IBM Application Security on Cloud

Pogoje uporabe ("Pogoji uporabe") sestavljajo ti IBM-ovi pogoji uporabe – pogoji posebne ponudbe SaaS ("Pogoji posebne ponudbe SaaS") in dokument IBM-ovi pogoji uporabe – splošni pogoji ("Splošni pogoji"), ki so na voljo na naslednjem naslovu URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

V primeru navzkrižja med splošnimi pogoji in pogoji posebne ponudbe SaaS prevladajo slednji. Naročnik z naročilom ali uporabo ponudbe IBM SaaS oziroma dostopanjem do nje soglaša s pogoji uporabe.

Pogoje uporabe ureja veljavna IBM-ova pogodba International Passport Advantage oz. International Passport Advantage Express ("pogodba"), ki skupaj s pogoji uporabe predstavlja celotno pogodbo.

1. IBM SaaS

Za naslednje ponudbe IBM SaaS veljajo ti pogoji posebne ponudbe SaaS:

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

2. Metrike zaračunavanja

Ponudba IBM SaaS se prodaja v skladu z naslednjo metriko zaračunavanja, določeno v transakcijskem dokumentu:

a. **Opravilo** je merska enota, na podlagi katere je mogoče pridobiti ponudbo IBM SaaS. Opravilo je objekt v ponudbi IBM SaaS, ki ga ni mogoče dalje deliti in predstavlja postopek računanja, ki vključuje vse svoje podprocese. Naročnik mora pridobiti primerna pooblastila, da z njimi pokrije skupno število opravil, ki jih ponudba IBM SaaS obdela ali upravlja v obdobjem merjenja, navedenim v naročnikovem dokazilu o upravičenosti (PoE) ali transakcijskem dokumentu.

b. **Primerek aplikacije** je merska enota, s katero je mogoče pridobiti ponudbo IBM Saas. Pooblastilo za primerek aplikacije je potrebno za vsak primerek aplikacije, ki je povezan s ponudbo IBM SaaS. Če ima aplikacija več komponent, pri čemer je vsaka posvečena drugačnemu namenu in/ali bazi uporabnikov ter je lahko vsaka povezana s ponudbo IBM SaaS oz. jo ponudba SaaS upravlja, se vsaka takšna komponenta šteje kot ločena aplikacija. Prav tako se preizkusno, razvojno, uprizoritveno in produkcijsko okolje aplikacije vsako posebej šteje kot ločen primerek aplikacije in mora imeti svoje pooblastilo. Če je v enem samem okolju več primerkov aplikacije, se vsak posebej šteje kot ločen primerek aplikacije in mora imeti svoje pooblastilo. Naročnik mora pridobiti zadostna pooblastila, da z njimi pokrije število primerkov aplikacije, ki so povezani s ponudbo IBM SaaS v obdobju merjenja, določenim v naročnikovem dokazilu o upravičenosti (PoE) ali transakcijskem dokumentu.

c. **Primerek** – je merska enota, na podlagi katere si je mogoče zagotoviti IBM SaaS. Primerek je dostop do določene konfiguracije storitve IBM SaaS. Naročnik mora pridobiti zadostna pooblastila za vsak primerek ponudbe IBM SaaS, za katerega sta omogočena dostop in uporaba v meritvenem obdobju, navedenem v naročnikovem dokazilu o upravičenosti (PoE) ali transakcijskem dokumentu.

   Za vsako pooblastilo primerka ni omejitve glede števila izvedenih opravil ali primerkov aplikacij (povezanih aplikacij), a le če se v določenem času ne izvaja več kot 30 opravil.

3. Stroški in zaračunavanje

Znesek, ki ga je treba plačati za ponudbo IBM SaaS, je naveden v transakcijskem dokumentu.

3.1 Plačilo glede na uporabo

Možnosti plačila na podlagi uporabe bodo zaračunane v mesecu, ki sledi, uporabi storitve in to po ceni, določeni v transakcijskem dokumentu.

3.2 Delni mesečni strošek

Delni mesečni strošek, kot je naveden v transakcijskem dokumentu, se lahko oceni na podlagi sorazmernega deleža.

4. Trajanje in možnosti podaljšanje

Naročniško obdobje za ponudbo IBM SaaS se začne z dnem, ko IBM obvesti naročnika, da ima na voljo dostop do ponudbe IBM SaaS, v skladu z navedbami v dokazilu o upravičenosti. V dokazilu o upravičenosti bo navedeno, ali se naročnina na IBM SaaS podaljša samodejno, se nadaljuje na podlagi neprekinjene uporabe, ali se konča ob izteku naročniškega obdobja.

Na podlagi samodejnega podaljšanja se bo naročnina na ponudbo IBM SaaS samodejno podaljševala za obdobje, navedeno v dokazilu o upravičenosti, razen če naročnik posreduje pisno obvestilo o prenehanju podaljšanja najmanj 90 dni pred iztekom naročniškega obdobja.

Na podlagi neprekinjene uporabe bo ponudba IBM SaaS neprestano na voljo iz meseca v mesec, dokler naročnik ne posreduje 90-dnevnega predhodnega obvestila o odpovedi. Ponudba IBM SaaS bo na voljo do konca koledarskega meseca po izteku takšnega 90-dnevnega obdobja.

5. Tehnična podpora

Tekom naročniškega obdobja in po tem ko IBM obvesti naročnika, da je na voljo dostop do ponudbe IBM SaaS, je tehnična podpora zagotovljena prek spletnih forumov in kot standardna podpora tekom časovnega obdobja, v katerem za naročnika nastane obveznost plačila glede na uporabo. Znotraj ponudbe IBM SaaS lahko naročniki predložijo prijavo za podporo ali začnejo sejo klepeta za pomoč. IBM bo omogočil dostop do priročnika za podporo SaaS, ki vsebuje kontaktne informacije o tehnični podpori ter druge informacije in postopke.

Resnost	Definicija resnosti	Ciljni odzivni čas	Kritje odzivnega časa
1	**Odločilen vpliv na poslovanje/izpad storitve:** Nedelovanje funkcije, ki je nujna za poslovanje, ali izpad nujno potrebnega vmesnika. To običajno velja za produkcijsko okolje in pomeni nezmožnost dostopanja do storitev, kar ima odločilen vpliv na delovanje. To stanje zahteva takojšnjo rešitev.	V roku 1 ure	24 ur na dan, 7 dni v tednu
2	**Velik vpliv na poslovanje:** Uporaba poslovne funkcije storitve ali delovanja storitve je zelo omejena in naročniku grozi, da bo zamudil poslovne roke.	V roku 2 delovnih ur	Delovni čas od ponedeljka do petka
3	**Manjši vpliv na poslovanje:** Označuje, da je storitev ali funkcijo mogoče uporabljati in težava nima odločilnega vpliva na postopke.	V roku 4 delovnih ur	Delovni čas od ponedeljka do petka
4	**Minimalen vpliv na poslovanje:** Poizvedba ali netehnična zahteva	V roku 1 delovnega dne	Delovni čas od ponedeljka do petka

5.1 Dostop do naročnikovih podatkov

IBM bo lahko dostopal do naročnikovih podatkov za namen diagnosticiranja težav s storitvijo in podpore pregledom naročnikove aplikacije s strani storitve. IBM bo dostopal do podatkov samo za namene odpravljanja napak ali zagotavljanja podpore za IBM-ove produkte in storitve.

6. Dodatni pogoji ponudbe IBM SaaS

Z varnostnimi pregledi morda ne bodo zaznana vsa varnostna tveganja v aplikaciji.

Ponudba IBM SaaS lahko naročniku pomaga pri doseganju skladnosti, ki lahko temelji na zakonih, predpisih, standardih ali praksah. Vsa navodila, predlagana uporaba ali smernice, ki jih zagotavlja storitev, ne predstavljajo pravnih, računovodskih ali drugih strokovnih nasvetov in naročnika se opozori, naj pridobi svojega pravnega ali drugega strokovnega svetovalca. Naročnik sam odgovarja, da skupaj s svojimi dejavnostmi, aplikacijami in sistemi izpolnjuje zahteve veljavne zakonodaje, predpisov, standardov in praks. Uporaba te storitve ne jamči skladnosti z zakonodajo, predpisi, standardi ali dobrimi praksami.

Ponudba IBM SaaS izvaja invazivna in neinvazivna preizkušanja spletnega mesta in spletnih ali mobilnih aplikacij, ki jih naročnik izbere za optično branje, preizkušanja katerih pa vključujejo določena tveganja, kar med drugim vključuje naslednje:

a. Naročnikovi računalniški sistemi se lahko med izvajanjem aplikacij, ki se preizkušajo, prenehajo odzivati ali se sesujejo, kar lahko povzroči začasno nedostopnost sistema ali izgubo podatkov;

b. zmogljivost in prepustnost naročnikovih sistemov ter zmogljivost in prepustnost povezanih usmerjevalnikov in požarnih zidov so lahko med preizkušanjem začasno zmanjšani;

c. generirajo se lahko prekomerne količine dnevniških sporočil, kar vodi v prekomerno porabo prostora na disku zaradi dnevniških datotek;

d. podatki se lahko spremenijo ali izbrišejo kot posledica pregleda ranljivosti;

e. sistemi zaznavanja vdorov lahko sprožijo alarme;

f. zaradi preizkušanja funkcije elektronske pošte v spletni aplikaciji se lahko sproži elektronska pošta;

g. IBM SaaS lahko prestreže promet nadzorovanega omrežja za namen iskanja dogodkov.

V primeru, da naročnik za prijavo v aplikacijo, ki se preizkuša, v storitev vnese overjene poverilnice, naj naročnik vnese samo poverilnice za preizkusne račune, in ne za produkcijske uporabnike. V primeru uporabe poverilnic produkcijskega uporabnika se lahko zgodi, da bodo osebni podatki preneseni prek storitve.

Ponudbo IBM SaaS je mogoče konfigurirati za optično branje produkcijskih spletnih aplikacij. Če odjemalec nastavi vrsto skeniranja kot 'proizvodnja', zasnova storitve izvede skeniranje na način, ki zmanjšuje tveganja, navedena zgoraj; v nekaterih primerih pa lahko IBM SaaS privede do poslabšanja delovanja ali nestabilnosti v testiranih produkcijskih spletnih mestih in infrastrukturi. IBM ne daje nobenih jamstev glede primernosti uporabe ponudbe IBM SaaS za skeniranje produkcijskih spletnih mest.

NAROČNIKOVA ODGOVORNOST JE, DA UGOTOVI, ALI JE STORITEV PRIMERNA ALI VARNA ZA NAROČNIKOVO SPLETNO MESTO, SPLETNO APLIKACIJO, MOBILNO APLIKACIJO ALI TEHNIČNO OKOLJE.

Ponudba IBM SaaS je zasnovana tako, da identificira različne morebitne varnostne težave in težave s skladnostjo v mobilnih in spletnih aplikacij ter spletnih storitev. Ne preizkusi vseh ranljivosti ali tveganj zaradi skladnosti, niti ne deluje kot prepreka pred napadi na varnost. Varnostna tveganja, predpisi in standardi se nenehno spreminjajo, in storitev morda ne odraža vseh takšnih sprememb. Varnost in skladnost naročnikovih spletnih aplikacij, sistemov in zaposlenih in vseh popravnih dejanj so izključno naročnikova odgovornost. Izključno naročnik lahko presodi, ali bo ali ne bo uporabil informacij, ki jih zagotavlja storitev.

Določeni zakoni prepovedujejo kakršenkoli nepooblaščen poskus prodora ali dostopa do računalniških sistemov. NAROČNIK PREVZEMA ODGOVORNOST, DA ZAGOTOVI, DA NAROČNIK STORITVE NE UPORABLJA ZA OPTIČNO BRANJE KATERIHKOLI SPLETNIH MESTI IN/ALI APLIKACIJ, KI NISO SPLETNA MESTA IN/ALI APLIKACIJE, KI JIH IMA V LASTI NAROČNIK, ALI TISTIH, ZA KATERE IMA NAROČNIK PRAVICO IN POOBLASTILO ZA OPTIČNO BRANJE.

6.2 Piškotki

Naročnik se zaveda in soglaša, da lahko IBM kot del običajnega delovanja in podpore ponudbe IBM SaaS prek sledenja in drugih tehnologij zbira naročnikove osebne podatke (podatke njegovih zaposlenih in pogodbenikov) v zvezi z uporabo ponudbe IBM SaaS prek sledenja in drugih tehnologij. IBM s tem pridobiva statistiko o uporabi in podatke o učinkovitosti storitve IBM SaaS z namenom izboljšanja uporabniške izkušnje in/ali prilagajanja interakcije z naročnikom. Naročnik potrjuje, da je/bo pridobil soglasje, ki IBM-u v skladu z veljavno zakonodajo dovoljuje obdelavo zbranih osebnih podatkov za navedeni namen znotraj IBM-a, drugih IBM-ovih podjetij in njihovih podizvajalcev ne glede na to, kje IBM in njegovi podizvajalci poslujejo. IBM bo upošteval zahteve naročnikovih uslužbencev in pogodbenikov za dostop, posodobitev, spremembo ali izbris njihovih zbranih osebnih podatkov.

6.3 Izpeljane lokacije prejemanja storitev

Kadar je to ustrezno, davki temeljijo na eni ali več lokacijah, ki jih naročnik navede kot lokacije prejemanja storitev iz ponudbe IBM SaaS. IBM obračuna davke na podlagi poslovnega naslova, ki ga je naročnik navedel pri naročilu ponudbe IBM SaaS kot primarno lokacijo uporabe storitev, razen če naročnik IBM-u posreduje dodatne informacije o tem. Naročnik je odgovoren, da posodablja takšne informacije in IBM-u sporoči morebitne spremembe.

Dodatek A

1. Splošen opis izdelka IBM Application Security on Cloud

IBM Application Security on Cloud zagotavlja enotno mesto za pomoč naročniku pri ugotavljanju varnostnih ranljivosti (kot so vstavljanje sestavljenega jezika za poizvedbe, skriptno izvajanje na več spletnih mestih in uhajanje podatkov) za različne aplikacije. Storitev vključuje različne vrste tehnik pregleda zaščite aplikacije, od katerih vsaka identificira varnostne težave v tej aplikaciji.

Storitev IBM Application Security on Cloud omogoča naslednje zmožnosti:

- Pregledovanje mobilnih aplikacij za varnostne ranljivosti. To se naredi prek dinamičnih (črna skrinjica) in interaktivnih (steklena skrinjica) tehnologij analize varnosti.
- Pregledovanje produkcijskih ali predprodukcijskih, javno dostopnih ali v zasebnem omrežju, spletnih strani za varnostne ranljivosti. To se naredi prek dinamičnih (črna skrinjica) tehnik analize varnosti.
- Pregledovanje podatkovnih tokov znotraj spletnih in namiznih aplikacij za varnostne ranljivosti. To se naredi s statičnimi (bela skrinjica) tehnikami analize varnosti.
- Podrobna poročila o varnostni ranljivosti, ki vsebujejo povzetke visoke ravni o korakih z ugotovitvami ter popravki/posodobitvami, katere lahko spremljajo razvijalci.
- Integracija z različnimi platformami DevOps.