Opis IBM-ovih storitev v oblaku

IBM Security AppScan Mobile Analyzer

Opis storitev iz vašega naročila:

1. Storitve v oblaku

Ponudba storitev v oblaku je opisana v nadaljevanju in podana v dokumentu naročila za izbrane ponudbe s pooblastilom. Dokument naročila bo sestavljen iz zagotovljene ponudbe in prejetega dokazila o upravičenosti, ki potrjuje datum začetka ter obdobje zagotavljanja storitev v oblaku. Zaračunavanje se začne po tem, ko so storitve v oblaku zagotovljene.

1.1 IBM Security AppScan Mobile Analyzer

Ta storitev določa težave z zaščito na ravni kode mobilnih aplikacij Android. Razvijalcu omogoča pregled ranljivosti na področju zaščite, ne da bi potreboval izvorno kodo aplikacije. Ko se pregled zaključi, storitev generira poročilo o zaščiti, ki vključuje podrobnosti o zaznanih ranljivostih, možna varnostna tveganja za mobilno aplikacijo, ki jih lahko povzročijo takšne ranljivosti, ter priporočila o odpravljanju navedenih težav.

2. Opis zaščite

2.1 Varnostni pravilniki

IBM ima svojo ekipo za informacijsko varnost ter izvaja pravilnike o zasebnosti in varnosti, s katerimi so seznanjeni vsi IBM-ovi zaposleni. IBM zahteva usposabljanje o zasebnosti in varnosti za zaposlene, ki podpirajo IBM-ove podatkovne centre. IBM svoje pravilnike o varnosti in standarde vsako leto pregleda in na novo oceni. IBM obravnava varnostne dogodke v skladu s celovitim postopkom odziva na dogodke.

2.2 Nadzor dostopa

Dostop do podatkov naročnika, če je ta potreben, je dovoljen samo pooblaščenim predstavnikom IBM-ove podpore in servisnemu osebju, in sicer v skladu z načeli delitve nalog. IBM-ovo osebje uporablja dvostopenjsko preverjanje pristnosti v vmesnem gostitelju "prehoda" za upravljanje. Vse povezave za dostop do podatkov naročnika so šifrirani kanali.

2.3 Celovitost in razpoložljivost storitve

Spremembe operacijskih sistemov in programske opreme aplikacij ureja IBM-ov postopek upravljanja sprememb. Spremembe pravil požarnega zidu ureja tudi postopek upravljanja sprememb in jih pred uvedbo pregleda IBM-ovo varnostno osebje. IBM nadzoruje podatkovni center 24 ur na dan, 7 dni v tednu. Pooblaščeni skrbniki in drugi ponudniki redno izvajajo notranja in zunanja preverjanja ranljivosti, s čimer se odkriva in odpravlja potencialno izpostavljenost sistema nevarnostim. V vseh IBM-ovih podatkovnih centrih se uporabljajo sistemi za odkrivanje zlonamerne programske opreme (protivirusni programi, zaznavanje vdorov, preverjanje ranljivosti in preprečevanje vdorov). IBM-ove storitve podatkovnih centrov podpirajo različne protokole dostave podatkov za prenos podatkov prek javnih omrežij. Primeri:HTTPS/SFTP/FTPS/S/MIME in VPN med spletnimi mesti. Podatki varnostnih kopij, ki se shranjujejo zunaj lokacije, se pred transportom šifrirajo.

2.4 Beleženje aktivnosti

IBM hrani dnevnike svojih dejavnosti v zvezi s sistemi, aplikacijami, podatkovnimi viri, vmesno opremo in napravami omrežne infrastrukture, ki omogočajo aktivnosti beleženja in so konfigurirane za ta namen. Zaradi zmanjševanja možnosti posegov in da se omogoči centralna analiza, se opozarjanje in poročanje ter beleženje aktivnosti v centralne dnevniške vire izvajajo v realnem času. Zaradi preprečevanja posegov so podatki podpisani. Dnevniki se analizirajo v realnem času in prek periodičnih analitičnih poročil, ki zaznavajo odstopanja v delovanju. Operativno osebje je opozorjeno na odstopanja in se po potrebi obrne na strokovnjaka za varnost, ki je po telefonu dosegljiv 24 ur na dan, 7 dni v tednu.

2.5 Fizična varnost

IBM ima določene standarde fizične varnosti, ki so zasnovani tako, da omejujejo nepooblaščen fizični dostop do IBM-ovih podatkovnih centrov. Do podatkovnih centrov vodi le omejeno število dostopnih točk, ki se nadzorujejo z dvostopenjskim preverjanjem pristnosti in nadzornimi kamerami. Dostop je dovoljen samo pooblaščenemu osebju, ki ima dovoljenje za dostop. Operativno osebje preveri dovoljenje in izda dostopno identifikacijsko priponko, s čimer se odobri potrebni dostop. Zaposleni, ki se jim izdajo take

identifikacijske priponke, morajo predati vse druge dostopne identifikacijske priponke in lahko imajo v času trajanja aktivnosti pri sebi samo dostopno identifikacijsko priponko za podatkovni center. Uporaba identifikacijskih priponk se zapisuje v dnevnik. Obiskovalci, ki niso uslužbenci IBM-a, se morajo ob prihodu v IBM-ove prostore prijaviti in dobijo spremstvo za ves čas prisotnosti v teh prostorih. Dostavna območja, nakladalne rampe in druge točke, kjer lahko nepooblaščene osebe vstopajo v IBM-ove prostore, so nadzorovani in izolirani.

2.6 Skladnost

IBM letno preverja skladnost svojih praks zasebnosti z načeli varnega ravnanja z osebnimi podatki ameriškega ministrstva za trgovino: obvestilo, izbira, prenos naprej, dostop in natančnost, varnost in nadzor/uveljavljanje. IBM letno izvaja revizije v skladu s standardom panoge SSAE 16 (ali enakovredne) v svojih produkcijskih podatkovnih centrih. IBM preverja skladnost aktivnosti, povezanih z varnostjo in zasebnostjo, z IBM-ovimi poslovnimi zahtevami. IBM redno izvaja ocenjevanja in revizije, s katerimi preverja skladnost s pravilniki informacijske varnosti. IBM-ovi uslužbenci in uslužbenci dobaviteljev se vsako leto udeležujejo izobraževanj o varnosti in usposabljanj z namenom ozaveščanja. IBM vsako leto opomni osebje na cilje njihovega dela in njihovo odgovornost glede upoštevanja etičnega poslovnega vedenja, zaupnosti in IBM-ovih varnostnih obveznosti.

3. Pooblastila in informacije o zaračunavanju

3.1 Metrika zaračunavanja

Storitve v oblaku so na voljo v skladu z naslednjo metriko zaračunavanja, kot je določeno v transakcijskem dokumentu:

- Primerek aplikacije je merska enota, na podlagi katere je mogoče pridobiti 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 prodobiti zadostna pooblastila, da z njimi pokrije število primerkov aplikacije, ki so povezani s ponudbo SaaS v obdobju merjenja, navedenem v naročnikovem dokazilu o upravičenosti ali transakcijskem dokumentu.

3.2 Stroški in zaračunavanje

Znesek za plačilo storitev v oblaku je določen v dokumentu naročila.

3.3 Plačilo po porabi

Možnosti plačila po porabi bodo zaračunane v mesecu, ki sledi mesecu uporabe storitve, in sicer v znesku, podanem v transakcijskem dokumentu.

4. Tehnična podpora

Tehnična podpora za storitve v oblaku je na voljo ves čas naročniškega obdobja.

Delovni čas podpore je naslednji:

Informacije o časih razpoložljivosti, spletnih sistemih za poročanje o težavah ter drugih načinih komunikacije in postopkih, povezanih s tehnično podporo, so opisane v priročniku o podpori za IBM-ovo programsko opremo kot storitev.

Podpora zunaj delovnega časa:

Podpora zunaj delovnega časa je na voljo samo za težave z najvišjo ravnjo resnosti ob delovnih dneh, vikendih in praznikih. Pri težavah z najvišjo ravnjo resnosti mora biti naročnik IBM-u na voljo 24 ur na dan in 7 dni v tednu za pomoč pri diagnosticiranju težav, sicer se raven resnosti težave zniža na resnost 2.

4.1 Podpora na forumu

Vsem naročnikom na storitve v oblaku je zagotovljena podpora na forumu, ki jo redno nadzirajo IBM-ovi predstavniki podpore in razvijalci.

a. Posredovanje vprašanj:

   https://developer.ibm.com/answers/questions/ask/?topics=appscan-mobile-analyzer

b. Ogled trenutnih objav:

   https://developer.ibm.com/answers/topics/appscan-mobile-analyzer/

4.2 Standardna podpora

Standardna podpora je na voljo v času trajanja obdobja, v katerem se naročniku zaračunavajo sprotni stroški. Naročniki lahko v storitvah v oblaku predložijo prijavo za podporo ali odprejo sejo klepeta za namen pridobitve pomoči. Za več informacij o postopkih podpore glejte IBM-ov spletni portal za podporo na naslovu: https://support.ibmcloud.com ali priročnik za podporo za programsko opremo IBM SaaS na naslovu: http://www.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf.

Resnost	Definicija resnosti	Ciljni odzivni čas	Kritje odzivnega časa
1	**Kritični vpliv na poslovanje/izpad storitve:** Nedelovanje funkcije, ki je odločilnega pomena za poslovanje ali izpad odločilnega vmesnika. To običajno velja za produkcijsko okolje in označuje 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 M-F
3	**Manjši vpliv na poslovanje:** Označuje, da je storitev ali funkcijo mogoče uporabljati in težava nima odločilnega vpliva na operacije.	V roku 4 delovnih ur	Delovni čas M-F
4	**Minimalen vpliv na poslovanje:** Poizvedba ali netehnična zahteva	V roku 1 delovnega dne	Delovni čas M-F

5. Skladnost z dogovorom o varnem ravnanju z osebnimi podatki

IBM še ni določil skladnosti teh storitev v oblaku z določili varnega pristana, sklenjenega med ZDA in EU ter med ZDA in Švico.

6. Dodatne informacije

Storitev v oblaku je zasnovana tako, da lahko prepozna različne morebitne varnostne težave in težave v zvezi s skladnostjo v mobilnih aplikacijah in mobilnih spletnih storitvah. 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. Naročnik je izključno odgovoren za varnost in skladnost svoje mobilne aplikacije, sistemov in zaposlenih, ter tudi za morebitne sanacijske ukrepe. Naročnik se po lastni presoji odloči, ali bo uporabil informacije, ki jih zagotovi storitev.

6.1 Izpeljane lokacije prejemanja storitev

Morebitne dajatve se zaračunajo na podlagi lokacij, ki jih je naročnik opredelil kot lokacije prejemanja storitev v oblaku. IBM bo zaračunal dajatve na podlagi poslovnega naslova, navedenega ob naročilu storitev v oblaku, ki bo veljal za primarno lokacijo za dajatve, razen če naročnik IBM-u posreduje drugačne podatke. Naročnik je odgovoren za aktualnost teh podatkov in obveščanje IBM-a o morebitnih spremembah.

6.2 Piškotki

Naročnik se zaveda in soglaša, da lahko IBM v okviru običajnega delovanja in podpore za storitve v oblaku zbira osebne podatke naročnika (njegovih zaposlenih in podizvajalcev) v povezavi z uporabo storitev v oblaku s sledenjem in drugimi tehnologijami. IBM s tem pridobiva statistiko o uporabi in podatke o učinkovitosti storitev v oblaku za izboljšanje uporabniške izkušnje in/ali prilagoditev interakcije z naročnikom. Naročnik potrjuje, da bo pridobil ali je že pridobil soglasje, ki IBM-u dovoljuje zbiranje osebnih podatkov za zgornje namene znotraj IBM-a, drugih IBM-ovih podjetij in njihovih podizvajalcev, kjerkoli IBM ali podizvajalci poslujejo, v skladu z veljavno zakonodajo. IBM bo upošteval zahteve naročnikovih zaposlenih in podizvajalcev za dostop, posodobitev, spremembo ali izbris njihovih zajetih osebnih podatkov.