Informacje o uprawnieniach i rozliczaniu

4.1 Opłaty rozliczeniowe

Przy sprzedaży Usługi Przetwarzania w Chmurze wysokość opłat rozliczeniowych jest ustalana na podstawie następujących miar, zgodnie z Dokumentem Transakcyjnym:

a. Jednostką miary, według której można korzystać z Usługi Przetwarzania w Chmurze, jest **Zadanie**. Pojęcie to oznacza obiekt w obrębie Usługi Przetwarzania w Chmurze, 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 Przetwarzania w Chmurze w okresie pomiarowym określonym w Dokumencie Zamówienia Klienta.

b. Jednostką miary, według której można korzystać z Usługi Przetwarzania w Chmurze, jest **Instancja Aplikacji**. Uprawnienie do Instancji Aplikacji jest wymagane dla każdej instancji Aplikacji połączonej z Usługą Przetwarzania w Chmurze. 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 Przetwarzania w Chmurze 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 Przetwarzania w Chmurze w okresie pomiarowym określonym w dokumencie PoE lub Dokumencie Transakcyjnym Klienta.

   W przypadku tej Usługi Przetwarzania w Chmurze Instancje Aplikacji to kolejne skanowania pojedynczej aplikacji, zdefiniowane w następujący sposób:

   - W przypadku Testów Dynamicznych: serwis WWW identyfikowany za pomocą publicznego lub prywatnego adresu URL. Każda Instancja Aplikacji uprawnia do serwisu obejmującego maksymalnie 5000 stron w pojedynczej domenie.
   - W przypadku Testów Statycznych: jednostka kodu stworzonego dla jednego środowiska wykonywalnego. Każda Instancja Aplikacji uprawnia do przeglądania jednostek kodu zawierających maksymalnie 1 mln wierszy.
   - W przypadku Testów Rozwiązań Mobilnych: jednostka kodu binarnego, którą można wykonać na urządzeniu mobilnym. Poszczególne platformy mobilne (np. iOS oraz Android) stanowią różne Instancje Aplikacji.

c. Jednostką miary, według której można korzystać z Usługi Przetwarzania w Chmurze, jest **Instancja**. Instancja oznacza dostęp do konkretnej konfiguracji Usługi Przetwarzania w Chmurze. 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.

d. Jednostką miary, według której można korzystać z usług, jest **Przedsięwzięcie**. Przedsięwzięcie obejmuje usługi specjalistyczne i/lub szkoleniowe związane z Usługą Przetwarzania w Chmurze. Klient musi uzyskać odpowiednie uprawnienia umożliwiające obsługę każdego Przedsięwzięcia.

4.2 Opłaty za niepełne miesiące

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

4.3 Opłaty za przekroczenie limitu

Jeśli rzeczywiste wykorzystanie Usługi Przetwarzania w Chmurze w okresie pomiarowym przekroczy uprawnienia określone w dokumencie PoE, Klientowi zostanie naliczona opłata za przekroczenie limitu zgodnie z postanowieniami Dokumentu Transakcyjnego.

4.4 Opłaty wstępne

Klient zostanie obciążony opłatą za konfigurowanie według stawki określonej w Dokumencie Transakcyjnym.

5. Okres obowiązywania i możliwości odnowienia

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

W przypadku odnawiania automatycznego Usługa Przetwarzania w Chmurze będzie automatycznie przedłużana na okres wskazany w dokumencie PoE, chyba że Klient złoży pisemny wniosek o jej nieprzedłużanie co najmniej 30 dni przed datą jej wygaśnięcia.

W przypadku kontynuacji na zasadzie nieprzerwanego używania dostępność Usługi Przetwarzania w Chmurze będzie przedłużana z miesiąca na miesiąc, chyba że Klient wypowie ją pisemnie z wyprzedzeniem co najmniej 30 dni. Po zakończeniu takiego 30-dniowego okresu wypowiedzenia Usługa Przetwarzania w Chmurze będzie dostępna do końca miesiąca kalendarzowego.

6. Warunki dodatkowe

Przeglądy bezpieczeństwa nie są sposobem na zidentyfikowanie wszystkich zagrożeń bezpieczeństwa w aplikacji. Ponadto przeglądy bezpieczeństwa nie zostały zaprojektowane z myślą o używaniu w środowiskach niebezpiecznych wymagających bezawaryjnego działania i nie są przeznaczone do użycia w takich środowiskach. W szczególności dotyczy to systemów nawigacji lotniczej, systemów kontroli lotów, systemów uzbrojenia, systemów podtrzymujących funkcje życiowe, urządzeń nuklearnych oraz wszelkich innych zastosowań, w przypadku których niezidentyfikowanie zagrożeń bezpieczeństwa może prowadzić do śmierci bądź uszkodzeń ciała lub mienia. Nie można zagwarantować, że przeglądy bezpieczeństwa będą przebiegać w sposób nieprzerwany lub wolny od błędów.

Usługa ta 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 Przetwarzania w Chmurze 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 Przetwarzania w Chmurze nie gwarantuje osiągnięcia zgodności z jakimikolwiek przepisami, normami bądź procedurami.

Ta Usługa Przetwarzania w Chmurze przeprowadza testy inwazyjne i nieinwazyjne serwisu WWW oraz aplikacji WWW lub aplikacji dla urządzeń mobilnych wybranych przez Klienta do skanowania. Niektóre systemy prawne zakazują nieautoryzowanych prób penetracji lub uzyskiwania dostępu do systemów komputerowych. Klient upoważnia IBM do świadczenia Usług zgodnie z opisem w niniejszym dokumencie oraz potwierdza, że świadczenie Usług stanowi autoryzowany dostęp do systemów komputerowych Klienta. IBM może ujawnić osobie trzeciej informację o udzieleniu powyższego upoważnienia, jeśli uzna to za niezbędne do świadczenia Usług.

Testowanie wiąże się z pewnymi zagrożeniami, a w szczególności:

a. Systemy komputerowe Klienta, które obsługują aplikacje podlegające 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 krótkotrwałego 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 Przetwarzania w Chmurze może przejmować ruch w monitorowanej sieci w celu wyszukiwania zdarzeń.

Wszelkie prawa lub zadośćuczynienia udzielane przez IBM z tytułu Umowy dotyczącej Poziomu Usług i mające związek z serwisami WWW lub aplikacjami poddawanymi testom zostaną wyłączone na czas czynności związanych z testowaniem.

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

Usługę Przetwarzania w Chmurze 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 Przetwarzania w Chmurze 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 Przetwarzania w Chmurze do skanowania serwisów produkcyjnych.

ODPOWIEDZIALNOŚĆ ZA STWIERDZENIE, CZY NINIEJSZA USŁUGA PRZETWARZANIA W CHMURZE 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 Przetwarzania w Chmurze 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 ulegają nieustannym zmianom, a niniejsza Usługa Przetwarzania w Chmurze 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 Przetwarzania w Chmurze 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 PRZETWARZANIA W CHMURZE 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.

W celu zachowania jasności zaznacza się, że należąca do Klienta zawartość opisana w paragrafie „Ochrona danych" Umowy dotyczącej Usługi Przetwarzania w Chmurze obejmuje także dane, które mogą zostać udostępnione IBM podczas Testów Penetracyjnych Aplikacji.

6.1 Systemy należące do osób trzecich

W odniesieniu do systemów (przy czym na potrzeby niniejszego postanowienia pojęcie to oznacza w szczególności aplikacje i adresy IP) należących do osoby trzeciej, które będą poddawane testom na mocy niniejszej umowy, Klient zobowiązuje się:

a. otrzymać od właściciela każdego systemu podpisany dokument, który upoważnia IBM do świadczenia Usług na danym systemie i potwierdza akceptację przez odpowiedniego właściciela warunków określonych w sekcji „Uprawnienie do wykonania testów", a także dostarczyć IBM egzemplarz takiego upoważnienia zanim IBM rozpocznie testy systemu należącego do osoby trzeciej;

b. ponosić wyłączną odpowiedzialność za informowanie odpowiedniego właściciela o wszelkich czynnikach ryzyka, obszarach zagrożenia i słabych punktach zabezpieczeń zidentyfikowanych w danym systemie w ramach testów zdalnych prowadzonych przez IBM;

c. przygotować i prowadzić wymianę informacji między właścicielem systemu a IBM w zakresie uznanym za konieczny przez IBM.

Klient zobowiązuje się:

- natychmiast informować IBM o wszelkich zmianach własności każdego systemu poddawanego testom na mocy niniejszego dokumentu;
- bez uprzedniej pisemnej zgody IBM nie ujawniać poza przedsiębiorstwem Klienta materiałów dostarczanych ani faktu, że IBM wykonał Usługi;
- w pełni zabezpieczać i chronić IBM przed wszelkimi szkodami i odpowiedzialnością na skutek roszczeń osoby trzeciej wynikających z nieprzestrzegania przez Klienta wymagań niniejszego paragrafu zatytułowanego „Systemy należące do osób trzecich", a także przed wszelkimi wezwaniami i roszczeniami skierowanymi przeciwko IBM lub jego podwykonawcom bądź agentom przez osoby trzecie w związku z (a) testami zagrożeń bezpieczeństwa, obszarów zagrożenia lub słabych punktów zabezpieczeń systemów poddawanych testom na mocy niniejszego dokumentu, (b) dostarczaniem wyników tych testów Klientowi lub (c) wykorzystywaniem bądź ujawnieniem tych wyników przez Klienta.

6.2 Informacje cookie

Klient przyjmuje do wiadomości i zgadza się, że IBM w ramach normalnej obsługi i wsparcia Usługi Przetwarzania w Chmurze może gromadzić dane osobowe Klienta, jego pracowników i wykonawców, dotyczące używania Usługi Przetwarzania w Chmurze, za pomocą mechanizmów śledzenia i innych technologii. IBM gromadzi informacje i dane statystyczne dotyczące używania i efektywności Usługi Przetwarzania w Chmurze, aby zapewnić użytkownikom lepszą obsługę i/lub dostosować usługę do ich wymagań. 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.

W ramach Usługi Przetwarzania w Chmurze, która obejmuje czynności z zakresu raportowania, IBM będzie przygotowywać i utrzymywać informacje pozbawione danych identyfikacyjnych oraz informacje zagregowane, pochodzące z Usługi Przetwarzania w Chmurze („Dane dotyczące Bezpieczeństwa"). Dane dotyczące Bezpieczeństwa nie mogą umożliwiać zidentyfikowania Klienta ani innych osób fizycznych z zastrzeżeniem postanowień punktu (d) poniżej. Klient zezwala IBM na wykorzystywanie i/lub kopiowanie Danych dotyczących Bezpieczeństwa wyłącznie w celu:

a. publikowania i/lub dystrybuowania Danych dotyczących Bezpieczeństwa (np. w opracowaniach i/lub analizach związanych z cyberbezpieczeństwem);
b. opracowywania i udoskonalania produktów i usług;
c. prowadzenia badań we własnym zakresie i z udziałem osób trzecich;
d. udostępniania zgodnie z prawem potwierdzonych informacji na temat sprawcy będącego osobą trzecią.

6.3 Oprogramowanie Pomocnicze

Ta Usługa Przetwarzania w Chmurze obejmuje Oprogramowanie Pomocnicze, z którego Klient może korzystać tylko w powiązaniu z tą usługą w okresie jej obowiązywania.