IBM Application Security on Cloud

Uvjeti upotrebe ("ToU") sastoje se od ovih IBM-ovih Uvjeta upotrebe – Uvjeti za određene SaaS ponude ("Uvjeti za određene SaaS ponude") i dokumenta nazvanog IBM-ovi Uvjeti upotrebe – Opći uvjeti ("Opći uvjeti") dostupnom na sljedećem URL-u: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

U slučaju sukoba, SaaS Uvjeti za određene SaaS ponude imaju prednost pred Općim uvjetima. Naručivanjem, pristupanjem ili korištenjem IBM SaaS-a Klijent prihvaća Uvjete upotrebe (ToU).

Uvjete upotrebe (ToU) uređuje IBM Međunarodni Passport Advantage ugovor, IBM Međunarodni Passport Advantage Express ugovor ili IBM Međunarodni ugovor za Izabrane IBM SaaS ponude, ovisno što se primjenjuje ("Ugovor"), koji zajedno s Uvjetima upotrebe čine cjeloviti ugovor.

1. IBM SaaS

Ovi Uvjeti za određene SaaS ponude odnose se na sljedeće IBM SaaS ponude:

- IBM Application Security Analyzer

2. Metrike naplate

IBM SaaS se prodaje u skladu sa sljedećim metrikama naplate navedenim u Transakcijskom dokumentu:

a. **Instanca aplikacije** – je jedinica mjere po kojoj se može dobiti IBM SaaS. Ovlaštenje Instance aplikacije je potrebno za svaku instancu Aplikacije koja je povezana na IBM SaaS. Ako Aplikacija ima više komponenti, pri čemu svaka ima posebnu svrhu i od kojih svaka može biti povezana ili upravljana od IBM SaaS-a, svaka takva komponenta se smatra zasebnom Aplikacijom. Dodatno, testna, razvojna, postavljačka i proizvodna okolina za Aplikaciju se svaka smatra zasebnom instancom Aplikacije i svaka mora imati ovlaštenje. Ako postoji više instanci Aplikacije u jednoj okolini, svaka se smatra zasebnom instancom Aplikacije i za svaku je potrebno ovlaštenje. Moraju se dobiti Ovlaštenja koja su dostatna za pokrivanje broja Instanci aplikacije navedenih u IBM SaaS-u za vrijeme perioda mjerenja navedenog u Klijentovom Dokazu o ovlaštenju (PoE) ili Transakcijskom dokumentu.

b. **Pristup** - je jedinica mjere po kojoj se može dobiti IBM SaaS. Pristup je pravo korištenja IBM SaaS-a. Klijent mora dobiti jedno pravo Pristupa da bi mogao koristiti IBM SaaS za vrijeme perioda mjerenja koji je naveden u Dokazu o ovlaštenju (PoE) ili Transakcijskom dokumentu Klijenta.

3. Naknade i naplata

Iznos koji se plaća za IBM SaaS naveden je u transakcijskom dokumentu.

3.1 Naplata po upotrebi

Račun za opciju Naplate po upotrebi izdat će se u sljedećem mjesecu kada je usluga korištena po cijeni navedenoj u Transakcijskom dokumentu.

3.2 Djelomična mjesečna naknada

Na temelju razmjerne procjene može se izračunati djelomična mjesečna naknada, kako je navedeno u transakcijskom dokumentu.

4. Tehnička podrška

Za vrijeme Perioda pretplate i nakon što IBM obavijesti Klijenta da mu je dostupan pristup na IBM SaaS, pruža se tehnička podrška za IBM SaaS putem online foruma i standardna podrška tijekom perioda u kojem je Klijent izložen Naplati po upotrebi. Klijenti mogu unutar IBM SaaS-a predati prijavu podrške ili otvoriti sesiju chata u kojoj će zatražiti pomoć. IBM će pružiti Priručnik za podršku za IBM Software as a Service koji sadrži informacije o kontaktiranju tehničke podrške i druge informacije i procese.

Ozbiljnost	Definicija ozbiljnosti	Ciljana vremena odgovora	Pokrivenost za vremena odgovora
1	**Kritičan utjecaj na poslovanje/prekid rada usluge:** Funkcionalnost kritična za poslovanje ne radi ili se dogodila greška sučelja od kritične važnosti. Ovo se obično odnosi na proizvodnu okolinu i označava da se ne može pristupiti uslugama, što ima kritičan utjecaj na operacije. Ovo stanje mora se odmah riješiti.	Unutar jednog sata	24x7
2	**Značajan utjecaj na poslovanje:** Poslovna komponenta ili funkcija usluge ima ozbiljno smanjenu mogućnost upotrebe ili se pojavila opasnost prekoračivanja krajnjih rokova u poslovanju.	Unutar 2 radna sata	Radno vrijeme od ponedjeljka do petka
3	**Manji utjecaj na poslovanje:** Označava da je usluga ili funkcionalnost upotrebljiva i nema kritičan utjecaj na operacije.	Unutar 4 radna sata	Radno vrijeme od ponedjeljka do petka
4	**Minimalan utjecaj na poslovanje:** Upit ili zahtjev koji se ne odnosi na tehničke probleme	Unutar 1 radnog dana	Radno vrijeme od ponedjeljka do petka

4.1 Pristup podacima Klijenta

IBM će moći pristupiti Klijentovim podacima u svrhu dijagnosticiranja problema s uslugom i omogućavanja pregledavanja Klijentove aplikacije od strane usluge. IBM će pristupiti podacima samo u svrhu popravljanja oštećenja ili za davanje podrške za IBM proizvode ili usluge.

5. Dodatni uvjeti za IBM SaaS ponude

Sigurnosni pregledi možda neće otkriti sve sigurnosne rizike u aplikaciji.

IBM SaaS može se koristiti kao pomoć Klijentu kod ispunjavanja obveza usklađenosti, koje mogu biti temeljene na propisima, pravilima, standardima ili praksi. Bilo koje upute, predložena upotreba ili smjernice dobivene od Usluge ne smatraju se pravnim, računovodstvenim ili drugim profesionalnim savjetima i Klijenta se upozorava da potraži vlastito pravno ili drugo profesionalno savjetovanje. Isključivo je Klijent odgovoran za osiguravanje da Klijent i Klijentove aktivnosti, aplikacije i sustavi poštuju sve mjerodavne propise, pravila, standarde i prakse koji se primjenjuju. Upotreba ove Usluge ne garantira usklađenost s bilo kojim propisom, pravilom, standardom ili praksom.

IBM SaaS izvodi invazivna i neinvazivna testiranja web stranice i web ili mobilne aplikacije koju Klijent odluči pregledati, a ta testiranja uključuju određene rizike, uključujući, ali ne ograničavajući se na sljedeće:

a. tijekom izvođenja aplikacija za vrijeme testiranja, Klijentovi računalni sustavi mogu prestati reagirati ili se srušiti, što rezultira privremenom nedostupnošću sustava ili gubitkom podataka;

b. performanse i propusnost Klijentovih sustava i performanse i propusnost povezanih usmjerivača i vatrozida mogu biti privremeno sniženi za vrijeme testiranja;

c. mogu se generirati ogromne količine poruka dnevnika, što rezultira prekomjernom potrošnjom prostora na disku od strane datoteke dnevnika;

d. podaci mogu biti promijenjeni ili izbrisani u sklopu istraživanja ranjivosti;

e. mogu se aktivirati alarmi ili sustavi za otkrivanje upada;

f. funkcija e-pošte u aplikaciji koja se testira može aktivirati slanje e-pošte;

i

g. cloud usluga može presresti promet nadgledane mreže za potrebe traženja događaja.

U slučaju da Klijent unosi ovlaštene pristupne podatke za prijavu u aplikaciju koja se testira u Usluzi, Klijent bi trebao unositi takve pristupne podatke samo za testne račune, a ne za proizvodne korisnike. Upotreba pristupnih podataka proizvodnog korisnika može rezultirati prijenosom osobnih podataka preko Usluge.

IBM SaaS se može konfigurirati za pregledavanje proizvodnih web aplikacija. Kada Klijent postavi tip pregledavanja na "proizvodni", usluga je dizajnirana za izvođenje pregledavanja na način koji će smanjiti rizike navedene iznad; međutim, u određenim situacijama Cloud usluga može uzrokovati snižene performanse ili nestabilnost unutar testiranih proizvodnih lokacija i infrastrukture. IBM ne daje nikakva jamstva ili izjave vezano uz prikladnost korištenja Cloud usluge za pregledavanje proizvodnih lokacija.

KLIJENT JE ODGOVORAN UTVRDITI DA LI JE USLUGA PRIKLADNA ILI SIGURNA ZA KLIJENTOVU WEB STRANICU, WEB APLIKACIJU, MOBILNU APLIKACIJU ILI TEHNIČKU OKOLINU.

IBM SaaS dizajniran je za otkrivanje raznovrsnih potencijalnih problema vezanih uz sigurnost i usklađenost u mobilnim i web aplikacijama i web uslugama. Ne testira sve propuste ili rizike vezane uz usklađenost niti ne predstavlja prepreku za sigurnosne napade. Sigurnosne prijetnje, propisi i standardi konstantno se mijenjaju i Usluga možda neće odražavati sve takve promjene. Isključivo je Klijent odgovoran za sigurnost i usklađenost Klijentove web aplikacije, sustava i zaposlenika i radnje koje se poduzimaju za ispravljanje problema. Isključivo je Klijentova odluka hoće li koristiti bilo koje informacije dostupne u Usluzi.

Određeni propisi zabranjuju bilo kakve neovlaštene pokušaje probijanja ili pristupanja računalnim sustavima. KLIJENTOVA JE ODGOVORNOST POBRINUTI SE DA KLIJENT NE KORISTI USLUGU ZA PREGLEDAVANJE BILO KOJIH WEB STRANICA I/ILI APLIKACIJA OSIM ONIH KOJE SU U VLASNIŠTVU KLIJENTA ILI KOJE KLIJENT IMA PRAVO I OVLAŠTENJE PREGLEDAVATI.

5.2 Cookieji

Klijent je svjestan i prihvaća da IBM može, kao dio uobičajene aktivnosti i podrške za IBM SaaS, prikupiti osobne informacije od Klijenta (vaših zaposlenika i ugovaratelja) koje se odnose na korištenje IBM SaaS-a, kroz praćenje i druge tehnologije. IBM to radi da bi prikupio korisne statističke podatke i podatke o učinkovitosti našeg IBM SaaS-a u svrhu poboljšanja korisničkog iskustva i/ili podešavanja interakcije s Klijentom. Klijent potvrđuje da će pribaviti ili je pribavio pristanak koji dozvoljava IBM-u da obrađuje prikupljene osobne podatke za gore navedenu svrhu unutar IBM-a, drugih IBM-ovih poduzeća i njihovih podugovarača, na svim lokacijama gdje mi i naši podugovarači poslujemo u skladu s mjerodavnim pravom. IBM će se pridržavati zahtjeva Klijentovih zaposlenika i ugovaratelja vezanih za pristup, ažuriranje, ispravke ili brisanje njihovih prikupljenih osobnih podataka.

5.3 Lokacije koje primaju izvedenu korist

Gdje je to primjenjivo, porezi se temelje na lokaciji (ili lokacijama) za koje Klijent navede da primaju korist od IBM SaaS-a. IBM će primijeniti poreze koristeći poslovnu adresu navedenu kod naručivanja IBM SaaS-a kao primarnu lokaciju koja prima korist, osim ako Klijent ne dostavi dodatne podatke IBM-u. Klijent je odgovoran održavati takve informacije ažurnima i dostaviti sve promjene IBM-u.

Dodatak A

1. IBM Application Security on Cloud - opći opis

IBM Application Security on Cloud pruža jedinstveno mjesto koje je pomoći Klijentu da identificira sigurnosne ranjivosti (na primjer umetanje SQL-a, skriptiranje između lokacija i curenje podataka) za razne aplikacije. Usluga uključuje različite tipove tehnika skeniranja sigurnosti aplikacije koje utvrđuju sigurnosne probleme u toj aplikaciji.

IBM Application Security on Cloud pruža sljedeće mogućnosti:

- Skeniranje mobilnih aplikacija radi otkrivanja sigurnosnih ranjivosti. Izvodi se pomoću dinamičkih (blackbox) i interaktivnih (glassbox) tehnologija analize sigurnosti.
- Skeniranje proizvodnih ili predproizvodnih web stranica radi otkrivanja sigurnosnih ranjivosti. Izvodi se pomoću dinamičkih (blackbox) tehnika analize sigurnosti.
- Skeniranje tokova podataka unutar mrežnih i stolnih aplikacija radi otkrivanja sigurnosnih ranjivosti. Izvodi se pomoću statičkih (whitebox) tehnika analize sigurnosti.
- Detaljni izvještaji o sigurnosnim ranjivostima, koji sadrže sažetke rezultata na visokoj razini i korake za ispravljanje koje programeri mogu slijediti.
- Integracija s različitim DevOps platformama, kao što su Maven i IBM UrbanCode