IBM Trusteer Fraud Protection

Ta opis storitve opisuje storitev v oblaku, ki jo IBM zagotavlja naročniku. Naročnik pomeni pogodbeno stranko ter njegove pooblaščene uporabnike in prejemnike storitev v oblaku. Veljavna ponudba in dokazilo o upravičenosti sta zagotovljena v obliki ločenih transakcijskih dokumentov.

1. Storitve v oblaku

Ta opis storitev velja za naslednje storitve v oblaku:

Storitve v oblaku Rapport:

- IBM Trusteer Rapport for Business
- IBM Trusteer Rapport for Business Premium Support
- IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport for Retail Premium Support
- IBM Trusteer Rapport II for Business
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Rapport Fraud Feeds for Business
- IBM Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Trusteer Rapport Fraud Feeds for Retail
- IBM Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Trusteer Rapport Phishing Protection for Business
- IBM Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Trusteer Rapport Phishing Protection for Retail
- IBM Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Trusteer Rapport Mandatory Service for Business
- IBM Trusteer Rapport Mandatory Service for Retail
- IBM Trusteer Rapport Additional Applications For Retail
- IBM Trusteer Rapport Additional Applications For Business
- IBM Trusteer Rapport Large Redeployment
- IBM Trusteer Rapport Small Redeployment

Storitve v oblaku Pinpoint:

- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Trusteer Pinpoint Carbon Copy for Business

- IBM Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Trusteer Pinpoint Carbon Copy for Retail
- IBM Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Advanced Edition
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Redeployment
- IBM Trusteer Pinpoint Criminal Detection Redeployment
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Rapport for Mitigation for Retail
- IBM Trusteer Rapport for Mitigation for Retail Premium Support
- IBM Trusteer Rapport for Mitigation for Business
- IBM Trusteer Rapport for Mitigation for Business Premium Support
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business
- IBM Trusteer Pinpoint Detect Standard Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard For Retail Premium Support
- IBM Trusteer Pinpoint Detect Standard For Business Premium Support

Storitve v oblaku Mobile:

- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser for Business
- IBM Trusteer Mobile Browser for Business Premium Support

- IBM Trusteer Mobile Browser for Retail
- IBM Trusteer Mobile Browser for Retail Premium Support

1.1 Poslovne in prodajne storitve v oblaku

Storitve v oblaku IBM Trusteer so odobrene za uporabo z določenimi vrstami aplikacij. Aplikacija je opredeljena kot ena od naslednjih vrst: prodajna ali poslovna. Za prodajne in poslovne aplikacije so na voljo ločene ponudbe.

a. Prodajna aplikacija je opredeljena kot aplikacija za spletno bančništvo, mobilna aplikacija ali aplikacija za e-trgovino, ki je zasnovana za uporabo s strani potrošnikov. Naročnikov pravilnik lahko klasificira določena mala podjetja kot primerna za prodajni dostop.

b. Poslovna aplikacija je opredeljena kot aplikacija za spletno bančništvo, mobilna aplikacija ali aplikacija za e-trgovino, ki je zasnovana za uporabo s strani podjetij, ustanov ali enakovrednih entitet, oz. katerakoli aplikacija, ki ni opredeljena kot prodajna.

1.1.1 Poslovne storitve v oblaku

- IBM Trusteer Rapport for Business
- IBM Trusteer Rapport II for Business
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile Browser for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business

1.1.2 Prodajne storitve v oblaku

- IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Standard Edition
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser for Retail

Za vsako poslovno (Business) in prodajno (Retail) storitev v oblaku je za dodatno plačilo na voljo povezani izdelek Premium Support, razen za storitve v oblaku IBM Trusteer Mobile SDK.

1.1.3 Dodatne storitve v oblaku za IBM Trusteer Rapport

a. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Rapport for Business:
   - IBM Trusteer Rapport Fraud Feeds for Business
   - IBM Trusteer Rapport Phishing Protection for Business
   - IBM Trusteer Rapport Mandatory Service for Business
   - IBM Trusteer Rapport Additional Applications For Business

b. b. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Rapport for Retail:
   - IBM Trusteer Rapport Fraud Feeds for Retail
   - IBM Trusteer Rapport Phishing Protection for Retail
   - IBM Trusteer Rapport Mandatory Service for Retail
   - IBM Trusteer Rapport Additional Applications For Retail

Za vse dodatke k storitvam v oblaku IBM Trusteer Rapport, tako za poslovanje (Business) kot za prodajo (Retail), razen za dodatke IBM Trusteer Rapport Mandatory Service, je za dodatno plačilo na voljo povezani izdelek Premium Support.

Naročnina na IBM Trusteer Rapport for Business ali IBM Trusteer Rapport for Retail je predpogoj za povezane dodatne storitve v oblaku, navedene v tem razdelku.

1.1.4 Dodatne storitve v oblaku za IBM Trusteer Pinpoint Malware Detection in/ali IBM Trusteer Pinpoint Malware Detection II

a. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition ali IBM Trusteer Pinpoint Malware Detection for Business Standard Edition ali za IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business ali IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business:
   - IBM Trusteer Pinpoint Carbon Copy for Business
   - IBM Trusteer Rapport Remediation for Business
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

b. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition ali IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition ali za IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition ali IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition:
   - IBM Trusteer Pinpoint Carbon Copy for Retail
   - IBM Trusteer Rapport Remediation for Retail
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail

Podpora Premium je na voljo za posebne ponudbe, kot je navedeno v tem dokumentu. Naročnina na IBM Trusteer Pinpoint Malware Detection for Business ali IBM Trusteer Pinpoint Malware Detection for Retail ali IBM Trusteer Pinpoint Malware Detection II for Business ali IBM Trusteer Pinpoint Malware Detection II for Retail je predpogoj za povezane dodatne storitve v oblaku, navedene v tem razdelku.

1.1.5 Dodatne storitve v oblaku za IBM Trusteer Pinpoint Criminal Detection in/ali IBM Trusteer Pinpoint Criminal Detection II

a. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Pinpoint Criminal Detection for Business ali IBM Trusteer Pinpoint Criminal Detection II:
   - IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business

b. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Pinpoint Criminal Detection for Retail in/ali IBM Trusteer Pinpoint Criminal Detection II for Retail:
   - IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Podpora Premium je na voljo za posebne ponudbe, kot je navedeno v tem dokumentu.

Naročnina na IBM Trusteer Pinpoint Criminal Detection for Business ali IBM Trusteer Pinpoint Criminal Detection for Retail ali IBM Trusteer Pinpoint Criminal Detection II for Business ali IBM Trusteer Pinpoint Criminal Detection II for Retail je predpogoj za povezane dodatne storitve v oblaku, navedene v tem razdelku.

1.1.6 Dodatne storitve v oblaku za IBM Trusteer Pinpoint Detect Standard in/ali IBM Trusteer Pinpoint Detect Premium in/ali IBM Security Pinpoint Detect Standard with access management integration in/ali IBM Security Detect Premium with access management integration

a. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Detect Standard for Business in/ali IBM Trusteer Pinpoint Detect Premium for Business in/ali IBM Security Pinpoint Detect Standard with access management integration for Business in/ali IBM Security Detect Premium with access management integration for Business:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

b. Dodatne storitve v oblaku, ki so na voljo za IBM Trusteer Detect Standard for Retail in/ali IBM Trusteer Pinpoint Detect Premium for Retail in/ali IBM Security Pinpoint Detect Standard with access management integration for Retail in/ali IBM Security Detect Premium with access management integration for Retail:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

Naročnina na IBM Trusteer Detect Standard ali IBM Trusteer Pinpoint Detect Premium ali IBM Security Pinpoint Detect Standard with access management integration ali IBM Security Detect Premium with access management integration je predpogoj za povezane dodatne storitve v oblaku, navedene v tem razdelku.

1.1.7 Druge dodatne storitve v oblaku

Morebitne dodatne naročnine za storitve v oblaku za zgornje osnovne naročnine, ki niso navedene v tem dokumentu, in so bodisi trenutno na voljo ali še v razvoju, se ne štejejo kot posodobitev in jih je treba odobriti ločeno.

1.2 Opredelitev pojmov

Imetnik računa – je naročnikov končni uporabnik, ki je namestil programsko opremo za aktiviranje odjemalca, sprejel licenčno pogodbo za končne uporabnike ("EULA") in se je vsaj enkrat overil v naročnikovi prodajni ali poslovni aplikaciji, za katero ima naročnik naročnino za storitve v oblaku.

Odjemalska programska oprema imetnika računa je programska oprema za aktiviranje odjemalca IBM Trusteer Rapport ali programska oprema za aktiviranje odjemalca IBM Trusteer Mobile Browser, ki je na voljo z nekaterimi storitvami v oblaku za namestitev v napravo končnega uporabnika.

Trusteer Splash se nanaša na pozdravno okno, ki se naročniku zagotovi na podlagi razpoložljivih pozdravnih predlog.

Pristajalna stran se nanaša na stran, ki jo gosti IBM ter se naročniku zagotovi skupaj s pozdravnim oknom za naročnike in odjemalsko programsko opremo imetnika računa, ki jo je mogoče prenesti.

2. IBM Trusteer Rapport Cloud Services

2.1 IBM Trusteer Rapport for Retail and/or IBM Trusteer Rapport for Business ("Trusteer Rapport")

Trusteer Rapport zagotavlja plast zaščite proti lažnemu predstavljanju in napadom zlonamerne programske opreme Man-in-the-Browser (MitB). Z omrežjem, ki vključuje na desetine milijonov končnih točk po svetu, IBM Trusteer Rapport zbira podatke o dejavnem lažnem predstavljanju in zlonamernih napadih na organizacije po vsem svetu. IBM Trusteer Rapport uporablja vedenjske algoritme, ki blokirajo napade lažnega predstavljanja ter preprečijo namestitev in delovanje zlonamerne programske opreme MitB.

Za to storitev v oblaku velja metrika zaračunavanja z upravičenimi udeleženci. Poslovna ponudba je naprodaj v paketih po 10 upravičenih udeležencev. Prodajna ponudba je naprodaj v paketih po 100 upravičenih udeležencev.

Ta ponudba storitev v oblaku vključuje:

a. Trusteer Management Application ("TMA"):

Aplikacija TMA je na voljo v okolju IBM Trusteer, ki gostuje v oblaku, prek katerega lahko naročnik (in neomejeno število njegovih pooblaščencev): (i) pregleduje in prenaša poročila o nekaterih podatkih o dogodkih in ocene tveganja ter (ii) pregleduje konfiguracijo programske opreme za

aktiviranje odjemalca, ki je brezplačno licencirana za naročnikove upravičene udeležence na podlagi licenčne pogodbe za končne uporabnike ("EULA"), pri čemer je na voljo za prenos na namizja ali v naprave (PC/Mac) upravičenega udeleženca - z drugim imenom zbirka programske opreme Trusteer Rapport ("odjemalska programska oprema imetnika računa"). Naročnik lahko odjemalsko programsko opremo imetnika računa trži samo prek platforme Trusteer Splash ali Rapport API in je ne sme uporabljati za notranje poslovanje ali uporabo s strani zaposlenih (razen za njihovo osebno uporabo).

b. Spletni skript:

   Za dostop na spletnem mestu za namene dostopa ali uporabe storitve v oblaku.

c. Podatki o dogodkih:

   Naročnik (in neomejeno število njegovih pooblaščencev) lahko uporablja aplikacijo TMA za prejemanje podatkov o dogodkih, ustvarjenih z odjemalsko programsko opremo imetnika računa na podlagi spletnih interakcij imetnikov računov z naročnikovimi poslovnimi in/ali prodajnimi aplikacijami, za katere ima naročnik naročnino za storitve v oblaku. Podatki o dogodkih bodo prejeti iz odjemalske programske opreme imetnika računa, ki se izvaja v napravah upravičenih udeležencev, ki so sprejeli pogodbo EULA in se vsaj enkrat overili v naročnikovi poslovni ali prodajni aplikaciji, pri čemer mora naročnikova konfiguracija vključevati zbirko ID-jev uporabnikov.

d. Trusteer Splash:

   Platforma za trženje Trusteer Splash predstavi in trži odjemalsko programsko opremo imetnika računa upravičenim udeležencem, ki dostopajo do naročnikovih poslovnih in/ali prodajnih aplikacij, za katere ima naročnik naročnino za storitve v oblaku. Naročnik lahko izbira med razpoložljivimi pozdravnimi predlogami. Pozdravno okno po meri se lahko pogodbeno določi na podlagi ločene pogodbe ali dogovora o obsegu del.

Naročnik lahko soglaša, da svoje blagovne znamke, logotipe ali ikone ponudi v uporabo v povezavi z aplikacijo TMA in samo za uporabo s platformo Trusteer Splash ter za prikaz v odjemalski programski opremi imetnika računa ali na pristajalnih straneh, ki jih gostita IBM in spletna stran IBM Trusteer. Vsaka uporaba naročnikovih blagovnih znamk, logotipov ali ikon bo v skladu z IBM-ovimi razumnimi načeli glede oglaševanja in uporabe blagovnih znamk.

Naročnik mora skleniti naročnino za IBM Trusteer Rapport Mandatory Service, če želi izvesti katerokoli vrsto obvezne razmestitve odjemalske programske opreme imetnika računa.

Obvezna razmestitev odjemalske programske opreme imetnika računa med drugim vključuje katerokoli vrsto obvezne razmestitve na podlagi kateregakoli mehanizma ali sredstva, ki od upravičenega udeleženca neposredno ali posredno zahteva prenos odjemalske programske opreme imetnika računa, ali katerokoli metodo, orodje, postopek, pogodbo ali mehanizem, ki ga IBM ni ustvaril ali odobril in je ustvarjen za to, da obide zahteve za licenciranje v okviru te obvezne razmestitve odjemalske programske opreme imetnika računa.

2.2 IBM Trusteer Rapport II for Retail and/or IBM Trusteer Rapport II for Business ("Trusteer Rapport II")

Trusteer Rapport II Cloud Service je nova izgradnja storitve IBM Trusteer Rapport za lažjo standardizacijo stroškov, povezanih z zaščito več aplikacij, in se uporablja namesto enkratnih stroškov pri dodajanju aplikacij.

Trusteer Rapport II zagotavlja plast zaščite proti lažnemu predstavljanju in napadom zlonamerne programske opreme Man-in-the-Browser (MitB). Z omrežjem, ki vključuje na desetine milijonov končnih točk po svetu, IBM Trusteer Rapport zbira podatke o dejavnem lažnem predstavljanju in zlonamernih napadih na organizacije po vsem svetu. IBM Trusteer Rapport uporablja vedenjske algoritme, ki blokirajo napade lažnega predstavljanja ter preprečijo namestitev in delovanje zlonamerne programske opreme MitB.

Upravičenost do te storitve v oblaku temelji na metriki zaračunavanja z upravičenimi udeleženci. Poslovna ponudba je naprodaj v paketih po 10 upravičenih udeležencev. Prodajna ponudba je naprodaj v paketih po 100 upravičenih udeležencev.

Ta ponudba storitev v oblaku vključuje:

a. Trusteer Management Application ("TMA"):

   Aplikacija TMA je na voljo v okolju IBM Trusteer, ki gostuje v oblaku, prek katerega lahko naročnik (in neomejeno število njegovih pooblaščencev): (i) pregleduje in prenaša poročila o nekaterih podatkih o dogodkih in ocene tveganja ter (ii) pregleduje konfiguracijo programske opreme za aktiviranje odjemalca, ki je brezplačno licencirana za naročnikove upravičene udeležence na podlagi licenčne pogodbe za končne uporabnike ("EULA"), pri čemer je na voljo za prenos na namizja ali v naprave (PC/Mac) upravičenega udeleženca - z drugim imenom zbirka programske opreme Trusteer Rapport ("odjemalska programska oprema imetnika računa"). Naročnik lahko odjemalsko programsko opremo imetnika računa trži samo prek platforme Trusteer Splash ali Rapport API in je ne sme uporabljati za notranje poslovanje ali uporabo s strani zaposlenih (razen za njihovo osebno uporabo).

b. Spletni skript:

   Za dostop na spletnem mestu za namene dostopa ali uporabe storitve v oblaku.

c. Podatki o dogodkih:

   Naročnik (in neomejeno število njegovih pooblaščencev) lahko uporablja aplikacijo TMA za prejemanje podatkov o dogodkih, ustvarjenih z odjemalsko programsko opremo imetnika računa na podlagi spletnih interakcij imetnikov računov z naročnikovimi poslovnimi in/ali prodajnimi aplikacijami, za katere ima naročnik naročnino za storitve v oblaku. Podatki o dogodkih bodo prejeti iz odjemalske programske opreme imetnika računa, ki se izvaja v napravah upravičenih udeležencev, ki so sprejeli pogodbo EULA in se vsaj enkrat overili v naročnikovi poslovni ali prodajni aplikaciji, pri čemer mora naročnikova konfiguracija vključevati zbirko ID-jev uporabnikov.

d. Trusteer Splash:

   Platforma za trženje Trusteer Splash predstavi in trži odjemalsko programsko opremo imetnika računa upravičenim udeležencem, ki dostopajo do naročnikovih poslovnih in/ali prodajnih aplikacij, za katere ima naročnik naročnino za storitve v oblaku. Naročnik lahko izbira med razpoložljivimi pozdravnimi predlogami. Pozdravno okno po meri se lahko pogodbeno določi na podlagi ločene pogodbe ali dogovora o obsegu del.

Naročnik lahko soglaša, da svoje blagovne znamke, logotipe ali ikone ponudi v uporabo v povezavi z aplikacijo TMA in samo za uporabo s platformo Trusteer Splash ter za prikaz v odjemalski programski opremi imetnika računa ali na pristajalnih straneh, ki jih gostita IBM in spletna stran IBM Trusteer. Vsaka uporaba naročnikovih blagovnih znamk, logotipov ali ikon bo v skladu z IBM-ovimi razumnimi načeli glede oglaševanja in uporabe blagovnih znamk.

Naročnik mora skleniti naročnino za IBM Trusteer Rapport Mandatory Service, če želi izvesti katerokoli vrsto obvezne razmestitve odjemalske programske opreme imetnika računa.

Obvezna razmestitev odjemalske programske opreme imetnika računa med drugim vključuje katerokoli vrsto obvezne razmestitve na podlagi kateregakoli mehanizma ali sredstva, ki od upravičenega udeleženca neposredno ali posredno zahteva prenos odjemalske programske opreme imetnika računa, ali katerokoli metodo, orodje, postopek, pogodbo ali mehanizem, ki ga IBM ni ustvaril ali odobril in je ustvarjen za to, da obide zahteve za licenciranje v okviru te obvezne razmestitve odjemalske programske opreme imetnika računa.

Posamezna ponudba Trusteer Rapport II for Business in/ali Trusteer Rapport II for Retail vključuje zaščito za eno aplikacijo. Za vsako dodatno aplikacijo mora naročnik pridobiti pooblastilo za IBM Trusteer Rapport Additional Applications.

2.3 Izbirne dodatne storitve v oblaku za IBM Trusteer Rapport for Business in/ali IBM Trusteer Rapport for Retail in/ali IBM Trusteer Rapport II for Business in/ali IBM Trusteer Rapport II for Retail

Naročnina na storitve v oblaku IBM Trusteer Rapport ali IBM Trusteer Rapport II je predpogoj za naročnino na katerokoli od naslednjih dodatnih storitev v oblaku. Če je storitev v oblaku označena za poslovanje ("for Business"), mora biti tudi dodatna pridobljena storitev v oblaku označena za poslovanje ("for Business"). Če je storitev v oblaku označena za prodajo ("for Retail"), mora biti tudi dodatna pridobljena storitev v oblaku označena za prodajo ("for Retail"). Naročnik bo prejel podatke o dogodkih od upravičenih udeležencev, ki izvajajo odjemalsko programsko opremo imetnika računa ter so sprejeli

pogodbo EULA in se vsaj enkrat overili v naročnikovi poslovni in/ali prodajni aplikaciji, pri čemer mora naročnikova konfiguracija vključevati zbirko ID-jev uporabnikov.

2.3.1 IBM Trusteer Rapport Fraud Feeds for Business and/or IBM Trusteer Rapport Fraud Feeds for Retail

Ko naročnik (in neomejeno število njegovih pooblaščencev) sklene naročnino za ta dodatek storitve v oblaku, lahko uporablja aplikacijo TMA za ogledovanje, konfiguriranje in naročanje na dostavo virov groženj, ki jih ustvari storitev v oblaku Trusteer Rapport. Viri so lahko poslani prek e-pošte na podan e-poštni naslov ali prek protokola SFTP v obliki besedilnih datotek.

2.3.2 IBM Trusteer Rapport Phishing Protection for Business and/or IBM Trusteer Rapport Phishing Protection for Retail

Naročnik (in neomejeno število njegovih pooblaščencev) lahko z aplikacijo TMA prejema obvestila s podatki o dogodkih, povezanih s predložitvijo prijavnih poverilnic imetnika računa na domnevnem spletnem mestu za lažno predstavljanje ali goljufivem spletnem mestu. Zakonite spletne aplikacije (URL-ji) so lahko zmotno označene kot spletna mesta za lažno predstavljanje in storitev v oblaku lahko opozori imetnike računov, da je zakonito spletno mesto spletno mesto za lažno predstavljanje. V tem primeru mora naročnik o taki napaki obvestiti IBM, ki bo napako odpravil. To je naročnikovo edino pravno sredstvo v zvezi s tako napako.

2.3.3 IBM Trusteer Rapport Mandatory Service for Business and/or IBM Trusteer Rapport Mandatory Service for Retail

Naročnik lahko uporabi primerek platforme za trženje Trusteer Splash za pooblastitev prenosa odjemalske programske opreme imetnika računa za upravičene udeležence, ki dostopajo do naročnikovih poslovnih in/ali prodajnih aplikacij, za katere ima naročnik naročnino za storitve v oblaku.

IBM Trusteer Rapport Premium Support for Business je predpogoj za IBM Security Rapport Mandatory Service for Business.

IBM Trusteer Rapport Premium Support for Retail je predpogoj za IBM Security Rapport Mandatory Service for Retail.

Naročnik lahko uvede dodatno funkcionalnost storitve IBM Trusteer Rapport Mandatory Service, samo če je bila ta storitev naročena in konfigurirana za uporabo z naročnikovo prodajno ali poslovno aplikacijo, za katero ima naročnik naročnino za storitve v oblaku.

2.3.4 IBM Trusteer Rapport Large Redeployment and/or IBM Trusteer Rapport Small Redeployment

Naročniki, ki želijo ponovno razmestiti aplikacije za spletno bančništvo med obdobjem storitve, kar posledično zahteva spremembe pri razmestitvi storitve IBM Trusteer Rapport in/ali IBM Trusteer Rapport II, naj kupijo IBM Trusteer Rapport Redeployment Cloud Service.

Razmestitev je lahko potrebna, ker je naročnik spremenil domeno ali URL gostitelja aplikacije, spremenil konfiguracijo pozdravnega okna ali se preselil na novo platformo spletnega bančništva.

V šestmesečnem obdobju prehoda na razmestitev je naročnik upravičen do dodatnih aplikacij, ki se izvajajo nad obstoječimi naročenimi aplikacijami na podlagi "ena proti ena".

IBM Trusteer Rapport Large Redeployment velja za okolja z več kot 20.000 uporabniki, IBM Trusteer Rapport Small Redeployment pa velja za okolja z manj ali enako kot 20.000 uporabniki.

2.3.5 IBM Trusteer Rapport Additional Applications for Business in/ali IBM Trusteer Rapport Additional Applications for Retail

Za IBM Trusteer Rapport II for Business se za razmestitev v vse dodatne poslovne aplikacije, ki niso prva aplikacija, zahteva pooblastilo za storitev v oblaku IBM Trusteer Rapport Additional Applications for Business. Za IBM Trusteer Rapport II for Retail se za razmestitev v vse dodatne poslovne aplikacije, ki niso prva aplikacija, zahteva pooblastilo za storitev v oblaku IBM Trusteer Rapport Additional Applications for Retail.

3. Storitve v oblaku IBM Trusteer Pinpoint

IBM Trusteer Pinpoint je storitev v oblaku, ki je zasnovana tako, da zagotavlja dodatno plast zaščite ter zaznava in blaži napade zlonamerne programske opreme, lažno predstavljanje in zlorabe računov. Trusteer Pinpoint lahko naročnik integrira v svoje poslovne in/ali prodajne aplikacije, za katere ima naročnik naročnino za storitve v oblaku, in so vključene v postopke za preprečevanje prevar.

Te storitve v oblaku vključujejo:

a. TMA:

   Aplikacija TMA je na voljo v okolju IBM Trusteer, ki ga gosti oblak in prek katerega lahko naročnik (in neomejeno število njegovih pooblaščencev): (i) pregleduje poročila o podatkih dogodkov in ocene tveganja ter (ii) ogleduje, se naroča na in konfigurira dostavo virov groženj, ki se ustvarijo s ponudbami Pinpoint.

b. Spletni skript in/ali API-ji:

   Za razmestitev na spletnem mestu za namene dostopa do storitve v oblaku ali njene uporabe.

3.1 IBM Trusteer Pinpoint Malware Detection and IBM Trusteer Pinpoint Criminal Detection Best Practices

V primeru zaznavanja zlonamerne programske opreme pri storitvah v oblaku IBM Trusteer Pinpoint Malware Detection ali IBM Trusteer Pinpoint Malware Detection II ali v primeru zaznavanja zlorabe računa pri storitvah v oblaku IBM Trusteer Pinpoint Criminal Detection ali IBM Trusteer Pinpoint Criminal Detection II mora naročnik upoštevati navodila v Vodiču s primeri dobrih praks Pinpoint. Storitev v oblaku IBM Trusteer Pinpoint Malware Detection ali IBM Trusteer Pinpoint Malware Detection II ali IBM Trusteer Pinpoint Criminal Detection ali IBM Trusteer Pinpoint Criminal Detection II ni dovoljeno uporabljati na način, ki bi vplival na izkušnjo upravičenega udeleženca neposredno po primeru zaznavanja zlonamerne programske opreme in bi drugim osebam omogočal povezavo naročnikovih dejanj z uporabo storitev v oblaku IBM Trusteer Pinpoint (npr. obvestila, sporočila, blokiranje naprav ali dostop do poslovne in/ali prodajne aplikacije neposredno po primeru zaznavanja zlonamerne programske opreme).

3.2 IBM Trusteer Pinpoint Criminal Detection for Business in/ali IBM Trusteer Pinpoint Criminal Detection for Retail

Brez-odjemalsko zaznavanje sumljive dejavnosti zlorabe računa v brskalniku pri povezovanju s poslovno ali prodajno aplikacijo na podlagi ID-ja naprave, zaznavanja lažnega predstavljanja in zaznavanja kraje poverilnic, ki jo omogoča zlonamerna programska oprema. Storitve v oblaku IBM Trusteer Pinpoint Criminal Detection zagotavljajo dodatno plast zaščite, zaznavajo poskuse zlorabe računov in naročniku posredujejo ocene tveganja brskalnikov ali mobilnih naprav (prek izvirnega brskalnika ali naročnikove mobilne aplikacije), ki dostopajo do poslovne ali prodajne aplikacije.

a. Podatki o dogodkih:

   Naročnik (in neomejeno število njegovih pooblaščencev) lahko uporablja aplikacijo TMA za prejemanje podatkov o dogodkih, ustvarjenih na podlagi spletnih interakcij upravičenih udeležencev z naročnikovimi poslovnimi in/ali prodajnimi aplikacijami, za katere ima naročnik naročnino za storitve v oblaku, ali prejema podatke o dogodkih v načinu dostave prek zalednega API-ja.

3.3 IBM Trusteer Pinpoint Criminal Detection II for Business in/ali IBM Trusteer Pinpoint Criminal Detection II for Retail

IBM Security Pinpoint Criminal Detection II je nova izgradnja storitve IBM Trusteer Pinpoint Criminal Detection za lažjo standardizacijo stroškov, povezanih z zaščito več aplikacij, in se uporablja namesto enkratnih stroškov pri dodajanju aplikacij.

Brez-odjemalsko zaznavanje sumljive dejavnosti zlorabe računa v brskalniku pri povezovanju s poslovno ali prodajno aplikacijo na podlagi ID-ja naprave, zaznavanja lažnega predstavljanja in zaznavanja kraje poverilnic, ki jo omogoča zlonamerna programska oprema. Storitve v oblaku IBM Trusteer Pinpoint Criminal Detection II zagotavljajo dodatno plast zaščite, zaznavajo poskuse zlorabe računov in naročniku posredujejo ocene tveganja brskalnikov ali mobilnih naprav (prek izvirnega brskalnika ali naročnikove mobilne aplikacije), ki dostopajo do poslovne ali prodajne aplikacije.

a. Podatki o dogodkih:

   Naročnik (in neomejeno število njegovih pooblaščencev) lahko uporablja aplikacijo TMA za prejemanje podatkov o dogodkih, ustvarjenih na podlagi spletnih interakcij upravičenih udeležencev z naročnikovimi poslovnimi in/ali prodajnimi aplikacijami, za katere ima naročnik naročnino za storitve v oblaku, ali prejema podatke o dogodkih v načinu dostave prek zalednega API-ja.

   Ta storitev v oblaku vključuje zaščito za eno aplikacijo. Za vsako dodatno aplikacijo mora naročnik pridobiti pooblastilo za IBM Trusteer Pinpoint Criminal Detection Additional Applications.

3.4 IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition in/ali IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition in/ali IBM Trusteer Pinpoint Malware Detection for Business Standard Edition in/ali IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition

Brez-odjemalsko zaznavanje finančnih brskalnikov, okuženih z zlonamerno programsko opremo (Man-in-the-Browser – MitB) pri povezovanju s poslovno ali prodajno aplikacijo. Storitve v oblaku IBM Trusteer Pinpoint Malware Detection zagotavljajo dodatno plast zaščite ter organizacijam omogočajo, da se osredotočijo na postopke preprečevanja prevar na podlagi tveganja okužbe z zlonamerno programsko opremo, ki temelji na ocenah in opozorilih o prisotnosti zlonamerne programske opreme MitB, usmerjene proti finančnim aplikacijam.

a. Podatki o dogodkih:

   Naročnik (in neomejeno število njegovih pooblaščencev) lahko uporablja aplikacijo TMA za prejemanje podatkov o dogodkih, ustvarjenih na podlagi spletnih interakcij upravičenih udeležencev z naročnikovimi poslovnimi in/ali prodajnimi aplikacijami.

b. Advanced Edition:

   Izdaje Advanced Edition za poslovanje in/ali prodajo ponujajo dodatno plast zaznavanja in zaščite, ki je prilagojena strukturi ter pretoku poslovnih in/ali prodajnih aplikacij podjetja in se lahko prilagodi glede na specifično okolje grožnje, ki cilja naročnika. To plast je mogoče umestiti na različne lokacije v naročnikovih poslovnih in/ali prodajnih aplikacijah.

   Izdaja Advanced Edition je naročniku na voljo v najmanjši količini 100.000 prodajnih upravičenih udeležencev ali 10.000 poslovnih upravičenih udeležencev, kar predstavlja 1.000 paketov po 100 upravičenih udeležencev za prodajo ali 1.000 paketov po 10 upravičenih udeležencev za poslovanje.

c. Standard Edition:

   Izdaja Standard Edition for Business ali Standard Edition for Retail je rešitev, hitra za razmeščanje, ki ponuja osnovno funkcionalnost teh storitev v oblaku, kot je opisano v tem dokumentu.

3.5 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business in/ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail in/ali IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business in/ali IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Security Pinpoint Malware Detection II je nova izgradnja storitve IBM Trusteer Pinpoint Malware Detection za lažjo standardizacijo stroškov, povezanih z zaščito več aplikacij, in se uporablja namesto enkratnih stroškov pri dodajanju aplikacij.

Brez-odjemalsko zaznavanje finančnih brskalnikov, okuženih z zlonamerno programsko opremo (Man-in-the-Browser – MitB) pri povezovanju s poslovno ali prodajno aplikacijo. Storitve v oblaku IBM Trusteer Pinpoint Malware Detection zagotavljajo dodatno plast zaščite ter organizacijam omogočajo, da se osredotočijo na postopke preprečevanja prevar na podlagi tveganja okužbe z zlonamerno programsko opremo, ki temelji na ocenah in opozorilih o prisotnosti zlonamerne programske opreme MitB, usmerjene proti finančnim aplikacijam.

a. Podatki o dogodkih:

   Naročnik (in neomejeno število njegovih pooblaščencev) lahko uporablja aplikacijo TMA za prejemanje podatkov o dogodkih, ustvarjenih na podlagi spletnih interakcij upravičenih udeležencev z naročnikovimi poslovnimi in/ali prodajnimi aplikacijami.

b. Advanced Edition:

   Izdaje Advanced Edition za poslovanje in/ali prodajo ponujajo dodatno plast zaznavanja in zaščite, ki je prilagojena strukturi ter pretoku poslovnih in/ali prodajnih aplikacij podjetja in se lahko prilagodi glede na specifično okolje grožnje, ki cilja naročnika. To plast je mogoče umestiti na različne lokacije v naročnikovih poslovnih in/ali prodajnih aplikacijah.

   Izdaja Advanced Edition je naročniku na voljo v najmanjši količini 100.000 prodajnih upravičenih udeležencev ali 10.000 poslovnih upravičenih udeležencev, kar predstavlja 1.000 paketov po 100 upravičenih udeležencev za prodajo ali 1.000 paketov po 10 upravičenih udeležencev za poslovanje.

c. Standard Edition:

Izdaja Standard Edition for Business ali Standard Edition for Retail je rešitev, hitra za razmeščanje, ki ponuja osnovno funkcionalnost teh storitev v oblaku, kot je opisano v tem dokumentu.

Ta storitev v oblaku vključuje zaščito za eno aplikacijo. Za vsako dodatno aplikacijo mora naročnik pridobiti pooblastilo za IBM Trusteer Pinpoint Malware Detection Additional Applications.

3.6 Izbirne dodatne storitve v oblaku za IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition in/ali IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition in/ali IBM Trusteer Pinpoint Malware Detection for Business Standard Edition in/ali IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition in/ali IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail in/ali IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business in/ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail in/ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business

- Za IBM Trusteer Rapport Remediation for Retail Cloud Service je predpogoj IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail ali IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail ali IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Za IBM Trusteer Rapport Remediation for Business Cloud Service je predpogoj IBM Trusteer Pinpoint Malware Detection Standard Edition for Business ali IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business ali IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.
- Za IBM Trusteer Pinpoint Carbon Copy for Retail je predpogoj IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail ali IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail ali IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Za IBM Trusteer Pinpoint Carbon Copy for Business je predpogoj IBM Trusteer Pinpoint Malware Detection Standard Edition for Business ali IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business ali IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.

3.6.1 IBM Trusteer Pinpoint Carbon Copy for Business in/ali IBM Trusteer Pinpoint Carbon Copy for Retail

Ponudbe IBM Trusteer Pinpoint Carbon Copy so zasnovane tako, da zagotavljajo dodatno plast zaščite in ponujajo storitev nadzora, ki omogoča zaznavanje napadov lažnega predstavljanja na poverilnice upravičenih udeležencev v povezavi z naročnikovimi prodajnimi ali poslovnimi aplikacijami, za katere ima naročnik naročnino za pokritje ponudb storitev v oblaku.

3.6.2 IBM Trusteer Rapport Remediation for Retail in/ali IBM Trusteer Rapport Remediation for Business

IBM Trusteer Rapport Remediation for Retail in IBM Trusteer Rapport Remediation for Business sta rešitvi, ki sproti preiskujeta, popravljata, blokirata in odstranjujeta okužbe z zlonamerno programsko opremo MitB iz okuženih naprav (PC/Mac), ki jih uporabljajo naročnikovi upravičeni udeleženci za ad-hoc dostop do njegove aplikacije, v kateri so bile okužbe z zlonamerno programsko opremo MitB zaznane na podlagi podatkov o dogodkih storitve IBM Trusteer Pinpoint Malware Detection. Naročnik mora imeti veljavno naročnino na IBM Trusteer Pinpoint Malware Detection ali IBM Trusteer Pinpoint Malware Detection II, ki se dejansko izvajata v naročnikovi aplikaciji. Naročnik lahko uporablja to ponudbo storitve v oblaku izključno v povezavi z upravičenimi udeleženci, ki dostopajo do naročnikove aplikacije, in izključno kot orodje, ki omogoča preiskovanje in popravilo določene okužene naprave (PC/Mac) na ad-hoc osnovi. Storitev IBM Security Trusteer Rapport Remediation se mora dejansko izvajati v taki okuženi napravi (PC/Mac) upravičenega udeleženca, ki mora soglašati s pogoji pogodbe za končnega uporabnika (EULA) in vsaj enkrat izvesti overjanje v povezavi z naročnikovimi aplikacijami, pri čemer mora naročnikova konfiguracija vključevati zbirko ID-jev uporabnikov. V izogib dvoumnosti: ta ponudba storitve v oblaku ne vključuje pravice do uporabe platforme Trusteer Splash in/ali promocije odjemalske programske opreme imetnika računa naročnikovim splošnim upravičenim udeležencem na kakršenkoli drug način.

3.6.3 IBM Trusteer Pinpoint Malware Detection Redeployment

Naročniki, ki želijo ponovno razmestiti aplikacije za spletno bančništvo med obdobjem storitve, kar posledično zahteva spremembe pri razmestitvi storitve IBM Trusteer Pinpoint Malware Detection in/ali IBM Trusteer Pinpoint Malware Detection II, naj kupijo IBM Trusteer Pinpoint Malware Detection Redeployment.

Razmestitev je lahko potrebna, ker je naročnik spremenil domeno ali URL gostitelja aplikacije, pretvoril spletno aplikacijo v novo tehnologijo, se preselil na novo platformo spletnega bančništva ali dodal nov potek za prijavo v obstoječo aplikacijo.

V šestmesečnem obdobju prehoda na razmestitev je naročnik upravičen do dodatnih aplikacij, ki se izvajajo nad obstoječimi naročenimi aplikacijami na podlagi "ena proti ena".

3.6.4 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail in/ali IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

Za IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business se za razmestitev v vse dodatne poslovne aplikacije, ki niso prva aplikacija, zahteva pooblastilo za IBM Trusteer Pinpoint Malware Detection Additional Applications for Business. Za IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ali IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail se za razmestitev v vse dodatne prodajne aplikacije, ki niso prva aplikacija, zahteva pooblastilo za IBM Security Trusteer Pinpoint Malware Detection Additional Applications for Retail.

3.7 Izbirne dodatne storitve v oblaku za IBM Trusteer Pinpoint Criminal Detection for Business in/ali IBM Trusteer Pinpoint Criminal Detection for Retail in/ali za IBM Trusteer Pinpoint Criminal Detection II for Business in/ali IBM Trusteer Pinpoint Criminal Detection II for Retail

3.7.1 IBM Trusteer Pinpoint Criminal Detection Redeployment

Naročniki, ki želijo ponovno razmestiti aplikacije za spletno bančništvo med obdobjem storitve, kar posledično zahteva spremembe pri razmestitvi storitve IBM Trusteer Pinpoint Criminal Detection Cloud Service, naj kupijo IBM Trusteer Pinpoint Criminal Detection Redeployment.

Razmestitev je lahko potrebna, ker je naročnik spremenil domeno ali URL gostitelja aplikacije, pretvoril spletno aplikacijo v novo tehnologijo, se preselil na novo platformo spletnega bančništva ali dodal nov potek za prijavo v obstoječo aplikacijo.

V šestmesečnem obdobju prehoda na razmestitev je naročnik upravičen do dodatnih aplikacij, ki se izvajajo nad obstoječimi naročenimi aplikacijami na podlagi "ena proti ena".

3.7.2 IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business in/ali IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Za IBM Trusteer Pinpoint Criminal Detection II for Business se za razmestitev v vse dodatne poslovne aplikacije, ki niso prva aplikacija, zahteva pooblastilo za IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business. Za IBM Trusteer Pinpoint Criminal Detection II for Retail se za razmestitev v vse dodatne prodajne aplikacije, ki niso prva aplikacija, zahteva pooblastilo za IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail.

4. IBM Trusteer Fraud Protection Suite

IBM Trusteer Fraud Protection Suite ("Suite") je zbirka storitev v oblaku, ki je zasnovana za zagotavljanje plasti zaščite pred prevarami in jo je mogoče integrirati z dodatnimi IBM-ovimi produkti, s čimer se zagotovi rešitev za upravljanje življenjskega cikla. Suite vključuje naslednje storitve v oblaku:

- IBM Trusteer Pinpoint Detect, ki zaznava in blaži napade zlonamerne programske opreme, lažno predstavljanje in zlorabe računov. Storitev Trusteer Pinpoint Detect lahko naročnik integrira v svoje poslovne in/ali prodajne aplikacije, za katere ima naročnik naročnino za storitve v oblaku, in so vključene v postopke za preprečevanje prevar.
- IBM Trusteer Rapport for Mitigation, ki odpravlja in ščiti okužene končne točke.

Storitve v oblaku vključujejo:

a. TMA:

   Aplikacija TMA je na voljo v okolju IBM Trusteer, ki gostuje v oblaku, prek katerega lahko naročnik (in neomejeno število njegovih pooblaščencev): (i) prejema poročila o podatkih dogodkov in ocene

tveganja ter (ii) pregleduje, konfigurira in nastavlja varnostne pravilnike in pravilnike v zvezi s poročanjem o podatkih dogodkov.

b. Podatki o dogodkih:

Naročnik (in neomejeno število njegovega pooblaščenega osebja) lahko uporablja aplikacijo TMA za prejemanje podatkov o dogodkih, ustvarjenih na podlagi spletnih interakcij upravičenih udeležencev z naročnikovimi poslovnimi in/ali prodajnimi aplikacijami, za katere ima naročnik naročnino za storitev v oblaku, ali prejema podatke o dogodkih v načinu dostave prek zalednega API-ja.

c. Spletni skript in/ali API-ji:

Za razmestitev na spletnem mestu za namene dostopa do storitve v oblaku ali njene uporabe.

Dobre prakse Pinpoint

V primeru zaznavanja zlonamerne programske opreme ali zlorabe računa mora naročnik upoštevati navodila v Vodiču s primeri dobrih praks Pinpoint. Storitev v oblaku IBM Trusteer Pinpoint Detect ni dovoljeno uporabljati na načine, ki bi vplivali na izkušnjo upravičenega udeleženca neposredno po primeru zaznavanja zlonamerne programske opreme ali zlorabe računa in bi drugim osebam omogočali povezavo naročnikovih dejanj z uporabo ponudb IBM Trusteer Pinpoint Detect (npr. obvestila, sporočila, blokiranje naprav ali dostop do poslovne in/ali prodajne aplikacije neposredno po primeru zaznavanja zlonamerne programske opreme).

4.1 IBM Trusteer Pinpoint Detect Standard for Business in/ali IBM Trusteer Pinpoint Detect Standard for Retail

Ta storitev v oblaku združuje IBM Trusteer Pinpoint Criminal Detection in IBM Trusteer Pinpoint Malware Detection, kar zagotavlja enotno rešitev.

Ta rešitev ponuja pomoč pri brez-odjemalskem zaznavanju zlonamerne programske opreme in/ali sumljive dejavnosti zlorabe računa v brskalniku pri povezovanju s poslovno ali prodajno aplikacijo na podlagi ID-ja naprave, zaznavanja lažnega predstavljanja in zaznavanja kraje poverilnic, ki jo omogoča zlonamerna programska oprema. Ponudbe IBM Trusteer Pinpoint zagotavljajo dodatno plast zaščite, zaznavajo poskuse zlorabe računov in naročniku posredujejo ocene tveganja brskalnikov ali mobilnih naprav (prek izvirnega brskalnika ali naročnikove mobilne aplikacije), ki dostopajo do poslovne ali prodajne aplikacije.

V to storitev v oblaku je vključena standardna podpora (kot je opredeljena spodaj v razdelku o tehnični podpori). Za najvišjo stopnjo podpore mora naročnik kupiti ponudbo Detect Premium.

Ta storitev v oblaku vključuje zaščito za eno aplikacijo. Za vsako dodatno aplikacijo mora naročnik pridobiti pooblastilo za IBM Trusteer Pinpoint Detect Standard Additional Applications.

4.2 IBM Trusteer Pinpoint Detect Premium for Business in/ali IBM Trusteer Pinpoint Detect Premium for Retail

Ta storitev v oblaku združuje IBM Trusteer Pinpoint Criminal Detection in IBM Trusteer Pinpoint Malware Detection, kar zagotavlja enotno rešitev, ki je preprosta za integracijo.

Ta rešitev ponuja pomoč pri brez-odjemalskem zaznavanju zlonamerne programske opreme in/ali sumljive dejavnosti zlorabe računa v brskalniku pri povezovanju s poslovno ali prodajno aplikacijo na podlagi ID-ja naprave, zaznavanja lažnega predstavljanja in zaznavanja kraje poverilnic, ki jo omogoča zlonamerna programska oprema. Ponudbe IBM Trusteer Pinpoint zagotavljajo dodatno plast zaščite, zaznavajo poskuse zlorabe računov in naročniku posredujejo ocene tveganja brskalnikov ali mobilnih naprav (prek izvirnega brskalnika ali naročnikove mobilne aplikacije), ki dostopajo do poslovne ali prodajne aplikacije.

Ta storitev vključuje izboljšano delovanje in storitve, vključno z razširjenimi storitvami razmestitve in nastavitve, prilagojenimi varnostnimi pravilniki, storitvami pregledovanja itd.

Ta storitev v oblaku vključuje zaščito za eno aplikacijo. Za vsako dodatno aplikacijo mora naročnik pridobiti pooblastilo za IBM Trusteer Pinpoint Detect Premium Additional Applications.

V to storitev v oblaku je vključena najvišja stopnja podpore.

Pinpoint Detect Policy Manager:

Aplikacija Policy Manager je vključena v storitev Pinpoint Detect Premium in je na voljo v okolju IBM Trusteer, ki gostuje v oblaku, prek katerega lahko naročnik (in neomejeno število njegovih

pooblaščencev): (i) načrtuje, preizkuša in v produkcijsko okolje uvaja logiko za odkrivanje goljufive dejavnosti, (ii) načrtuje poročila in nadzorne plošče ter (iii) pregleduje, konfigurira in nastavlja varnostne pravilnike in pravilnike za odkrivanje sumljive dejavnosti v aplikaciji naročnika.

Za aktiviranje funkcije Policy Manager in za podporo za dodatno poglobljeno obravnavo so zahtevane svetovalne storitve. Podrobnosti o svetovalnih storitvah bodo podane ločeno v dogovoru o obsegu del.

Ko je funkcija Policy Manager aktivirana, si IBM pridržuje pravico do dostopa do naročnikovega okolja za namene podpore, da se naročnikovi pravilniki prilagodijo za odpravljanje večjih težav, ki izhajajo iz sprememb pravilnika.

Naročnik se zavezuje, da bo pred zlorabo varoval katere koli podatke, izpostavljene prek funkcije Policy Manager.

Ko je funkcija Policy Manager aktivirana, mora naročnik upoštevati IMB-ove smernice za določanje pravil, kot je navedeno v dokumentaciji. Naročnik potrjuje, da IBM ni odgovoren za nobeno situacijo, ki bi lahko izhajala iz naročnikovega neupoštevanja teh priporočil.

Kakršne koli težave s stabilnostjo in/ali poslabšanjem kakovosti storitve, ki bi lahko nastale zaradi naročnikove napačne konfiguracije funkcije Policy Manager, se ne bodo obravnavale kot čas nedelovanja za izračun v okviru pogodbe o ravni storitve.

4.3 IBM Trusteer Pinpoint Detect Standard with access management integration for Business in/ali IBM Trusteer Pinpoint Detect Standard with access management integration for Retail

Storitev v oblaku IBM Trusteer Pinpoint Detect Standard with access management integration vključuje funkcionalnost IBM Security Pinpoint Detect Standard, kot je opisano zgoraj v razdelku 4.1.

IBM Trusteer Pinpoint Detect Standard with access management integration se uporablja, ko je storitev kupljena s sistemi za upravljanje dostopa, kot je IBM Security Access Management ("ISAM"). Če je storitev kupljena s storitvijo ISAM, morata biti omogočeni obe ponudbi. Ta ponudba vključuje možnost integracije s sistemom za upravljanje dostopa. Ne vključuje pooblastila za sistem za upravljanje dostopa.

Ta ponudba vključuje zaščito za eno aplikacijo. Za vsako dodatno aplikacijo mora naročnik pridobiti pooblastilo za IBM Trusteer Pinpoint Detect Standard Additional Applications.

V to storitev v oblaku je vključena standardna podpora (kot je opredeljena v razdelku o tehnični podpori). IBM Trusteer Pinpoint Detect Premium with access management integration for Business in/ali IBM Trusteer Pinpoint Detect Premium with access management integration for Retail

Storitev v oblaku IBM Trusteer Pinpoint Detect Premium with access management integration vključuje funkcionalnost IBM Security Pinpoint Detect Premium, kot je opisano zgoraj v razdelku 4.2, in možnost integracije s sistemom za upravljanje dostopa.

IBM Trusteer Pinpoint Detect Premium with access management integration se uporablja, ko je storitev kupljena s sistemi za upravljanje dostopa, kot je IBM Security Access Management ("ISAM"). Če je storitev kupljena s storitvijo ISAM, morata biti omogočeni obe ponudbi. Ta storitev v oblaku vključuje možnost integracije s sistemom za upravljanje dostopa. Ne vključuje pooblastila za sistem za upravljanje dostopa.

Ta storitev v oblaku vključuje zaščito za eno aplikacijo. Za vsako dodatno aplikacijo mora naročnik pridobiti pooblastilo za IBM Trusteer Pinpoint Detect Premium Additional Applications.

V to ponudbo je vključena podpora Premium.

4.4 Izbirne storitve za IBM Trusteer Pinpoint Detect Standard in/ali IBM Trusteer Pinpoint Detect Premium

Za storitve v oblaku v tem razdelku je potrebno pooblastilo za ponudbo IBM Trusteer Pinpoint Detect Premium for Retail ali ponudbo IBM Trusteer Pinpoint Detect Standard for Retail.

4.5 IBM Trusteer Rapport for Mitigation for Retail in/ali IBM Trusteer Rapport for Mitigation for Business

IBM Trusteer Rapport for Mitigation je rešitev, ki preišče, popravi, blokira in odstrani okužbe z zlonamerno programsko opremo iz okuženih naprav (PC/Mac), ki jih uporabljajo naročnikovi upravičeni uporabniki za ad-hoc dostop do njegovih prodajnih aplikacij, v katerih so bile okužbe z zlonamerno programsko opremo zaznane na podlagi podatkov o dogodkih storitve IBM Trusteer Pinpoint Detect Premium ali IBM Trusteer Pinpoint Detect Standard. Naročnik mora imeti veljavno naročnino na ponudbo IBM Trusteer Pinpoint

Detect Premium ali IBM Trusteer Pinpoint Detect Standard, ki se dejansko izvajata v naročnikovi prodajni aplikaciji. Naročnik lahko uporablja to storitev v oblaku izključno v povezavi z upravičenimi udeleženci, ki dostopajo do naročnikove prodajne aplikacije, in izključno kot orodje, ki omogoča preiskovanje in popravilo določene okužene naprave (PC/Mac) na ad-hoc osnovi. Storitev IBM Trusteer Rapport for Mitigation for Retail se mora dejansko izvajati v taki okuženi napravi (PC/Mac) upravičenega udeleženca, ki mora soglašati s pogoji pogodbe EULA in vsaj enkrat izvesti overjanje v povezavi z naročnikovimi prodajnimi aplikacijami, pri čemer mora naročnikova konfiguracija vključevati zbirko ID-jev uporabnikov. V izogib dvoumnosti: ta storitev v oblaku ne vključuje pravice do uporabe platforme Trusteer Splash in/ali promocije odjemalske programske opreme imetnika računa naročnikovim splošnim upravičenim udeležencem na kakršenkoli drug način.

4.5.1 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business in/ali IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail in/ali IBM Trusteer Pinpoint Detect Premium Additional Applications for Business in/ali IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

Za razmestitev IBM Trusteer Pinpoint Detect Standard for Business v katerekoli dodatne poslovne aplikacije poleg prve aplikacije je potrebno pooblastilo za IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.

Za razmestitev IBM Trusteer Pinpoint Detect Standard for Retail v katerekoli dodatne prodajne aplikacije poleg prve aplikacije je potrebno pooblastilo za IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.

Za razmestitev IBM Trusteer Pinpoint Premium for Business v katerekoli dodatne poslovne aplikacije poleg prve aplikacije je potrebno pooblastilo za IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

Za razmestitev IBM Trusteer Pinpoint Premium for Retail v katerekoli dodatne prodajne aplikacije poleg prve aplikacije je potrebno pooblastilo za IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.

4.5.2 IBM Trusteer Pinpoint Detect Standard Redeployment in/ali IBM Trusteer Pinpoint Detect Premium Redeployment

Naročniki, ki želijo ponovno razmestiti aplikacije za spletno bančništvo med obdobjem storitve, kar posledično zahteva spremembe pri razmestitvi storitve IBM Trusteer Pinpoint Detect, naj kupijo IBM Trusteer Pinpoint Detect Redeployment.

Razmestitev je lahko potrebna, ker je naročnik spremenil domeno ali URL gostitelja aplikacije, pretvoril spletno aplikacijo v novo tehnologijo, se preselil na novo platformo spletnega bančništva ali dodal nov potek za prijavo v obstoječo aplikacijo.

V šestmesečnem obdobju prehoda na razmestitev je naročnik upravičen do dodatnih aplikacij, ki se izvajajo nad obstoječimi naročenimi aplikacijami na podlagi "ena proti ena".

5. Storitve v oblaku IBM Trusteer Mobile

5.1 IBM Trusteer Mobile Browser for Business in/ali IBM Trusteer Mobile Browser for Retail

Storitve v oblaku IBM Trusteer Mobile Browser so zasnovane tako, da zagotavljajo dodatno plast zaščite in mobilnim napravam upravičenih udeležencev omogočajo varen spletni dostop do naročnikovih prodajnih ali poslovnih aplikacij, za katere ima naročnik naročnino za storitve v oblaku, oceno tveganja mobilnih naprav in zaščito pred lažnim predstavljanjem. Zaznavanje varne povezave Wi-Fi je na voljo samo za platforme sistema Android. Mobilne naprave v okviru te storitve v oblaku vključujejo mobilne telefone ali tablične računalnike in ne vključujejo prenosnih računalnikov s sistemom Windows/Mac.

V okviru aplikacije TMA lahko naročnik prejema podatke o dogodkih, analize in statistične podatke v zvezi z napravami upravičenih udeležencev, ki so: (i) brezplačno prenesli odjemalsko programsko opremo imetnika računa, javno licencirano aplikacijo na podlagi licenčne pogodbe za končne uporabnike ("EULA"), ki je na voljo za prenos v mobilne naprave upravičenih udeležencev, ter (ii) podali soglasje s pogoji pogodbe EULA in vsaj enkrat izvedli overjanje v povezavi z naročnikovimi poslovnimi ali prodajnimi aplikacijami, za katere ima naročnik naročnino za storitve v oblaku. Naročnik lahko odjemalsko programsko opremo imetnika računa trži samo prek platforme Trusteer Splash in je ne sme uporabljati za interne poslovne operacije.

a. Podatki o dogodkih:

Naročnik (in neomejeno število njegovih pooblaščencev) lahko uporablja aplikacijo TMA za prejemanje podatkov o dogodkih, ustvarjenih na podlagi spletnih interakcij mobilnih naprav z naročnikovimi poslovnimi in/ali prodajnimi aplikacijami, za katere ima naročnik naročnino za storitve v oblaku.

b. Trusteer Splash:

Platforma za trženje Trusteer Splash predstavi in trži odjemalsko programsko opremo imetnika računa upravičenim udeležencem, ki dostopajo do naročnikovih poslovnih in/ali prodajnih aplikacij, za katere ima naročnik naročnino za storitve v oblaku. Naročnik lahko izbira med razpoložljivimi pozdravnimi predlogami ("pozdravna predloga"). Pozdravno okno po meri se lahko pogodbeno določi na podlagi ločene pogodbe ali dogovora o obsegu del.

Naročnik lahko soglaša, da svoje blagovne znamke, logotipe ali ikone ponudi v uporabo v povezavi z aplikacijo TMA in samo za uporabo s platformo Trusteer Splash ter za prikaz v odjemalski programski opremi imetnika računa ali na pristajalnih straneh, ki jih gosti IBM ali spletna stran IBM Trusteer. Vsaka uporaba naročnikovih blagovnih znamk, logotipov ali ikon bo v skladu z IBM-ovimi razumnimi načeli glede oglaševanja in uporabe blagovnih znamk.

5.2 IBM Trusteer Mobile SDK for Business in/ali IBM Trusteer Mobile SDK for Retail

Storitve v oblaku IBM Trusteer Mobile SDK so zasnovane tako, da zagotavljajo dodatno plast zaščite in varen spletni dostop do naročnikovih prodajnih ali poslovnih aplikacij, za katere ima naročnik naročnino za storitve v oblaku, oceno tveganja naprav in zaščito pred lažnim predstavljanjem. Zaznavanje varne povezave Wi-Fi je na voljo samo za platforme sistema Android.

Storitve v oblaku IBM Trusteer Mobile SDK vključujejo lastniški mobilni komplet razvijalca programske opreme ("SDK"), paket programske opreme, ki vključuje dokumentacijo, lastniške knjižnice s programsko opremo za programiranje in druge povezane datoteke in elemente (z drugim imenom mobilna knjižnica IBM Trusteer) ter "komponento za izvajalno okolje" oz. "kodo za vnovično razpošiljanje", ki je lastniška programska koda, generirana s kompletom IBM Trusteer Mobile SDK, katero je mogoče vdelati ali integrirati v naročnikove zaščitene samostojne mobilne aplikacije za sistem iOS ali Android, za katere ima naročnik naročnino za storitve v oblaku ("naročniško integrirana mobilna aplikacija").

IBM Trusteer Mobile SDK for Retail je na voljo v paketih po 100 upravičenih udeležencev ali 100 odjemalskih naprav, IBM Trusteer Mobile SDK for Business pa je na voljo v paketih po 10 upravičenih udeležencev ali 10 odjemalskih naprav.

Naročnik (in neomejeno število njegovih pooblaščencev) lahko prek aplikacije TMA prejme podatke o dogodku, ki poročajo o trendih tveganj in takšna tveganja tudi ocenjujejo. Naročnik lahko prek naročniško integrirane mobilne aplikacije prejema podatke o analizi tveganj in podatke o mobilnih napravah upravičenih udeležencev, ki so prenesli naročniško integrirano mobilno aplikacijo, s čimer se naročniku omogoči oblikovanje pravilnika za preprečevanje goljufij, na podlagi katerega je mogoče uvesti ukrepe za zmanjševanje teh tveganj. "Mobilne naprave" v okviru te ponudbe vključujejo samo mobilne telefone in tablične računalnike ter ne vključujejo prenosnih računalnikov (PC/Mac).

Naročnik lahko:

a. interno uporablja IBM Trusteer Mobile SDK izključno za namene razvijanja naročniško integrirane mobilne aplikacije;

b. vdela lastniško kodo za vnovično razpošiljanje (samo v obliki objektne kode) na združen, neločljiv način v naročniško integrirano mobilno aplikacijo Vsakršen spremenjeni ali spojeni del kode za vnovično razpošiljanje v okviru določil te licence bo predmet pogojev tega opisa storitev; ter

c. trži in razpošilja lastniško kodo za vnovično razpošiljanje za prenos v mobilne naprave upravičenih udeležencev ali odjemalsko napravo imetnika računa, pri čemer velja naslednje:

- Razen če je izrecno dovoljeno v tej pogodbi, naročnik ne sme (1) uporabljati, kopirati, spreminjati ali razširjati kompleta SDK; (2) obratno sestaviti, obratno prevesti ali drugače prevesti ali izvesti obratni inženiring kompleta SDK, razen v obsegu, ki je zakonsko izrecno brez možnosti pogodbene odpovedi; (3) izdajati podlicenc, izposojati ali dajati v najem kompleta SDK; (4) odstraniti nobene datoteke o avtorskih pravicah ali datoteke z obvestili, shranjene v paketu za vnovično razpošiljanje; (5) uporabiti istega imena poti kot je uporabljeno za izvorne datoteke/module za vnovično razpošiljanje; in (6) brez predhodnega pisnega soglasja IBM-a ali zadevnega dajalca licence oz. distributerja uporabiti imen ali blagovnih

znamk IBM-a, njegovih dajalcev licenc ali distributerjev v povezavi s trženjem naročniško integrirane mobilne aplikacije.

- Lastniška koda za vnovično razpošiljanje mora biti v naročniško integrirani mobilni aplikaciji integrirana na neločljiv način. Lastniška koda za vnovično razpošiljanje je lahko samo v obliki objektne kode ter mora biti v skladu z vsemi smernicami, navodili in specifikacijami v kompletu SDK in njegovi dokumentaciji. Naročnikova licenčna pogodba za končnega uporabnika za naročniško integrirano mobilno napravo mora končnega uporabnika obveščati o tem, da se lastniške kode za vnovično razpošiljanje ne sme i) uporabljati za noben drug namen kot omogočanje naročniško integrirane mobilne aplikacije, ii) kopirati (razen za namene varnostnega kopiranja), iii) nadalje razpošiljati ali prenesti, iv) obratno sestaviti, obratno prevesti ali kako drugače prevesti, razen v obsegu, ki je zakonsko izrecno dovoljen brez možnosti pogodbene odpovedi. IBM mora biti v naročnikovi licenčni pogodbi zaščiten vsaj v tolikšni meri kot z določili te pogodbe.
- Komplet SDK se sme razmestiti le kot del naročnikovega notranjega razvoja in preizkušanja enot, in sicer v mobilne naprave za preizkušanje, ki jih določi naročnik. Naročnik nima pooblastila za uporabo kompleta SDK za obdelavo produkcijskih delovnih obremenitev, simulacije produkcijskih delovnih obremenitev ali preizkušanja razširljivosti katerekoli kode, aplikacije ali sistema. Naročnik ni pooblaščen za uporabo kateregakoli dela kompleta SDK za katerikoli drug namen.

Naročnik je sam izključno odgovoren za razvoj, preizkušanje in podporo naročniško integrirane mobilne aplikacije. Naročnik je odgovoren za vso tehnično podporo v zvezi z naročniško integrirano mobilno aplikacijo in vse spremembe lastniških kod za vnovično razpošiljanje, ki jih izvede naročnik, in so dovoljene s to pogodbo.

Naročnik je pooblaščen za namestitev in uporabo kod za vnovično razpošiljanje in kompleta IBM Security Mobile SDK samo za namene podpore naročnikove uporabe storitev v oblaku.

IBM je preizkusil delovanje vzorčnih aplikacij, ustvarjenih z mobilnimi orodji kompleta IBM Trusteer Mobile SDK ("mobilna orodja"), in preveril, ali se izvajajo pravilno v nekaterih različicah mobilnih platform operacijskega sistema družb Apple (iOS), Google (Android) in drugih (s skupnim imenom "mobilne platforme OS"). Vendar mobilne platforme OS zagotavljajo drugi ponudniki, ki niso pod IBM-ovim nadzorom in se lahko spremenijo brez obvestila IBM-u. V skladu s tem in ne glede na morebitne nasprotne določbe IBM ne jamči za pravilno izvajanje, medsebojno delovanje ali združljivost katerekoli aplikacije ali drugega produkta, ki je ustvarjen z mobilnimi orodji, v kakršnihkoli platformah z mobilnim operacijskim sistemom ali mobilnih napravah.

Komponente v izvorni kodi in vzorčno gradivo - IBM Security Trusteer Mobile SDK lahko vključuje nekatere komponente v obliki izvorne kode ("komponente v izvorni kodi") in drugo gradivo, označeno kot vzorčno gradivo. Naročnik lahko kopira in spreminja komponente v izvorni kodi in vzorčno gradivo samo za notranjo uporabo v skladu z omejitvami licenčnih pravic iz te pogodbe, vendar ne sme spremeniti ali izbrisati katerihkoli informacij o avtorskih pravicah ali obvestil, ki jih vsebujejo komponente v izvorni kodi ali vzorčno gradivo. IBM zagotavlja komponente izvorne kode in vzorčno gradivo brez obvez podpore ter "TAKŠNO, KAKRŠNO JE", BREZ VSAKRŠNIH JAMSTEV, IZRECNIH ALI PREDPOSTAVLJENIH, KAR VKLJUČUJE JAMSTVO GLEDE PRAVNEGA NASLOVA, NEKRŠITVE OZ. NEMOTENJA TER PREDPOSTAVLJENA JAMSTVA IN POGOJE GLEDE PRIMERNOSTI ZA PRODAJO IN USTREZNOSTI ZA DOLOČEN NAMEN. Naročnik naj upošteva, da so komponente v izvorni kodi ali vzorčno gradivo zagotovljeni samo kot primer načina uvedbe elementov, ki jih je mogoče vdelati v naročniško integrirano mobilno aplikacijo, da komponente v izvorni kodi ali vzorčna gradiva morda ne bodo združljivi z naročnikovim razvojnim okoljem, in da je naročnik sam odgovoren za preizkušanje in uvedbo elementov, ki jih je mogoče vdelati, v svojo naročniško integrirano mobilno aplikacijo.

Naročnik soglaša s tem, da bo ustvaril, hranil ter IBM-u in njegovim revizorjem posredoval točno pisno dokumentacijo, rezultate sistemskega orodja in druge zadostne informacije o sistemu, ki omogočajo zanesljivo preverjanje tega, ali je naročnikova uporaba kompleta IBM Trusteer Mobile SDK v skladu s pogoji tega opisa storitev.

6. Najvišja stopnja podpore

Naročnik je upravičen do podpore Premium le za storitve v oblaku, za katere ima naročnino na povezano ponudbo Premium Support.

7. Razmestitev izdelka IBM Trusteer Fraud Protection

Za vsako aplikacijo, na katero se naročnik naroči, osnovna naročnina vključuje potrebna dejanja nastavitve in začetne razmestitve v oblak IBM Trusteer, vključno z začetnim enkratnim zagonom, konfiguracijo, pozdravno predlogo, preizkušanjem in usposabljanjem.

Dejanja razmestitve ne vključujejo dejanj uvedbe, ki so potrebna pri naročnikovih aplikacijah ali sistemih.

Faza uvedbe različnih storitev v oblaku je zasnovana za uvedbo znotraj časovnih okvirov, kot je opisano v ustreznih vodičih o razmestitvi.

Dokončanje teh faz uvedbe v dodeljenem časovnem okviru je odvisno od polne zavezanosti in sodelovanja naročnikovega vodstva in osebja. Naročnik mora pravočasno zagotoviti zahtevane podatke. IBM-ova učinkovitost temelji na naročnikovih pravočasnih informacijah in odločitvah, morebitne zamude pa lahko povzročijo dodatne stroške in/ali zamudo pri dokončanju teh storitev uvedbe.

Za vsako aplikacijo, na katero se naročnik naroči, osnovna naročnina vključuje potrebna dejanja nastavitve in začetne razmestitve v oblak IBM Trusteer, vključno z začetnim enkratnim zagonom, konfiguracijo, pozdravno predlogo, preizkušanjem in usposabljanjem.

Naročnikova naročnina vključuje podporo in preizkušanje strani v naročnikovih aplikacijah, ki jih bo IBM pri začetni razmestitvi označil kot priporočljive. IBM ni odgovoren za: (i) delno razmestitev, (ii) naročnikovo izbiro, da ne bo razmestil IBM-ovih storitev tako, kot priporoča IBM, ali (iii) naročnikovo izbiro, da bo razmestitev, nastavitev in preizkušanje izvedel sam, (iv) delno razmestitev ali rezultate zaščite zaradi neustreznih informacij naročnika. Za dodatne storitve, vključno z dodatnimi razmestitvami poleg začetne razmestitve, se lahko sklene ločena pogodba, ki zajema dodatne stroške.

8. Zasebnost in varstvo osebnih podatkov

Ta storitev v oblaku je v skladu z IBM-ovimi načeli glede zaščite podatkov in zasebnosti za storitve v oblaku, ki so na voljo na spletnem mestu http://www.ibm.com/cloud/data-security, in vsemi drugimi določili v tem razdelku. Morebitne spremembe IBM-ovih načel glede zaščite podatkov in zasebnosti ne bodo zmanjšale stopnje varnosti storitev v oblaku.

Te storitve v oblaku se lahko uporabljajo za obdelavo vsebine z osebnimi podatki, če naročnik kot upravljavec podatkov presodi, da so tehnični in organizacijski varnostni ukrepi ustrezni glede na tveganje, ki ga pomenita obdelava in vrsta podatkov, ki jih je treba zaščititi. Naročnik se zaveda, da te storitev v oblaku ne ponujajo funkcij za zaščito občutljivih osebnih podatkov ali podatkov, za katere veljajo dodatne regulativne zahteve.

Te storitve v oblaku so vključene v IBM-ovo potrdilo o zasebnostnem ščitu in se uporabljajo, če se naročnik odloči gostovati storitve v oblaku v podatkovnem središču v Združenih državah, zanje pa velja IBM-ov zasebnostni pravilnik o zasebnostnem ščitu, ki je na voljo na naslovu http://www.ibm.com/privacy/details/us/en/privacy_shield.html.

8.1 Varnostne funkcije in dolžnosti

Storitve v oblaku vključujejo naslednje varnostne funkcije:

Storitev v oblaku šifrira vsebino pri prenosu podatkov v IBM-ovo omrežje in iz njega ter pri čakanju na prenos podatkov s končne točke.

8.2 Zakonita uporaba in soglasje

Zakonita uporaba

Uporaba te storitve v oblaku lahko vključuje različne zakone ali predpise. Storitev v oblaku se lahko uporablja samo za zakonite namene in na zakonit način. Naročnik soglaša, da bo uporabljal storitev v oblaku v skladu z veljavnimi zakoni, predpisi in pravilniki, pri čemer prevzema vso odgovornost za njihovo upoštevanje.

Pooblastilo za zbiranje in obdelavo podatkov

Storitev v oblaku bo zbirala informacije od upravičenih udeležencev in odjemalskih naprav, ki komunicirajo s poslovnimi ali prodajnimi aplikacijami, za katere ima naročnik naročnino za pokritje storitev v oblaku. Storitev v oblaku zbira informacije, ki lahko samostojno ali v kombinaciji v nekaterih sodnih pristojnostih štejejo za osebne podatke. Osebni podatki so vsi podatki, ki omogočajo identifikacijo posameznika, kot so ime, e-poštni naslov, domači naslov ali telefonska številka, in so posredovani IBM-u za shranjevanje, obdelavo ali prenos v imenu naročnika.

Postopki zbiranja in obdelave podatkov se lahko posodobijo zaradi zagotavljanja boljše funkcionalnosti storitve v oblaku. Po potrebi je posodobljen tudi dokument s popolnim opisom teh postopkov, ki je naročniku na voljo na podlagi zahteve. Naročnik pooblašča IBM za zbiranje teh podatkov in njihovo obdelavo v skladu z razdelkoma Prenos prek meje in Zasebnost podatkov iz tega opisa storitve.

Za ponudbe IBM Trusteer, ki vključujejo Trusteer Management Application (TMA):

Za skrbnike TMA iz podpornega podjetja se v aplikaciji Trusteer Management Application (TMA) zbirajo in shranjujejo naslednji podatki: e-poštni naslov (za prijavo), zgoščeno geslo, ime, priimek, službeni naziv in oddelek.

Za storitve v oblaku IBM Trusteer Pinpoint:

Zbrani podatki lahko vključujejo naslednje:

- identifikatorje uporabnika ali končne točke, kot je šifriran ID uporabnika ali ID uporabnika z enkratno razpršitvijo, trajni ID uporabnika (PUID), ključ posrednika za Rapport in ID seje stranke;
- podatke, povezane z zaščiteno aplikacijo, na primer posamezni atributi/elementi strankine aplikacije za spletno bančništvo, kot so upodobljeni v brskalniku, obiskih spletnih mest in zgodovini brskanja končnega uporabnika;
- podatke o okolju nameščene programske opreme, atributih in nastavitvah brskalnika in naprav ter dolžini zgodovine brskalnika;
- podatke o strojni opremi in časovni žig strojne opreme;
- glave brskalnika in podatke o komunikacijskem protokolu, kot so uporabnikov naslov IP, piškotki, glava sklicatelja in druge glave HTTP;
- podatke o premikanju miške končnega uporabnika, kot so koordinate kazalnika miške, kliki in premiki drsnega kolesca (in njegovih ekvivalentov), ter časovni žig pri interakciji z naročnikovo aplikacijo za spletno bančništvo;
- spletna mesta za lažno predstavljanje in podatke, poslane v spletna mesta za lažno predstavljanje; in
- po izbiri naročnika tudi transakcijske podatke (znesek transakcije, valuto transakcije in oznako cilja, identifikacijsko kodo banke prejemnika transakcije z enkratno razpršitvijo, identifikacijsko kodo računa prejemnika transakcije z enkratno razpršitvijo, binarno vrednost, če gre pri transakciji za novega plačnika, in datum/čas transakcije) ter izbirno oceno podatkov o tveganju.
- izključno po naročnikovi izbiri: vnašanje ritmov s tipkovnico in zaporedij skupin pritiskov na tipke, ki jih je uporabil končni uporabnik za vnos uporabniškega imena, gesla in drugega besedila (toda ne črk, številk ali posebnih znakov samih in brez možnosti razločevanja uporabniškega imena ali gesla);

Ko je funkcija Policy Manager aktivirana, je za vse dodatne podatke, ki se uporabljajo, odgovoren izključno naročnik. IBM priporoča razprševanje ali šifriranje podatkov, ki se lahko obravnavajo kot osebni identifikatorji.

Naročnik razume in soglaša, da IBM ne pridobiva, shranjuje, upravlja ali hrani uradnih evidenc in/ali zapisov o naročniku.

Ko naročnik sklene naročnino za ponudbo IBM Trusteer Rapport for Remediation, ali v nekaterih primerih podpore za Pinpoint, lahko IBM priporoči namestitev odjemalske programske opreme imetnika računa za Rapport v napravo upravičenega udeleženca za namen raziskovanja in preiskovanja suma okužbe z zlonamerno programsko opremo. Zbrani podatki ponudb Rapport so navedeni spodaj.

Za storitve v oblaku IBM Trusteer Rapport (vključno z Rapport for Remediation ali Rapport for Mitigation pri razmestitvi v povezavi s ponudbami Pinpoint):

Zbrani podatki lahko vključujejo naslednje:

- URL-je in naslove internetnega protokola (IP) spletnih mest, ki jih imetnik računa obišče in za katera IBM meni, da so lahko goljufiva, lažna ali izkoriščevalska, ter podatke o vrsti prepoznanih groženj;
- URL-je in naslove IP spletnih mest, ki jih imetnik računa obišče in jih naročnik nadzoruje ter so zaščitena s storitvami v oblaku, kot so spletna mesta za spletno bančništvo; naslove IP imetnika računa;

- podatke o prepoznavanju strojne opreme, operacijskih sistemih, aplikacijski programski opremi, periferni strojni opremi, varnostni konfiguraciji, sistemskih nastavitvah in omrežnih povezavah končne točke kakor tudi ID, ime, vzorce uporabe in druge podatke za prepoznavo končne točke;
- podatke, povezane z namestitvijo in delovanjem programa, ID programa, različico programa, varnostne dogodke, ki jih ustvari končna točka, in podatke o napakah programa;
- statistiko uporabe in statistične podatke o grožnjah, ki jih je program zaznal; dnevniške datoteke zrušitev brskalnika, datum in čas okužbe ter podatke o vrsti prepoznanih groženj ali okvar delovanja;
- naročnikovo pripadnost organizaciji, imenovani tudi podporno podjetje. Pripadnost se vzpostavi, ko končni uporabnik prenese Rapport z naročnikovega spletnega mesta, izbere določenega naročnika, ko prenaša Rapport s podpornega spletnega mesta za Trusteer, ali ko se prijavi v bančno aplikacijo naročnika. Končni uporabnik ima lahko več kot eno pripadnost naročniku;
- kopijo šifriranega ID-ja uporabnika, ki ga imetnik računa uporablja za interakcijo z naročnikom (izbirno);
- šifrirano kopijo številke kreditne kartice, ki jo imetnik računa vnese na spletno mesto, potem ko program imetnika računa obvesti, da na spletnem mestu obstaja tveganje;
- datoteke in druge podatke končne točke, za katere IBM-ovi strokovnjaki za varnost sumijo, da so povezani z zlonamerno programsko opremo ali drugo zlonamerno dejavnostjo ali da so lahko povezani s splošno okvaro delovanja programa; in
- osebne kontaktne podatke, vključno z imenom in e-poštnim naslovom, ko se uporabnik obrne na ekipo za podporo.

Za storitve v oblaku IBM Trusteer Mobile SDK in IBM Trusteer Mobile Browser:

Zbrani podatki lahko vključujejo naslednje:

- identifikatorje uporabnika, kot je šifriran ID uporabnika ali ID uporabnika z enkratno razpršitvijo;
- podatke o napravi, kot so IP-naslov, razpršen ID naprave, časovni žig, nameščene vrednosti paketa MD5 in druge podatke o strojni in programski opremi;
- različico programske opreme Mobile SDK ali Mobile Browser in datum namestitve;
- podatke o obiskih zaščitenih aplikacij;
- podatke o naročnikovi pripadnosti organizacijam; in
- podatke o tveganju v napravi (npr. prisotnost zlonamerne programske opreme, skrivanje korenskega dostopa, stanje šifriranosti omrežij Wi-Fi, ali ima naprava odprt dostop do sistema);
- sledi zrušenih skladov (v primeru nepričakovane prekinitve delovanja aplikacije);
- podatke o gradnji telefona (npr. model, proizvajalec);
- interakcija končnih uporabnikov z zaslonom na dotik, vključno s koordinatami x, y, področjem dotika ter vrsto dejanja (dol, gor in premik);
- podatke senzorja gibanja, uporabe energije/virov, nastavitev povezljivosti, senzorjev okolja, kot so podatki temperature, svetlobe in zračnega tlaka, ter splošnih nastavitev naprave (glasnost, zvonec, svetlost zaslona itd.).

8.3 Prostovoljno soglasje posameznikov, na katere se nanašajo osebni podatki

Za storitve v oblaku IBM Trusteer Pinpoint in storitve v oblaku IBM Trusteer Mobile SDK:

Naročnik izjavlja, da bo oziroma je pridobil vsa informirana soglasja, dovoljenja ali licence, ki jih potrebuje za to, da lahko zakonito uporablja storitev v oblaku in dovoli IBM-u zbiranje in obdelavo podatkov prek storitve v oblaku.

Za storitve v oblaku IBM Trusteer Rapport (vključno z Rapport Remediation ali Rapport for Mitigation pri razmestitvi v povezavi s storitvami v oblaku Pinpoint) in storitve v oblaku IBM Trusteer Mobile Browser:

Naročnik pooblašča IBM za pridobitev informiranih soglasij, ki so potrebna za omogočanje zakonite uporabe storitev v oblaku, ter za zbiranje in obdelavo informacij, kot je opisano v licenčni pogodbi za končne uporabnike, dostopni na naslovu https://www.trusteer.com/support/end-user-license-agreement. Če se naročnik odloči, da bo sam (in ne IBM) vzpostavil komunikacijo glede soglasja s končnimi uporabniki, soglaša, da je oziroma bo pridobil morebitna informirana soglasja, dovoljenja ali licence,

potrebne za omogočanje zakonite uporabe IBM-ovih storitev v oblaku, ter bo IBM-u kot svojemu obdelovalcu podatkov dovolil zbiranje in obdelavo podatkov v okviru IBM-ovih storitev v oblaku.

8.4 Uporaba varnostnih podatkov

Kot del storitev v oblaku, ki vključujejo poročanje, bo IBM pripravil in hranil anonimizirane in/ali združene podatke, zbrane iz storitev v oblaku ("varnostni podatki"). Varnostni podatki ne bodo razkrili identitete naročnika, njegovih upravičenih udeležencev ali posameznikov, razen v spodnjih primerih iz točke (d). Naročnik soglaša, da lahko IBM trajno uporablja in/ali kopira varnostne podatke le za naslednje namene:

a. objavljanje in/ali distribucija varnostnih podatkov (npr. pri zbiranju in/ali analizi v povezavi s kibernetično varnostjo);

b. razvijanje ali izboljševanje produktov ali storitev;

c. izvajanje raziskav znotraj IBM-a ali v sodelovanju s tretjimi osebami;

d. zakonito skupno rabo potrjenih informacij o storilcu, ki je tretja oseba; in

e. deidentificirana pravila iz funkcije Policy Manager.

8.5 Prenos prek meje

Naročnik soglaša, da lahko IBM v skladu z veljavno zakonodajo in zahtevami za posredovanje podatkov prek državne meje posreduje vsebino, vključno z morebitnimi osebnimi podatki, opredeljenimi v razdelku Zakonita uporaba in soglasje, prek državne meje obdelovalcem in podobdelovalcem v naslednjih državah zunaj Evropskega gospodarskega prostora in državah, ki imajo po mnenju Evropske komisije ustrezne ravni zaščite: Združene države Amerike.

8.6 Zasebnost podatkov

Če naročnik da na voljo osebne podatke storitvi v oblaku v državah članicah EU, Islandiji, Lihtenštajnu, Norveški ali Švici oziroma če ima naročnik v teh državah upravičene udeležence ali odjemalske naprave, naročnik kot izključni upravljavec imenuje IBM kot obdelovalca za obdelavo osebnih podatkov (kot so ti izrazi opredeljeni v Direktivi EU 95/46/ES). IBM bo obdeloval takšne osebne podatke samo v obsegu, ki je potreben za zagotavljanje storitve v oblaku v skladu z IBM-ovimi objavljenimi opisi storitve v oblaku, pri čemer naročnik potrjuje, da je takšna obdelava v skladu z njegovimi navodili. Če IBM bistveno spremeni lokacijo obdelave ali način varovanja osebnih podatkov v okviru storitve v oblaku, bo naročnika o tem primerno vnaprej obvestil prek portala za naročnike. Naročnik lahko odpove trenutno naročniško obdobje za ustrezno storitev v oblaku, tako da IBM-u predloži pisno obvestilo o odpovedi storitve trideset (30) dni po IBM-ovem obvestilu o spremembi.

Pogodbeni stranki ali njune povezane družbe lahko sklenejo ločeno standardno pogodbo z nespremenjenimi vzorčnimi klavzulami EU za ustrezne vloge v skladu s Sklepom Komisije 2010/87/EU, iz katere so odstranjene izbirne klavzule. Pogodbeni stranki bosta vsak spor ali odgovornost, ki izhaja iz teh dogovorov, tudi če so take dogovore sklenile povezane družbe, obravnavali, kot da je do spora ali odgovornosti prišlo med njima na podlagi določb te pogodbe.

a. Naročnik soglaša, da lahko IBM za storitev, zagotovljeno prek nemškega podatkovnega središča, kot je bilo določeno v postopku zagotavljanja, posreduje vsebino, vključno z morebitnimi osebnimi podatki, v obdelavo prek državne meje naslednjim obdelovalcem in podobdelovalcem:

Ime obdelovalca/podobdelovalca	Vloga (obdelovalec ali podobdelovalec podatkov)	Lokacija
IBM-ov pogodbeni subjekt	Obdelovalec	Kot je navedeno v transakcijskem dokumentu
Spletne storitve Amazon (Nemčija)	Podobdelovalec	Nemčija
IBM Ireland Ltd.	Obdelovalec	Irska
IBM Israel Ltd.	Obdelovalec	Izrael

Za storitve, ki se opravljajo prek nemškega podatkovnega središča, lahko nekatere storitve podpore strankam zagotavljajo zaposleni podjetja Trusteer v kateri koli državi Evropske unije.

b. Naročnik soglaša, da lahko IBM za storitev, zagotovljeno prek japonskega podatkovnega središča, kot je bilo določeno v postopku zagotavljanja, posreduje vsebino, vključno z morebitnimi osebnimi podatki, v obdelavo prek državne meje naslednjim obdelovalcem in podobdelovalcem:

Ime obdelovalca/podobdelovalca	Vloga (obdelovalec ali podobdelovalec podatkov)	Lokacija
IBM-ov pogodbeni subjekt	Obdelovalec	Japonska, kot je navedeno v transakcijskem dokumentu
Spletne storitve Amazon (Japonska)	Podobdelovalec	Japonska
IBM Ireland Ltd.	Obdelovalec	Irska
IBM Israel Ltd.	Obdelovalec	Izrael

c. Naročnik soglaša, da lahko IBM za storitev, zagotovljeno prek ameriškega podatkovnega središča, posreduje vsebino, vključno z morebitnimi osebnimi podatki, v obdelavo prek državne meje naslednjim obdelovalcem in podobdelovalcem:

Ime obdelovalca/podobdelovalca	Vloga (obdelovalec ali podobdelovalec podatkov)	Lokacija
IBM-ov pogodbeni subjekt	Obdelovalec	Kot je navedeno v transakcijskem dokumentu
Amazon Web Services LLC	Podobdelovalec	Združene države Amerike
IBM Ireland Ltd.	Obdelovalec	Irska
IBM Israel Ltd.	Obdelovalec	Izrael
IBM Corp	Obdelovalec	Združene države Amerike

d. Za storitve, zagotovljene prek podatkovnih središč iz razdelka 8.5.c. zgoraj, "ameriško podatkovno središče", lahko IBM obdeluje tudi prek enega ali več ustreznih podobdelovalcev, ki sledijo v nadaljevanju, kot je bilo določeno v postopku zagotavljanja:

Ime obdelovalca/podobdelovalca	Vloga (obdelovalec ali podobdelovalec podatkov)	Lokacija
Spletne storitve Amazon (Avstralija)	Podobdelovalec	Avstralija
Spletne storitve Amazon (Singapur)	Podobdelovalec	Singapur
Spletne storitve Amazon (Irska)	Podobdelovalec	Irska

e. Naročnik soglaša, da lahko IBM ob predhodnem obvestilu prek portala za naročnike preseli obdelavo iz spletnih storitev Amazon v IBM-ova podatkovna središča. IBM lahko ob predhodnem obvestilu prek portala za naročnike spremeni seznam zgornjih podobdelovalcev.

f. Podatki imetnika računa bodo obdelani v regiji, v kateri je imetnik računa prvotno namestil svojo odjemalsko programsko opremo. To lahko pomeni, da je vsebina imetnika računa lahko obdelana v dveh regijah, in sicer v prvotni regiji in regiji, s katero soglaša naročnik.

g. Podatki o podpori za stranke so shranjeni v strežniku v oblaku Salesforce.com, ki se nahaja v Irski.

h. Za namen razjasnitve: ker je Trusteer Fraud Protection integrirana rešitev, lahko IBM v primeru, če naročnik odpove katero od teh storitev v oblaku, obdrži podatke naročnika za namene zagotavljanja preostalih storitev v oblaku naročniku v skladu s tem opisom storitve.

9. Pogodba o ravni storitev

IBM za storitev v oblaku zagotavlja naslednjo pogodbo o ravni storitev za razpoložljivost ("SLA"), kot je navedeno v dokazilu o upravičenosti. Pogodba o ravni storitev ne zagotavlja jamstva/garancije. Pogodba o ravni storitev je na voljo samo naročniku in velja samo za uporabo v produkcijskih okoljih.

9.1 Dobropisi za razpoložljivost

Naročnik mora pri IBM-ovi službi za tehnično podporo vložiti prijavo za podporo ravni resnosti 1, in sicer v 24 urah od trenutka, ko ugotovi, da je dogodek vplival na razpoložljivost storitev v oblaku. Naročnik mora razumno pomagati IBM-u pri diagnosticiranju in razreševanju težav.

Naročnik mora predložiti zahtevek za podporo na podlagi prijave zaradi neizpolnjevanja pogodbe o ravni storitev v treh delovnih dneh po koncu pogodbenega meseca. Nadomestilo za upravičen zahtevek na podlagi pogodbe o ravni storitev (SLA) bo priznano kot dobropis pri naslednjem računu za storitev v oblaku na podlagi obdobja, v katerem obdelovanje produkcijskega sistema za storitev v oblaku ni na voljo ("nerazpoložljivost"). Nerazpoložljivost se meri od trenutka, ko je naročnik poročal o dogodku, do trenutka, ko je bilo obnovljeno delovanje storitve v oblaku, in ne vključuje časa, ki je povezan z izpadom zaradi načrtovanega ali napovedanega vzdrževanja; zaradi vzrokov, ki so zunaj IBM-ovega nadzora; zaradi težav z vsebino, tehnologijo, zasnovo ali navodili naročnika ali tretje osebe; zaradi nepodprtih sistemskih konfiguracij in platform ali zaradi drugih napak naročnika; ali zaradi varnostnega incidenta, ki ga je povzročil naročnik ali naročnikovo preizkušanje varnosti. IBM bo uveljavil najvišje veljavno nadomestilo na podlagi zbirne razpoložljivosti storitve v oblaku v vsakem pogodbenem mesecu, kot je prikazano v spodnji tabeli. Celotno nadomestilo za posamezni pogodbeni mesec ne sme presegati 10 odstotkov ene dvanajstine (1/12) letnih stroškov za storitev v oblaku.

9.2 Ravni storitev

Razpoložljivost storitve v oblaku v pogodbenem mesecu

Razpoložljivost v pogodbenem mesecu	Nadomestilo (odstotek mesečne naročnine* za pogodbeni mesec, na katerega se nanaša zahtevek)
< 99,5 %	2 %
< 98,0 %	5 %
< 96,0 %	10 %

* Če je naročnik storitev v oblaku pridobil od IBM-ovega poslovnega partnerja, se mesečna naročnina izračuna na podlagi takrat veljavne cene za storitev v oblaku, ki velja za pogodbeni mesec, na katerega se nanaša zahtevek, pri čemer bo upoštevan 50-odstotni popust. IBM bo rabat omogočil neposredno naročniku.

Ravni storitev in s tem povezani dobropisi za storitev se merijo ločeno za vsako posamezno storitev v oblaku in aplikacijo naročnika.

Pri izračunavanju dobropisov za raven storitve za storitve v oblaku na podlagi pooblastil za aplikacijo, se razpoložljivost izračuna na podlagi naslednjih smernic:

- Vsaki aplikaciji se dodeli utežen delež glede na prešteto število sej tekom pogodbenega meseca.
- Čas nerazpoložljivosti vsake storitve v oblaku na aplikacijo se akumulira ločeno za pogodbeni mesec.

V nadaljevanju je predstavljen primer izračuna za en mesec dejavnosti ter s tem povezano uteževanje. Namenjen je le ponazoritvi:

Prodajne aplikacije	Delež skupnega št. sej v danem pogodbenem mesecu	Skupni čas nerazpoložljivosti tekom pogodbenega meseca	Utežene minute časa nerazpoložljivosti
Pogodbena aplikacija A	40 %	300 minut	40 % x. 300 minut = 120 minut
Pogodbena aplikacija B	20 %	250 minut	20 % x 250 minut = 50 minut
Pogodbena aplikacija C	40 %	150 minut	40 % x 150 minut = 60
			Skupno uteženih minut časa nerazpoložljivosti = 230

Razpoložljivost, izražena v odstotkih, se izračuna kot: skupno število minut v pogodbenem mesecu, zmanjšano za skupno število uteženih minut nerazpoložljivosti v pogodbenem mesecu, deljeno s skupnim številom minut v pogodbenem mesecu. Vzorčni izračun na podlagi zgornjega uteženega primera je naslednji:

Skupaj 43.200 minut v 30-dnevnem pogodbenem mesecu - 230 minut uteženega časa nerazpoložljivosti = 42.970 minut _____ Skupaj 43.200 minut	= 2-odstotni dobropis za razpoložljivost za 99,4-odstotno razpoložljivost v pogodbenem mesecu

10. Tehnična podpora

Naročniku in njegovim upravičenim udeležencem je kot pomoč pri uporabi storitev v oblaku na voljo tehnična podpora.

Standardna podpora je vključena v naročnino za vse ponudbe. Trusteer Rapport Mandatory Service, ki je dodatek k produktu Trusteer Rapport, zahteva podporo Premium za osnovne naročnine Trusteer Rapport.

Za vsako storitev v oblaku je za dodatno plačilo na voljo podpora Premium, razen za storitve v oblaku IBM Security Trusteer Mobile SDK in storitve v oblaku IBM Trusteer Rapport Mandatory Service. Naročnik naj se obrne na IBM-ovega prodajnega predstavnika ali IBM-ovega poslovnega partnerja.

Standardna podpora:

- Podpora od 8.00 do 17.00 po lokalnem času.
- Naročniki in njihovi upravičeni udeleženci lahko vložijo elektronske prijave za podporo, kot je podrobno navedeno v priročniku za podporo programske opreme kot storitve [SaaS].
- Naročniki imajo dostop do portala za podporo naročnikom, kjer so na voljo obvestila, dokumenti, poročila o primerih in odgovori na pogosta vprašanja: http://www-01.ibm.com/software/security/trusteer/support/.
- Možnosti podpore in podrobnosti o dostopu so na voljo v priročniku za podporo programske opreme kot storitve [SaaS]: http://www-01.ibm.com/software/support/handbook.html.

Podpora Premium:

- Neprekinjena podpora za vse ravni resnosti.
- Naročniki lahko dobijo podporo neposredno po telefonu ali z zahtevo po povratnem klicu.
- Naročniki in njihovi upravičeni udeleženci lahko vložijo elektronske prijave za podporo, kot je podrobno navedeno v priročniku za podporo programske opreme kot storitve [SaaS].
- Naročniki imajo dostop do portala za podporo naročnikom, kjer so na voljo obvestila, dokumenti, poročila o primerih in odgovori na pogosta vprašanja: http://www-01.ibm.com/software/security/trusteer/support/.
- Možnosti podpore in podrobnosti o dostopu so na voljo v priročniku za podporo programske opreme kot storitve [SaaS]: http://www-01.ibm.com/software/support/handbook.html.

11. Pooblastila in zaračunavanje

11.1 Metrike zaračunavanja

Storitev v oblaku je na voljo na podlagi naslednje metrike zaračunavanja, ki je določena v transakcijskem dokumentu:

a. Upravičeni udeleženec je merska enota, na podlagi katere je mogoče pridobiti storitev v oblaku. Upravičeni udeleženec je vsak posameznik ali subjekt, ki lahko sodeluje v kateremkoli programu za dobavo storitev, ki ga upravlja ali mu sledi storitev v oblaku. Naročnik mora pridobiti zadostna pooblastila za kritje vseh upravičenih udeležencev, ki jih upravlja ali sledi storitev v oblaku med meritvenim obdobjem, navedenim v naročnikovem transakcijskem dokumentu.

   Vsak program za dobavo storitev, ki ga upravlja storitev v oblaku, se analizira ločeno in nato prišteje k drugim. Posamezniki ali subjekti, ki lahko uporabljajo več programov za dobavo storitev, morajo pridobiti ločena pooblastila.

   Za namene pooblaščanja v okviru teh storitev v oblaku je upravičeni udeleženec naročnikov končni uporabnik, ki ima unikatne prijavne poverilnice za naročnikovo aplikacijo za poslovanje ali prodajo.

b. Odjemalska naprava je merska enota, na podlagi katere je mogoče pridobiti storitev v oblaku. Odjemalska naprava je posamezna uporabniška računalniška naprava ali senzorska ali telemetrična naprava za posebni namen, ki zahteva izvajanje ali prejme v izvajanje niz ukazov, postopkov ali aplikacij iz drugega računalniškega sistema ali ki posreduje podatke v drug računalniški sistem, ki je običajno poimenovan strežnik ali ki jo kako drugače upravlja strežnik. Več odjemalskih naprav lahko souporablja dostop do skupnega strežnika. Odjemalska naprava lahko vključuje nekatere zmožnosti obdelave podatkov ali programiranja za omogočanje uporabniškega dela. Naročnik mora pridobiti pooblastilo za vsako odjemalsko napravo, ki izvaja storitev v oblaku, ji posreduje podatke, uporablja njene storitve ali do nje kako drugače dostopa med meritvenim obdobjem, navedenim v naročnikovem transakcijskem dokumentu.

c. Aplikacija je merska enota, na podlagi katere je mogoče pridobiti storitev v oblaku. Aplikacija je programska oprema z edinstvenim imenom. Naročnik mora pridobiti zadostna pooblastila za vsako aplikacijo, do katere je mogoče dostopati in jo uporabljati v meritvenem obdobju, navedenem v naročnikovem dokazilu o upravičenosti ali transakcijskem dokumentu.

   V okviru storitve v oblaku je aplikacija ena sama naročnikova poslovna ali prodajna aplikacija.

d. Sodelovanje je merska enota, na podlagi katere je mogoče pridobiti storitve. Sodelovanje je sestavljeno iz strokovnih storitev in/ali storitev usposabljanja, povezanih s storitvami v oblaku. Naročnik mora pridobiti zadostna pooblastila, da z njimi pokrije vse primere uporabe.

12. Ustreznost in preverjanje

Največje število aplikacij, upravičenih udeležencev in/ali odjemalskih naprav, ki lahko dostopajo do storitev v oblaku IBM Security Trusteer Fraud Protection, je navedeno v transakcijskem dokumentu. Naročnik mora zagotoviti, da njegovo število aplikacij, upravičenih udeležencev in/ali odjemalskih naprav ne preseže največjega dovoljenega števila, ki je navedeno v transakcijskem dokumentu.

IBM lahko preveri skladnost z največjim številom aplikacij, upravičenih udeležencev in/ali odjemalskih naprav.

13. Obdobje trajanja in možnosti podaljšanja

Obdobje trajanja storitev v oblaku se začne z dnem, ko IBM naročnika obvesti, da ima dostop do storitev v oblaku, navedenih v dokazilu o upravičenosti. V dokazilu o upravičenosti bo navedeno, ali se storitve v oblaku podaljšajo samodejno, se nadaljujejo na podlagi neprekinjene uporabe ali se končajo ob izteku naročniškega obdobja.

Na podlagi samodejnega podaljšanja se bo naročnina na storitve v oblaku samodejno podaljševala v okviru naročniškega obdobja, navedenega 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 storitev v oblaku neprestano na voljo iz meseca v mesec, dokler naročnik ne posreduje pisnega obvestila o odpovedi z 90-dnevnim odpovednim rokom. Po izteku takega 90-dnevnega obdobja bo storitev v oblaku na voljo še do konca koledarskega meseca.

14. Dodatna določila

14.1 Podporna programska oprema

Te storitve v oblaku vključujejo podporno programsko opremo, ki se sme uporabljati le v povezavi z naročnikovo uporabo storitev v oblaku in le v času trajanja storitev v oblaku.

14.2 Letno povišanje zneska naročnine za IBM Trusteer

IBM si pridržuje pravico do prilagajanja naročnine za storitve v oblaku. Prilagoditev naročnine se bo odrazila v navedenih cenah in za obdobje veljavne ponudbe. Dodatne prilagoditve naročnine, ki bodo uveljavljene največ enkrat na vsakih dvanajst (12) mesecev za odstotek, ki ga določi IBM in ne presega 3 %, lahko veljajo, če se obdobje trajanja storitev v oblaku podaljša s samodejnim podaljšanjem ali z neprekinjeno nadaljnjo uporabo. Te prilagoditve naročnine ne spreminjajo naročnikove upravičenosti do storitev v oblaku in ne vplivajo na metriko zaračunavanja, po kateri je bila storitev v oblaku pridobljena. IBM-ovi poslovni partnerji so neodvisni od IBM-a in enostransko določajo svoje cene in pogoje.