IBM Application Security on Cloud

Podmínky užívání ("ToU") sestávají z těchto dokumentů IBM: podmínek užívání - Podmínek specifických pro nabídku IBM SaaS ("Podmínky specifické pro nabídku IBM SaaS") a z dokumentu nazvaného IBM podmínky užívání - Všeobecné podmínky ("Všeobecné podmínky"), které jsou dostupné na následující adrese: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

V případě rozporu mají Podmínky specifické pro nabídku IBM SaaS přednost před Všeobecnými podmínkami. Objednáním, přístupem nebo užíváním IBM SaaS vyjadřuje Zákazník svůj souhlas s těmito Podmínkami užívání.

Podmínky užívání se řídí podmínkami Mezinárodní smlouvy IBM Passport Advantage, Mezinárodní smlouvy IBM Passport Advantage Express nebo Mezinárodní smlouvy IBM pro vybrané nabídky IBM SaaS, podle toho, co je relevantní ("Smlouva"), a spolu s Podmínkami užívání tvoří úplnou smlouvu.

1. IBM SaaS

Tyto Podmínky specifické pro nabídku IBM SaaS se vztahují na následující nabídky IBM SaaS:

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

2. Metriky poplatků

IBM SaaS je prodávána na základě níže uvedených metrik poplatků, jak je uvedeno v Transakčním dokumentu:

a. **Úloha** – je měrnou jednotkou, na jejímž základě lze získat IBM SaaS. Úloha je objekt v rámci IBM SaaS, který nelze dále dělit a který představuje proces výpočetního zpracování včetně všech jeho podprocesů. Je nutné získat dostatečný počet oprávnění, který bude pokrývat celkový počet Úloh zpracovaných nebo spravovaných prostřednictvím služby IBM SaaS během období měření uvedeného v Dokumentu o oprávnění (Proof of Entitlement) Zákazníka nebo v Transakčním dokumentu.

b. **Instance aplikace** – je měrnou jednotkou, na jejímž základě lze získat IBM SaaS. Pro každou Aplikaci připojenou k IBM SaaS je vyžadováno oprávnění Instance aplikace. Pokud má Aplikace více komponent, každá z nich slouží k jinému účelu nebo jiné uživatelské základně a každá z nich může být připojena k nabídce IBM SaaS nebo může být nabídkou spravována, považuje se každá taková komponenta za samostatnou Aplikaci. Navíc testovací, vývojové, fázovací a produktivní prostředí Aplikace se považují za samostatné instance Aplikace a každé toto prostředí musí mít oprávnění. Více Instancí aplikace v jednom prostředí se považuje za samostatné instance Aplikace a oprávnění musí mít každá z nich. Je nutno získat dostatečný počet Oprávnění, který bude pokrývat počet Instancí aplikace připojených k IBM SaaS během období měření uvedeného v Dokumentu o oprávnění (Proof of Entitlement) nebo v Transakčním dokumentu Zákazníka.

c. **Instance** – je měrnou jednotkou, na jejímž základě lze získat IBM SaaS. Instance je přístup ke specifické konfiguraci IBM SaaS. Pro každou Instanci IBM SaaS zpřístupněnou a používanou během období měření uvedeného v Dokumentu o oprávnění (Proof of Entitlement) nebo v Transakčním dokumentu je nutno získat dostatečný počet oprávnění.

   Pro jednotlivá oprávnění Instance neexistuje omezení počtu prováděných Úloh ani Instancí aplikace (připojených Aplikací). Současně lze však spustit maximálně 30 Úloh.

3. Poplatky a fakturace

Výše platby za IBM SaaS je specifikována v Transakčním dokumentu.

3.1 Poplatky typu Pay per Use

Poplatky typu Pay per Use budou fakturovány v měsíci následujícím po použití služby, a to za sazbu uvedenou v Transakčním dokumentu.

3.2 Poplatky za neúplný měsíc

Poplatek za neúplný měsíc uvedený v Transakčním dokumentu bude stanoven na poměrném základě.

4. Smluvní období a možnost obnovení

Smluvní období pro poskytování IBM SaaS začíná datem, kdy IBM Zákazníkovi oznámí, že mu byl udělen přístup ke službě IBM SaaS, jak je uvedeno v Dokumentu o oprávnění (Proof of Entitlement). Dokument o oprávnění určí, zda se IBM SaaS obnovuje automaticky, je používána nepřetržitě, nebo zda je po uplynutí smluvního období ukončena.

V případě automatického obnovení platí, že pokud Zákazník neposkytne 90 dní před datem ukončení období písemné oznámení o záměru nabídku neobnovit, bude nabídka IBM SaaS automaticky obnovena na období uvedené v Dokumentu o oprávnění (Proof of Entitlement).

V případě průběžného používání bude nabídka IBM SaaS dále dostupná na měsíční bázi, dokud Zákazník neposkytne 90 dní předem písemnou výpověď. IBM SaaS zůstane po ukončení takového 90denního období na konci kalendářního měsíce k dispozici.

5. Technická podpora

Během Období registrace a poté, co IBM Zákazníkovi oznámí, že přístup k IBM SaaS je k dispozici, je technická podpora poskytována prostřednictvím online fór a jako standardní podpora během období, ve kterém jsou Zákazníkovi účtovány poplatky typu Pay per Use. Z IBM SaaS mohou Zákazníci odeslat tiket podpory nebo zahájit relaci konverzace a požádat o asistenci. IBM zpřístupní Software IBM jako Příručku podpory služby, která poskytuje informace o technické podpoře a další informace a procesy.

Závažnost	Definice Závažnosti	Cílové hodnoty doby odezvy	Pokrytí doby odezvy
1	**Kritický dopad na obchodní činnost/selhání služby:** Funkčnost, která je rozhodující pro obchodní činnost, není provozuschopná nebo došlo k selhání kritického rozhraní. Tato Závažnost se obvykle vztahuje na produktivní prostředí a označuje neschopnost přístupu ke službám, která má za následek kritický dopad na provoz. Tento stav vyžaduje okamžité řešení.	Do jedné hodiny	24 hodin, 7 dní v týdnu
2	**Významný dopad na obchodní činnost:** Obchodní komponenty nebo funkce služby jsou, pokud jde o jejich užívání, vážně omezeny nebo hrozí nedodržení obchodních termínů.	Do dvou hodin (v průběhu pracovní doby)	Pondělí až pátek, v průběhu pracovní doby
3	**Mírný dopad na obchodní činnost:** Službu nebo funkčnost lze používat a dopad na provoz není kritický.	Do čtyř hodin (v průběhu pracovní doby)	Pondělí až pátek, v průběhu pracovní doby
4	**Minimální dopad na obchodní činnost:** Dotaz nebo netechnický požadavek	Do jednoho pracovního dne	Pondělí až pátek, v průběhu pracovní doby

5.1 Přístup k Datům Zákazníka

IBM bude mít možnost přistupovat k datům Zákazníka pro účely diagnostiky problémů se službou a podpory skenování vaší aplikace službou. IBM bude k datům přistupovat pouze pro účely opravy vad a poskytnutí podpory pro produkty nebo služby IBM.

6. Dodatečné podmínky pro nabídky IBM SaaS

Bezpečnostní skenování nemusí identifikovat všechna rizika v aplikaci.

IBM SaaS je nástroj, který pomáhá Zákazníkovi zajistit dodržování závazků, jež pro něj mohou vyplývat z právních předpisů, zákonných a jiných standardů nebo postupů. Jakékoli instrukce, informace týkající se doporučeného užívání nebo jiné pokyny, které Zákazník získá prostřednictvím Služby, nepředstavují právní, účetní nebo jinou odbornou radu a Zákazník by si měl obstarat svou vlastní právní nebo jinou odbornou konzultaci. Zákazník nese výhradní odpovědnost za dodržování všech příslušných právních předpisů, směrnic, standardů a postupů. Totéž platí pro všechny jeho činnosti, aplikace a systémy. Užívání této Služby nezaručuje soulad s právními předpisy, nařízeními, standardy nebo postupy.

IBM SaaS provádí invazivní a neinvazivní testy na webových serverech a webových nebo mobilních aplikacích, které se Zákazník rozhodne skenovat; takové testování znamená určité riziko, včetně - bez omezení - následujících rizik:

a. počítačové systémy Zákazníka se mohou během testování aplikací zablokovat nebo se mohou zhroutit, což může mít za následek dočasnou nedostupnost systému nebo ztrátu dat;

b. výkon a propustnost systémů Zákazníka a rovněž výkon a propustnost souvisejících směrovačů a ochranných bariér mohou být během testování dočasně sníženy;

c. může být generováno nadměrné množství zpráv protokolu, což může mít za následek nadměrnou spotřebu prostoru na disku pro soubory protokolu;

d. data mohou být změněna nebo vymazána v důsledku testování ohrožení zabezpečení;

e. systémy pro detekci proniknutí do systému mohou spustit alarmy;

f. e-mailová funkce testované webové aplikace může spustit e-maily;

g. služba IBM SaaS může zachytit provoz monitorované sítě pro účely hledání událostí.

V případě, že Zákazník použije ověřená přihlašovací pověření pro testovanou aplikaci do Služby, je povinen používat taková pověření pouze pro testovací účty, a nikoli pro produktivní uživatele. Použití pověření produktivních uživatelů může mít za následek přenos osobních údajů přes Službu.

IBM SaaS lze nakonfigurovat ke skenování produktivních webových aplikací. Pokud Zákazník nastaví typ skenování na "produktivní", služba bude provádět skenování způsobem, který sníží rizika uvedená výše; v některých situacích však služba IBM SaaS může způsobit snížení výkonu nebo nestabilitu testovaných produktivních webů a infrastruktury. Společnost IBM neposkytuje žádné záruky ani garance s ohledem na vhodnost použití služby IBM SaaS ke skenování produktivních webů.

ZÁKAZNÍK NESE ODPOVĚDNOST ZA URČENÍ, ZDA JE SLUŽBA VHODNÁ ČI BEZPEČNÁ PRO JEHO WEBOVÝ SEVER, WEBOVOU APLIKACI, MOBILNÍ APLIKACI NEBO TECHNICKÉ PROSTŘEDÍ.

IBM SaaS je určena k identifikaci širokého spektra potenciálních problémů týkajících se zabezpečení a dodržování právních předpisů v oblasti mobilních a webových aplikací a služeb. Netestuje všechna ohrožení zabezpečení nebo všechna rizika v oblasti dodržování právních předpisů, ani nefunguje jako bariéra proti útokům na zabezpečení. Bezpečnostní rizika, regulace a standardy se průběžně mění a Služba nemůže všechny takové změny zohledňovat. Zákazník odpovídá za zabezpečení svých webových aplikací, systémů a zaměstnanců a za dodržování právních předpisů a rovněž za jakékoli nápravné akce samostatně. Záleží výhradně na uvážení Zákazníka, zda bude, či nebude využívat jakékoli informace poskytnuté Službou.

Příslušné zákony zakazují jakýkoli neoprávněný pokus o proniknutí do počítačových systémů nebo pokus o přístup do počítačových systémů. ZÁKAZNÍK JE POVINEN ZAJISTIT, ABY SLUŽBA NEBYLA POUŽÍVÁNA KE SKENOVÁNÍ JAKÝCHKOLI JINÝCH WEBOVÝCH SERVERŮ A/NEBO APLIKACÍ, NEŽ JSOU WEBOVÉ SERVERY A/NEBO APLIKACE VE VLASTNICTVÍ ZÁKAZNÍKA NEBO WEBOVÉ SERVERY A/NEBO APLIKACE, K JEJICHŽ SKENOVÁNÍ MÁ ZÁKAZNÍK OPRÁVNĚNÍ.

6.2 Soubory cookie

Zákazník si je vědom a souhlasí, že IBM smí v rámci své běžné obchodní činnosti a podpory služeb IBM SaaS od Zákazníka (zaměstnanců a smluvních partnerů Zákazníka) shromažďovat osobní údaje týkající se užívání služeb IBM SaaS prostřednictvím sledovacích a jiných technologií. IBM tak činí za účelem získání statistik užívání a informací o efektivitě služeb IBM SaaS, které IBM umožní zlepšit zkušenosti uživatelů a/nebo přizpůsobit interakce se Zákazníkem na míru. Zákazník potvrzuje, že získá nebo získal souhlas, který IBM uděluje oprávnění zpracovávat, v souladu s příslušnými právními předpisy, shromážděné osobní údaje pro výše uvedené účely v rámci IBM, jiných společností IBM a jejích subdodavatelů, kdekoli IBM a její subdodavatelé provádějí obchodní činnost. IBM vyhoví požadavkům zaměstnanců a smluvních partnerů Zákazníka, pokud jde o přístup, aktualizaci, opravu nebo vymazání jejich shromážděných osobních údajů.

6.3 Lokality, v nichž jsou využívány výhody

V případech, kdy je to relevantní, budou daně založeny na lokalitě(ách), kterou(é) Zákazník uvedl jako místo, kde využívá výhod služeb IBM SaaS. IBM uplatní daně na základě obchodní adresy, která byla při objednání služby IBM SaaS uvedena jako primární lokalita pro využívání výhod, pokud Zákazník IBM neposkytne doplňující informace. Zákazník nese odpovědnost za aktualizaci takových informací a za informování IBM o jakýchkoli změnách.

Příloha A

1. Všeobecný popis služby IBM Application Security on Cloud

IBM Application Security on Cloud je místem, které Zákazníkovi poskytuje asistenci s identifikací zranitelných míst v zabezpečení (jako například SQL injection, cross-site scripting nebo únik dat) pro řadu aplikací. Služba zahrnuje řadu různých typů a technik skenování zabezpečení aplikace identifikujících problémy se zabezpečením dané aplikace.

IBM Application Security on Cloud poskytuje následující funkce:

- Skenování mobilních aplikací z hlediska zranitelných míst v zabezpečení. Skenování probíhá prostřednictvím dynamických (blackbox) a interaktivních (glassbox) technologií analýzy zabezpečení.
- Skenování produktivních a preprodukčních webových serverů ve veřejné nebo soukromé síti z hlediska ohrožení zabezpečení. Skenování probíhá prostřednictvím dynamických (blackbox) technik analýzy zabezpečení.
- Skenování datových toků webových a desktop aplikací z hlediska zranitelných míst v zabezpečení. Skenování probíhá prostřednictvím statických (whitebox) technik analýzy zabezpečení.
- Podrobné sestavy týkající se zranitelných míst v zabezpečení, které zahrnují souhrny zjištění a kroky k nápravě, podle kterých mohou vývojáři postupovat.
- Integrace s různými platformami DevOps.