IBM Trusteer Fraud Protection

Tento Popis stanovuje podmínky služby Cloud Service, kterou IBM poskytuje Zákazníkovi. Zákazník znamená smluvní stranu a její oprávněné uživatele a příjemce služby Cloud Service. Příslušná Cenová nabídka a Dokument o oprávnění (Proof of Entitlement) jsou poskytnuty ve formě samostatných Transakčních dokumentů.

1. Cloud Service

Tento Popis služeb zahrnuje následující služby Cloud Service:

Služby Rapport Cloud:

- 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

Služby Pinpoint Cloud:

- 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

Služby Mobile Cloud:

- 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 Obchodní a maloobchodní cloudové služby

Služby IBM Trusteer Cloud Service jsou poskytovány k použití s konkrétními typy Aplikací. Aplikace je definována jako jeden z následujících typů: Maloobchodní nebo Obchodní. Pro Maloobchodní a Obchodní aplikace jsou k dispozici oddělené nabídky.

a. Maloobchodní aplikace je definována jako aplikace online bankovnictví, mobilní aplikace nebo aplikace e-commerce určená pro zákazníky služby. Zásady Zákazníka mohou klasifikovat určité malé podniky jako vhodné pro maloobchodní přístup.

b. Obchodní aplikace je definována jako aplikace online bankovnictví, mobilní aplikace nebo aplikace e-commerce určená pro podnikové, institucionální nebo ekvivalentní subjekty nebo jakákoli aplikace, která není kategorizována jako Maloobchodní.

1.1.1 Obchodní cloudové služby

- 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 Criminal Detection for Business
- IBM Trusteer Pinpoint Criminal Detection for Business Mobile
- 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 Maloobchodní cloudové služby

- 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 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

Pro každou z obchodních a maloobchodních služeb je za další poplatek k dispozici související podpora Premium, a to s výjimkou služeb IBM Trusteer Mobile SDK Cloud Service.

1.1.3 Další služby Cloud Service pro produkt IBM Trusteer Rapport

a. Další služby Cloud Service dostupné pro produkt 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. Další služby Cloud Service dostupné pro produkt 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

Pro každý obchodní nebo maloobchodní doplněk pro služby IBM Trusteer Rapport Cloud Service je s výjimkou doplňků IBM Trusteer Rapport Mandatory Service za další poplatek k dispozici související podpora Premium.

Registrace produktu IBM Trusteer Rapport for Business nebo IBM Trusteer Rapport for Retail je předpokladem pro další související služby Cloud Service uvedené v této části.

1.1.4 Další služby Cloud Service pro IBM Trusteer Pinpoint Malware Detection anebo IBM Trusteer Pinpoint Malware Detection II

a. Další služby Cloud Service pro IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition, IBM Trusteer Pinpoint Malware Detection for Business Standard Edition nebo pro IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business nebo 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. Další služby Cloud Service pro IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition nebo IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition nebo pro IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition nebo 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 poskytována pro konkrétní nabídky podle ustanovení tohoto dokumentu. Registrace produktů IBM Trusteer Pinpoint Malware Detection for Business nebo IBM Trusteer Pinpoint Malware Detection for Retail nebo IBM Trusteer Pinpoint Malware Detection II for Business nebo IBM Trusteer Pinpoint Malware Detection II for Retail je předpokladem pro další související služby Cloud Service uvedené v tomto oddílu.

1.1.5 Další služby Cloud Service pro IBM Trusteer Pinpoint Criminal Detection anebo IBM Trusteer Pinpoint Criminal Detection II

a. Další služby Cloud Service pro IBM Trusteer Pinpoint Criminal Detection for Business nebo IBM Trusteer Pinpoint Criminal Detection II:

- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business

b. Další služby Cloud Service pro IBM Trusteer Pinpoint Criminal Detection for Retail anebo IBM Trusteer Pinpoint Criminal Detection II for Retail:

- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Podpora Premium je poskytována pro konkrétní nabídky podle ustanovení tohoto dokumentu.

Registrace produktů IBM Trusteer Pinpoint Criminal Detection for Business nebo IBM Trusteer Pinpoint Criminal Detection for Retail nebo IBM Trusteer Pinpoint Criminal Detection II for Business nebo IBM Trusteer Pinpoint Criminal Detection II for Retail je předpokladem pro další související služby Cloud Service uvedené v tomto oddílu.

1.1.6 Další služby Cloud Service pro IBM Trusteer Pinpoint Detect Standard anebo IBM Trusteer Pinpoint Detect Premium anebo IBM Security Pinpoint Detect Standard with access management integration anebo IBM Security Detect Premium with access management integration

a. Další služby Cloud Service pro IBM Trusteer Detect Standard for Business anebo IBM Trusteer Pinpoint Detect Premium for Business anebo IBM Security Pinpoint Detect Standard with access

management integration for Business anebo 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. Další služby Cloud Service dostupné pro IBM Trusteer Detect Standard for Retail anebo IBM Trusteer Pinpoint Detect Premium for Retail anebo IBM Security Pinpoint Detect Standard with access management integration for Retail anebo 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

Registrace produktů IBM Trusteer Detect Standard nebo IBM Trusteer Pinpoint Detect Premium nebo IBM Security Pinpoint Detect Standard with access management integration nebo IBM Security Detect Premium with access management integration je předpokladem pro další související služby Cloud Service uvedené v tomto oddílu.

1.1.7 Další dodatečné služby Cloud Service

Jakékoli dodatečné registrace služeb Cloud Service pro základní registrace výše, které zde nejsou uvedeny, ať už aktuálně dostupné nebo ve vývoji, nejsou považovány za aktualizaci a musí být uděleny odděleně.

1.2 Definice

Vlastník účtu – označuje koncového uživatele Zákazníka, který si nainstaloval software s podporou klienta, uzavřel licenční smlouvu pro koncového uživatele ("EULA") a minimálně jednou se ověřil v Maloobchodní nebo Obchodní aplikaci, pro kterou si Zákazník zaregistroval pokrytí služeb IBM Cloud Service.

Klientský software majitele účtu – označuje software s podporou klienta IBM Trusteer Rapport nebo software s podporou klienta IBM Trusteer Mobile Browser či jakýkoli jiný software s podporou zákazníka, který je poskytován s některými službami Cloud Service k instalaci na zařízení koncového uživatele.

Úvodní stránka Trusteer Splash – označuje úvodní stránku, která je poskytována Zákazníkovi na základě dostupných šablon úvodních stránek.

Vstupní stránka – označuje stránku hostovanou IBM, která je poskytována Zákazníkovi s úvodní stránkou Zákazníka a Softwarem klienta vlastníka účtu ke stažení.

2. IBM Trusteer Rapport Cloud Services

2.1 IBM Trusteer Rapport for Retail nebo IBM Trusteer Rapport for Business ("Trusteer Rapport")

Trusteer Rapport poskytuje vrstvu ochrany proti phishingovým útokům a malwarovým útokům Man-in-the-Browser (MitB). S využitím sítě desítek milionů koncových bodů všude na světě IBM Trusteer Rapport shromažďuje informace o aktivních phishingových a malwarových útocích cílených na organizace po celém světě. IBM Trusteer Rapport aplikuje behaviorální algoritmy s cílem blokovat phishingové úroky a zabránit instalaci a běhům filtrace malwaru MitB.

Tyto služby Cloud Service mají metriku poplatku Vybraný účastník. Obchodní nabídka je prodávána v balíčcích po 10 Vybraných účastnících. Maloobchodní nabídka je prodávána v balíčcích po 100 Vybraných účastnících.

Tato nabídka služby Cloud Service zahrnuje:

a. Trusteer Management Application ("TMA"):

Aplikace TMA je zpřístupněna v prostředí IBM Trusteer hostovaném v cloudu, prostřednictvím kterého Zákazník (a neomezený počet jeho oprávněných pracovníků) může: (i) zobrazovat a stahovat určité úkoly vytváření sestav s daty událostí a posouzení rizik, (ii) zobrazovat konfiguraci aktivačního softwaru klienta licencovaného Vybraným účastníkům Zákazníka na základě licenční smlouvy s koncovým uživatelem ("EULA") , a to bez poplatku, a zpřístupnit takový software, který je také označován jako sada softwaru Trusteer Rapport ("Software klienta vlastníka účtu"), ke stažení do stolních počítačů a zařízení Vybraného účastníka (PC/MAC). Zákazník může nabízet Software klienta vlastníka účtu pouze pomocí Úvodní stránky Trusteer Splash nebo rozhraní API Rapport a

Zákazník tento software nesmí používat pro své interní obchodní operace nebo k použití svými zaměstnanci (mimo osobního použití zaměstnanců).

b. Webový skript:

Pro přístup na webovou stránku pro účely přístupu nebo použití služby Cloud Service.

c. Data události:

Zákazník (a neomezený počet jeho oprávněných pracovníků) může TMA používat k přijímání dat událostí generovaných ze Softwaru klienta vlastníka účtu v důsledku online interakcí Vlastníků účtu s jejich Obchodní nebo Maloobchodní aplikací, pro kterou si Zákazník zaregistroval pokrytí služeb IBM Cloud Service. Data události budou přijata ze Softwaru klienta vlastníka účtu Vybraných účastníků běžícího na jejich zařízeních, kteří uzavřeli smlouvu EULA a minimálně jednou provedli ověření v Obchodní nebo Maloobchodní aplikaci Zákazníka; konfigurace Zákazníka musí zahrnovat shromažďování ID uživatele.

d. Úvodní stránka Trusteer Splash:

Marketingová platforma Úvodní stránky Trusteer Splash identifikuje a prodává Software klienta vlastníka účtu Vybraným účastníkům přistupujícím k Obchodním anebo Maloobchodním aplikacím Zákazníka, pro které si Zákazník zaregistroval pokrytí služeb IBM Cloud Service. Zákazník si může vybrat z dostupných šablon Úvodní stránky. Na základě samostatné smlouvy nebo rozsahu prací lze sjednat přizpůsobenou úvodní stránku.

Zákazník může souhlasit s poskytnutím ochranných známek, log nebo ikon k použití v souvislosti s TMA a pouze pro využití Úvodní stránky Trusteer Splash a zobrazení v Softwaru klienta vlastníka účtu nebo na vstupních stránkách hostovaných IBM a na webu IBM Trusteer. Každé použití poskytnutých ochranných známek, log nebo ikon bude v souladu s přiměřenými zásadami IBM týkajícími se inzerce a využití ochranných známek.

Zákazník si musí zaregistrovat službu IBM Trusteer Rapport Mandatory Service Cloud Service, pokud si přeje využít jakýkoli typ povinného nasazení Softwaru klienta vlastníka účtu.

Povinné nasazení Softwaru klienta vlastníka účtu zahrnuje mimo jiné jakýkoli typ povinné implementace za využití libovolného mechanizmu nebo libovolného prostředku, který přímo nebo nepřímo nutí Vybraného účastníka ke stažení Softwaru klienta vlastníka účtu, nebo libovolné metody, nástroje, postupu, smlouvy či mechanizmu, které nevytvořila nebo neschválila IBM a které byly vytvořeny k obejití licenčních požadavků tohoto povinného nasazení Softwaru klienta vlastníka účtu.

2.2 IBM Trusteer Rapport II for Retail anebo IBM Trusteer Rapport II for Business ("Trusteer Rapport II")

Trusteer Rapport II Cloud Service je nová forma produktu IBM Trusteer Rapport, která pomáhá standardizovat poplatky týkající se ochrany více Aplikací a nahrazuje jednorázové poplatky při přidávání Aplikací.

Trusteer Rapport II poskytuje vrstvu ochrany proti phishingovým útokům a malwarovým útokům Man-in-the-Browser (MitB). S využitím sítě desítek milionů koncových bodů všude na světě IBM Trusteer Rapport shromažďuje informace o aktivních phishingových a malwarových útocích cílených na organizace po celém světě. IBM Trusteer Rapport aplikuje behaviorální algoritmy s cílem blokovat phishingové úroky a zabránit instalaci a běhům filtrace malwaru MitB.

Tato služba Cloud Service má metriku poplatku Vybraný účastník. Obchodní nabídka je prodávána v balíčcích po 10 Vybraných účastnících. Maloobchodní nabídka je prodávána v balíčcích po 100 Vybraných účastnících.

Tato nabídka služby Cloud Service zahrnuje:

a. Trusteer Management Application ("TMA"):

Aplikace TMA je zpřístupněna v prostředí IBM Trusteer hostovaném v cloudu, prostřednictvím kterého Zákazník (a neomezený počet jeho oprávněných pracovníků) může: (i) zobrazovat a stahovat určité úkoly vytváření sestav s daty událostí a posouzení rizik, (ii) zobrazovat konfiguraci aktivačního softwaru klienta licencovaného Vybraným účastníkům Zákazníka na základě licenční smlouvy s koncovým uživatelem ("EULA") , a to bez poplatku, a zpřístupnit takový software, který je také označován jako sada softwaru Trusteer Rapport ("Software klienta vlastníka účtu"), ke stažení do stolních počítačů a zařízení Vybraného účastníka (PC/MAC). Zákazník může nabízet Software klienta vlastníka účtu pouze pomocí Úvodní stránky Trusteer Splash nebo rozhraní API Rapport a

Zákazník tento software nesmí používat pro své interní obchodní operace nebo k použití svými zaměstnanci (mimo osobního použití zaměstnanců).

b. Webový skript:

Pro přístup na webovou stránku pro účely přístupu nebo použití služby Cloud Service.

c. Data události:

Zákazník (a neomezený počet jeho oprávněných pracovníků) může TMA používat k přijímání dat událostí generovaných ze Softwaru klienta vlastníka účtu v důsledku online interakcí Vlastníků účtu s jejich Obchodní nebo Maloobchodní aplikací, pro kterou si Zákazník zaregistroval pokrytí služeb IBM Cloud Service. Data události budou přijata ze Softwaru klienta vlastníka účtu Vybraných účastníků běžícího na jejich zařízeních, kteří uzavřeli smlouvu EULA a minimálně jednou provedli ověření v Obchodní nebo Maloobchodní aplikaci Zákazníka; konfigurace Zákazníka musí zahrnovat shromažďování ID uživatele.

d. Úvodní stránka Trusteer Splash:

Marketingová platforma Úvodní stránky Trusteer Splash identifikuje a prodává Software klienta vlastníka účtu Vybraným účastníkům přistupujícím k Obchodním anebo Maloobchodním aplikacím Zákazníka, pro které si Zákazník zaregistroval pokrytí služeb IBM Cloud Service. Zákazník si může vybrat z dostupných šablon Úvodní stránky. Na základě samostatné smlouvy nebo rozsahu prací lze sjednat přizpůsobenou úvodní stránku.

Zákazník může souhlasit s poskytnutím ochranných známek, log nebo ikon k použití v souvislosti s TMA a pouze pro využití Úvodní stránky Trusteer Splash a zobrazení v Softwaru klienta vlastníka účtu nebo na vstupních stránkách hostovaných IBM a na webu IBM Trusteer. Každé použití poskytnutých ochranných známek, log nebo ikon bude v souladu s přiměřenými zásadami IBM týkajícími se inzerce a využití ochranných známek.

Zákazník si musí zaregistrovat službu IBM Trusteer Rapport Mandatory Service Cloud Service, pokud si přeje využít jakýkoli typ povinného nasazení Softwaru klienta vlastníka účtu.

Povinné nasazení Softwaru klienta vlastníka účtu zahrnuje mimo jiné jakýkoli typ povinné implementace za využití libovolného mechanizmu nebo libovolného prostředku, který přímo nebo nepřímo nutí Vybraného účastníka ke stažení Softwaru klienta vlastníka účtu, nebo libovolné metody, nástroje, postupu, smlouvy či mechanizmu, které nevytvořila nebo neschválila IBM a které byly vytvořeny k obejití licenčních požadavků tohoto povinného nasazení Softwaru klienta vlastníka účtu.

Trusteer Rapport II for Business anebo Trusteer Rapport II for Retail zahrnují ochranu pro jednu Aplikaci. Pro každou další Aplikaci by Zákazník měl získat oprávnění pro další aplikace IBM Trusteer Rapport Additional Applications.

2.3 Volitelné další služby Cloud Service pro IBM Trusteer Rapport for Business anebo IBM Trusteer Rapport for Retail anebo IBM Trusteer Rapport II for Business anebo IBM Trusteer Rapport II for Retail

Registrace služeb IBM Trusteer Rapport Cloud Service nebo IBM Trusteer Rapport II Cloud Service je předpokladem registrace jakékoli z následujících dodatečných služeb Cloud Service. Pokud jsou služba Cloud Service označeny jako "for Business", musí být získané dodatečné služby Cloud Service také označeny jako "for Business". Pokud jsou služba Cloud Service označeny jako "for Retail", musí být získané dodatečné služby Cloud Service také označeny jako "for Retail". Zákazník bude přijímat data události od Vybraných účastníků používajících Software klienta vlastníka účtu, kteří uzavřeli smlouvu EULA pro koncové uživatele a minimálně jednou provedli ověření v Obchodní anebo Maloobchodní aplikaci Zákazníka; konfigurace Zákazníka musí zahrnovat shromažďování ID uživatele.

2.3.1 IBM Trusteer Rapport Fraud Feeds for Business nebo IBM Trusteer Rapport Fraud Feeds for Retail

Po registraci této doplňkové služby Cloud Service může Zákazník (a neomezený počet jeho oprávněných pracovníků) používat aplikaci TMA k zobrazování, registraci a konfiguraci doručení kanálů hrozeb generovaných službou Trusteer Rapport Cloud Service. Kanály lze odesílat prostřednictvím e-mailu na určené e-mailové adresy nebo prostřednictvím SFTP jako textové soubory.

2.3.2 IBM Trusteer Rapport Phishing Protection for Business nebo IBM Trusteer Rapport Phishing Protection for Retail

Zákazník (a neomezený počet jeho oprávněných pracovníků) může TMA používat k přijímání oznámení o datech událostí souvisejících s poskytnutím přihlašovacích údajů Vlastníka účtu na webu s podezřením

na phishing nebo na potenciálně podvodném webu. Legitimní online aplikace (adresy URL) mohou být chybně označeny jako phishingové weby a službu Cloud Service může Vlastníky účtu upozornit, že legitimní web je phishingový web. V takovém případě musí Zákazník na tuto chybu upozornit IBM, která ji odstraní. Toto bude výhradní náprava Zákazníka v případě takové chyby.

2.3.3 IBM Trusteer Rapport Mandatory Service for Business nebo IBM Trusteer Rapport Mandatory Service for Retail

Zákazník smí používat instanci marketingové platformy Úvodní stránky Trusteer Splash k povolení stahování Softwaru klienta vlastníka účtu Vybraným účastníkům přistupujícím k Obchodním anebo Maloobchodním aplikacím Zákazníka, pro které si Zákazník zaregistroval pokrytí služeb Cloud Service.

IBM Trusteer Rapport Premium Support for Business je předpokladem pro IBM Security Rapport Mandatory Service for Business.

IBM Trusteer Rapport Premium Support for Retail je předpokladem pro IBM Security Rapport Mandatory Service for Retail.

Zákazník smí implementovat další funkce IBM Trusteer Rapport Mandatory Service, pouze pokud byly objednány a konfigurovány pro použití s Obchodními nebo Maloobchodními aplikacemi Zákazníka, pro které si Zákazník zaregistroval pokrytí služeb Cloud Service.

2.3.4 IBM Trusteer Rapport Large Redeployment anebo IBM Trusteer Rapport Small Redeployment

Zákazníci, kteří během období poskytování služby znovu nasadí své aplikace pro online bankovnictví, a vyžadují proto změny svého nasazení služby IBM Trusteer Rapport nebo IBM Trusteer Rapport II, by si měli zakoupit službu IBM Trusteer Rapport Redeployment Cloud Service.

Nové nasazení může být vyžadováno z důvodu změny domény nebo hostující adresy URL Aplikace Zákazníkem, použití změn konfigurace úvodní stránky nebo přechodu na novou platformu online bankovnictví.

Během přechodového období nového nasazení v délce šesti měsíců má Zákazník nárok na další Aplikace (vždy po jedné aplikaci), které běží na již registrovaných Aplikacích.

IBM Trusteer Rapport Large Redeployment se vztahuje na prostředí s maximálně 20 000 uživateli a IBM Trusteer Rapport Small Redeployment se vztahuje na prostředí, kde je počet uživatelů menší nebo roven 20 000.

2.3.5 IBM Trusteer Rapport Additional Applications for Business anebo IBM Trusteer Rapport Additional Applications for Retail

IBM Trusteer Rapport II for Business vyžaduje nasazení na další Obchodní aplikaci nad rámec první Aplikace oprávnění k IBM Trusteer Rapport Additional Applications for Business Cloud Service. IBM Trusteer Rapport II for Retail vyžaduje nasazení na další Maloobchodní aplikaci nad rámec první Aplikace oprávnění k IBM Trusteer Rapport Additional Applications for Retail Cloud Service.

3. Služby IBM Trusteer Pinpoint Cloud Service

IBM Trusteer Pinpoint je cloudová služba, která je určena k zajištění další vrstvy ochrany a jejím cílem je zjistit a zmírnit útoky malwaru a phishingu a snahu o převzetí účtu. Trusteer Pinpoint lze integrovat do Obchodních anebo Maloobchodních aplikací Zákazníka, pro které si Zákazník zaregistroval pokrytí služeb Cloud Service a procesů prevence podvodu.

Tato služba Cloud Service zahrnuje:

a. TMA:

   Aplikace TMA je zpřístupněna v prostředí IBM Trusteer hostovaném v cloudu, prostřednictvím kterého Zákazník (a neomezený počet jeho oprávněných pracovníků) může: (i) zobrazovat a stahovat určité úkoly vytváření sestav s daty událostí a posouzení rizik, (ii) zobrazovat, registrovat a konfigurovat doručení kanálů hrozeb generovaných z nabídek Pintpoint.

b. Webový skript nebo rozhraní API:

   Pro implementaci na webu pro účely přístupu nebo použití služby Cloud Service.

3.1 IBM Trusteer Pinpoint Malware Detection a IBM Trusteer Pinpoint Criminal Detection

V případě zjištění malwaru ve službách IBM Trusteer Pinpoint Malware Detection Cloud Service nebo zjištění převzetí účtu IBM Trusteer Pinpoint Malware Detection II Cloud Service ve službách IBM Trusteer Pinpoint Criminal Detection Cloud Service nebo IBM Trusteer Pinpoint Criminal Detection II Cloud

Services musí Zákazník dodržovat příručku s osvědčenými postupy Pinpoint Best Practices Guide. Služby IBM Trusteer Pinpoint Malware Detection Cloud Service nebo IBM Trusteer Pinpoint Malware Detection II Cloud Service nebo IBM Trusteer Pinpoint Criminal Detection Cloud Service nebo IBM Trusteer Pinpoint Criminal Detection II Cloud Service nepoužívejte žádným způsobem, který ovlivní prostředí Vybraných účastníků ihned po zjištění malwaru nebo převzetí účtu tak, aby ostatní uživatelé mohli propojit akce Zákazníka s použitím služeb IBM Trusteer Pinpoint Cloud Service (např. oznámení, zprávy, blokování zařízení nebo blokování přístupu k Obchodní anebo Maloobchodní aplikaci ihned po zjištění malwaru nebo převzetí účtu).

3.2 IBM Trusteer Pinpoint Criminal Detection for Business nebo IBM Trusteer Pinpoint Criminal Detection for Retail

Detekce podezřelého převzetí účtu bez klienta ze strany prohlížečů připojujících se k Obchodní nebo Maloobchodní aplikaci za použití ID zařízení, detekce phishingu a detekce odcizení pověření iniciované malwarem. Služby IBM Trusteer Pinpoint Criminal Detection Cloud Service poskytují další vrstvu ochrany a jejich cílem je zjistit pokusy o převzetí účtu a poskytnout skóre posouzení rizika prohlížečů nebo mobilních zařízení (prostřednictvím nativního prohlížeče nebo mobilní aplikace Zákazníka) přistupujících k Obchodní nebo Maloobchodní aplikaci přímo pro Zákazníka.

a. Data události:

   Zákazník (a neomezený počet jeho oprávněných zaměstnanců) může TMA používat k přijímání dat událostí generovaných v důsledku online interakcí Vybraných účastníků s Maloobchodními anebo Obchodními aplikacemi Zákazníka, pro které si Zákazník zaregistroval pokrytí Cloud Service, nebo Zákazník může přijímat data události prostřednictvím režimu doručování backendového rozhraní API.

3.3 IBM Trusteer Pinpoint Criminal Detection II for Business anebo IBM Trusteer Pinpoint Criminal Detection II for Retail

IBM Security Pinpoint Criminal Detection II je nová forma produktu IBM Trusteer Pinpoint Criminal Detection, která pomáhá standardizovat poplatky týkající se ochrany více Aplikací a nahrazuje jednorázové poplatky při přidávání Aplikací.

Detekce podezřelého převzetí účtu bez klienta ze strany prohlížečů připojujících se k Obchodní nebo Maloobchodní aplikaci za použití ID zařízení, detekce phishingu a detekce odcizení pověření iniciované malwarem. Služby IBM Trusteer Pinpoint Criminal Detection II Cloud Service poskytují další vrstvu ochrany a jejich cílem je zjistit pokusy o převzetí účtu a poskytnout skóre posouzení rizika prohlížečů nebo mobilních zařízení (prostřednictvím nativního prohlížeče nebo mobilní aplikace Zákazníka) přistupujících k Obchodní nebo Maloobchodní aplikaci přímo pro Zákazníka.

a. Data události:

   Zákazník (a neomezený počet jeho oprávněných zaměstnanců) může TMA používat k přijímání dat událostí generovaných v důsledku online interakcí Vybraných účastníků s Maloobchodními anebo Obchodními aplikacemi Zákazníka, pro které si Zákazník zaregistroval pokrytí Cloud Service, nebo Zákazník může přijímat data události prostřednictvím režimu doručování backendového rozhraní API.

   Tato služba Cloud Service zahrnuje ochranu pro jednu Aplikaci. Pro každou další Aplikaci by Zákazník měl získat oprávnění pro další Aplikace IBM Trusteer Pinpoint Criminal Detection.

3.4 IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition nebo IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition nebo IBM Trusteer Pinpoint Malware Detection for Business Standard Edition nebo IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition

Detekce připojení prohlížečů infikovaných finančním malwarem bez klienta během připojování k Obchodní anebo Maloobchodní aplikaci. Služby IBM Trusteer Pinpoint Malware Detection Cloud Service poskytují další vrstvu ochrany a jejich cílem je umožnit organizacím zaměřit se na procesy prevence podvodů na základě rizika malwaru tím, že Zákazníkovi zajistí posouzení a výstrahy na přítomnost finančního malwaru MitB.

a. Data události:

Zákazník (a neomezený počet jeho oprávněných zaměstnanců) může TMA používat k přijímání dat událostí generovaných v důsledku online interakcí Vybraných účastníků s Maloobchodními anebo Obchodními aplikacemi Zákazníka.

b. Advanced Edition:

Edice Advanced Edition for Business nebo for Retail nabízí další úroveň detekce a ochrany, která je přizpůsobena struktuře a toku Obchodních a Maloobchodních aplikací Zákazníka a lze ji upravit podle konkrétního prostředí hrozeb zacílených na Zákazníka. Produkty lze začlenit na různých pracovištích do Obchodních anebo Maloobchodních aplikací Zákazníka.

Advanced Edition je Zákazníkovi nabízena s minimálním množstvím minimálně 100 000 Maloobchodních oprávněných účastníků nebo 10 000 Obchodních vybraných účastníků, což je 1000 balíčků 100 Vybraných účastníků pro Maloobchodní aplikace nebo 1000 balíčků 10 Vybraných účastníků pro Obchodní aplikace.

c. Standard Edition:

Standard Edition for Business nebo for Retail je řešení s rychlým nasazením, které poskytuje základní funkce této služby Cloud Service popsané v tomto dokumentu.

3.5 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business anebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail anebo IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business anebo IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Security Pinpoint Malware Detection II je nová forma produktu IBM Trusteer Pinpoint Malware Detection, která pomáhá standardizovat poplatky týkající se ochrany více Aplikací a nahrazuje jednorázové poplatky při přidávání Aplikací.

Detekce připojení prohlížečů infikovaných finančním malwarem bez klienta během připojování k Obchodní anebo Maloobchodní aplikaci. Služby IBM Trusteer Pinpoint Malware Detection Cloud Service poskytují další vrstvu ochrany a jejich cílem je umožnit organizacím zaměřit se na procesy prevence podvodů na základě rizika malwaru tím, že Zákazníkovi zajistí posouzení a výstrahy na přítomnost finančního malwaru MitB.

a. Data události:

Zákazník (a neomezený počet jeho oprávněných zaměstnanců) může TMA používat k přijímání dat událostí generovaných v důsledku online interakcí Vybraných účastníků s Maloobchodními anebo Obchodními aplikacemi Zákazníka.

b. Advanced Edition:

Edice Advanced Edition for Business nebo for Retail nabízí další úroveň detekce a ochrany, která je přizpůsobena struktuře a toku Obchodních a Maloobchodních aplikací Zákazníka a lze ji upravit podle konkrétního prostředí hrozeb zacílených na Zákazníka. Produkty lze začlenit na různých pracovištích do Obchodních anebo Maloobchodních aplikací Zákazníka.

Advanced Edition je Zákazníkovi nabízena s minimálním množstvím minimálně 100 000 Maloobchodních oprávněných účastníků nebo 10 000 Obchodních vybraných účastníků, což je 1000 balíčků 100 Vybraných účastníků pro Maloobchodní aplikace nebo 1000 balíčků 10 Vybraných účastníků pro Obchodní aplikace.

c. Standard Edition:

Standard Edition for Business nebo for Retail je řešení s rychlým nasazením, které poskytuje základní funkce této služby Cloud Service popsané v tomto dokumentu.

Tato služba Cloud Service zahrnuje ochranu pro jednu Aplikaci. Pro každou další Aplikaci musí Zákazník získat oprávnění pro IBM Trusteer Pinpoint Malware Detection Additional Applications.

3.6 Volitelné další služby Cloud Service pro IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition anebo IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition anebo IBM Trusteer Pinpoint Malware Detection for Business Standard Edition anebo IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition anebo IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail anebo IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business anebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail anebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business

- Předpokladem pro službu IBM Trusteer Rapport Remediation for Retail Cloud Service je IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail nebo IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Předpokladem pro službu IBM Trusteer Rapport Remediation for Business Cloud Service je IBM Trusteer Pinpoint Malware Detection Standard Edition for Business nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business nebo IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.
- Předpokladem pro službu IBM Trusteer Pinpoint Carbon Copy for Retail je IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail nebo IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Předpokladem pro službu IBM Trusteer Pinpoint Carbon Copy for Business je IBM Trusteer Pinpoint Malware Detection Standard Edition for Business nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business nebo IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.

3.6.1 IBM Trusteer Pinpoint Carbon Copy for Business nebo IBM Trusteer Pinpoint Carbon Copy for Retail

Nabídky IBM Trusteer Pinpoint Carbon Copy určené k zajištění další vrstvy ochrany a monitorovacích služeb, které pomohou identifikovat případy, kdy byla pověření Vybraných účastníků kompromitována útoky phishing na Maloobchodní nebo Obchodní aplikace Zákazníka, pro které Zákazník získal registraci pokrytí nabídek Cloud Service.

3.6.2 IBM Trusteer Rapport Remediation for Retail anebo IBM Trusteer Rapport Remediation for Business

Cílem produktů IBM Trusteer Rapport Remediation for Retail a IBM Trusteer Rapport Remediation for Business je prošetřit, napravit, zablokovat a odebrat napadení malwarem typu man-in-the-browser (MitB) z infikovaných zařízení (PC/MAC) Vybraných účastníků Zákazníka, kteří přistupují k Aplikaci Zákazníka na ad hoc bázi, kde napadení malwarem MitB bylo zjištěno daty událostí IBM Security Trusteer Pinpoint Malware Detection. Zákazník musí mít ve své Aplikaci spuštěnu aktuální registraci produktu IBM Trusteer Pinpoint Malware Detection nebo IBM Trusteer Pinpoint Malware Detection II. Zákazník smí tuto nabídku Cloud Service použít pouze ve spojení s Vybranými účastníky, kteří přistupují k Aplikaci Zákazníka, a výhradně jako nástroj, jehož cílem je prošetřit a opravit konkrétní infikované zařízení (PC/MAC) na ad hoc bázi. IBM Trusteer Rapport Remediation musí běžet na dotčených zařízeních Vybraného účastníka (PC/MAC) a tento dotčený Vybraný účastník musí uzavřít smlouvu EULA a minimálně jednou provést své ověření v Aplikaci (Aplikacích) Zákazníka a konfigurace Zákazníka musí zahrnovat shromažďování ID uživatele. Pro vyloučení pochybností se uvádí, že tato nabídka Cloud Service nezahrnuje právo na používání Úvodní stránky Trusteer Splash nebo k jiné podpoře klientského softwaru vlastníka účtu určené pro obecné Vybrané účastníky Zákazníka.

3.6.3 IBM Trusteer Pinpoint Malware Detection Redeployment

Zákazníci, kteří během období poskytování služby znovu nasadí své aplikace pro online bankovnictví, a vyžadují proto změny svého nasazení služby IBM Trusteer Pinpoint Malware Detection anebo IBM Trusteer Pinpoint Malware Detection II, by si měli zakoupit službu IBM Trusteer Pinpoint Malware Detection Redeployment.

Nové nasazení může být vyžadováno z důvodu změny domény nebo hostující adresy URL Aplikace Zákazníkem, převodu online Aplikace na novou technologii, přechodu na novou platformu online bankovnictví nebo přidání nového postupu přihlašování do stávající Aplikace.

Během přechodového období nového nasazení v délce šesti měsíců má Zákazník nárok na další Aplikace (vždy po jedné aplikaci), které běží na již registrovaných Aplikacích.

3.6.4 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail anebo IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business vyžaduje nasazení na jakékoli další Obchodní aplikaci nad rámec první Aplikace oprávnění pro IBM Trusteer Pinpoint Malware Detection Additional Applications for Business. IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail nebo IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail vyžaduje nasazení na jakékoli další Maloobchodní aplikaci nad rámec první Aplikace oprávnění pro IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail.

3.7 Volitelné další služby Cloud Service pro IBM Trusteer Pinpoint Criminal Detection for Business anebo IBM Trusteer Pinpoint Criminal Detection for Retail anebo pro IBM Trusteer Pinpoint Criminal Detection II for Business anebo IBM Trusteer Pinpoint Criminal Detection II for Retail

3.7.1 IBM Trusteer Pinpoint Criminal Detection Redeployment

Zákazníci, kteří během období poskytování služby znovu nasadí své aplikace pro online bankovnictví, a vyžadují proto změny svého nasazení služby IBM Trusteer Pinpoint Criminal Detection Cloud Service, by si měli zakoupit službu IBM Trusteer Pinpoint Criminal Detection Redeployment.

Nové nasazení může být vyžadováno z důvodu změny domény nebo hostující adresy URL Aplikace Zákazníkem, převodu online Aplikace na novou technologii, přechodu na novou platformu online bankovnictví nebo přidání nového postupu přihlašování do stávající Aplikace.

Během přechodového období nového nasazení v délce šesti měsíců má Zákazník nárok na další Aplikace (vždy po jedné aplikaci), které běží na již registrovaných Aplikacích.

3.7.2 IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business anebo IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

IBM Trusteer Pinpoint Criminal Detection II for Business vyžaduje nasazení na jakékoli další Obchodní aplikaci nad rámec první Aplikace oprávnění pro IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business. IBM Trusteer Pinpoint Criminal Detection II for Retail vyžaduje nasazení na jakékoli další Maloobchodní aplikaci nad rámec první Aplikace oprávnění pro IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail.

4. IBM Trusteer Fraud Protection Suite

IBM Trusteer Fraud Protection Suite ("Sada") je kolekce cloudových služeb, která poskytuje vrstvu ochrany proti podvodům a lze ji integrovat s dalšími produkty IBM za účelem poskytnutí řešení pro správu životního cyklu. Sada zahrnuje následující cloudové služby:

- IBM Trusteer Pinpoint Detect, jejímž cílem je detekovat a zmírňovat útoky malwaru, phishingové útoky a útoky zacílené na převzetí účtu. Službu Trusteer Pinpoint Detect lze integrovat do Obchodních anebo Maloobchodních aplikací Zákazníka, pro které si Zákazník sjednal registraci pokrytí služby Cloud Service, a do procesů prevence podvodů.
- IBM Trusteer Rapport for Mitigation, jejímž cílem je obnovit a chránit infikované koncové body.

Tyto služby Cloud Service zahrnují:

a. TMA:

   Aplikace TMA je zpřístupněna v prostředí IBM Trusteer hostovaném v cloudu, prostřednictvím kterého Zákazník (a neomezený počet jeho oprávněných pracovníků) může: (i) přijímat úkoly vytváření sestav s daty událostí a posouzení rizik, (ii) zobrazovat, konfigurovat a nastavovat zásady zabezpečení a zásady související s vytvářením sestav s daty událostí.

b. Data události:

   Zákazník (a neomezený počet jeho oprávněných zaměstnanců) může TMA používat k přijímání dat událostí generovaných v důsledku online interakcí Vybraných účastníků s Maloobchodními anebo

Obchodními aplikacemi Zákazníka, pro které si Zákazník zaregistroval pokrytí Cloud Service, nebo Zákazník může přijímat data události prostřednictvím režimu doručování backendového rozhraní API.

c. Webový skript nebo rozhraní API:

Pro implementaci na webu pro účely přístupu nebo použití služby Cloud Service.

Osvědčené postupy pro produkt Pinpoint

V případě detekce malwaru nebo převzetí účtu musí Zákazník postupovat podle příručky Pinpoint Best Practices Guide. Služby IBM Trusteer Pinpoint Detect Cloud Service nepoužívejte žádným způsobem, který by ovlivnil zkušenost Vybraných účastníků ihned po detekci malwaru nebo převzetí účtu, například by umožnil ostatním propojit činnost Zákazníka s použitím nabídek IBM Trusteer Pinpoint Detect (např. oznámení, zprávy, blokování zařízení nebo blokování přístupu k Obchodní anebo Maloobchodní aplikaci ihned po detekci malwaru nebo převzetí účtu).

4.1 IBM Trusteer Pinpoint Detect Standard for Business anebo IBM Trusteer Pinpoint Detect Standard for Retail

Tato služba Cloud Service kombinuje služby Cloud Service IBM Trusteer Pinpoint Criminal Detection a IBM Trusteer Pinpoint Malware Detection a nabízí jedno jednotné řešení.

Toto řešení pomáhá s detekcí malwaru anebo podezřelé činnosti prohlížečů připojených k Obchodní nebo Maloobchodní aplikaci zaměřenou na převzetí účtu bez klienta, s použitím ID zařízení, detekce phishingu a detekce odcizení pověření řízeného malwarem. Nabídky IBM Trusteer Pinpoint poskytují další vrstvu ochrany. Jejich cílem je zjistit pokusy o převzetí účtu a poskytnout skóre posouzení rizika prohlížečů nebo mobilních zařízení (prostřednictvím nativního prohlížeče nebo mobilní aplikace Zákazníka) přistupujících k Obchodní nebo Maloobchodní aplikaci přímo Zákazníkovi.

Součástí této služby Cloud Service je standardní podpora (definována v části Technická podpora níže). Pro podporu Premium si Zákazník musí zakoupit produkt Detect Premium.

Tato služba Cloud Service zahrnuje ochranu pro jednu Aplikaci. Pro každou další Aplikaci by Zákazník měl získat oprávnění pro další aplikace IBM Trusteer Pinpoint Detect Standard.

4.2 IBM Trusteer Pinpoint Detect Premium for Business anebo IBM Trusteer Pinpoint Detect Premium for Retail

Tato služba Cloud Service kombinuje produkty IBM Trusteer Pinpoint Criminal Detection a IBM Trusteer Pinpoint Malware Detection a nabízí jedno jednotné řešení se snadnou integrací a rozšířenými funkcemi a službami, včetně: rozšířených služeb nasazení a nastavení, přizpůsobených zásad zabezpečení, služeb šetření atd.

Tato služba Cloud Service zahrnuje ochranu pro jednu Aplikaci. Pro každou další Aplikaci by Zákazník měl získat oprávnění pro další aplikace IBM Trusteer Pinpoint Detect Premium.

Součástí této služby Cloud Service je podpora Premium.

4.3 IBM Trusteer Pinpoint Detect Standard with access management integration for Business anebo IBM Trusteer Pinpoint Detect Standard with access management integration for Retail

Služba IBM Trusteer Pinpoint Detect Standard with access management integration Cloud Service zahrnuje funkce služby IBM Security Pinpoint Detect Standard uvedené v oddíle 4.1 výše.

IBM Trusteer Pinpoint Detect Standard with access management integration se používá při zakoupení se systémy řízení přístupu, například IBM Security Access Management ("ISAM"). V případě zakoupení se službou ISAM je nutné aktivovat obě nabídky. Tato nabídka zahrnuje volbu integrace se systémem řízení přístupu. Pro systém řízení přístupu však nezahrnuje oprávnění.

Tato nabídka zahrnuje ochranu pro jednu Aplikaci. Pro každou další Aplikaci by Zákazník měl získat oprávnění pro další aplikace IBM Trusteer Pinpoint Detect Standard.

Součástí této služby Cloud Service je standardní podpora (definována v části Technická podpora). IBM Trusteer Pinpoint Detect Premium with access management integration for Business anebo IBM Trusteer Pinpoint Detect Premium with access management integration for Retail

Služba IBM Trusteer Pinpoint Detect Premium with access management integration Cloud Service zahrnuje funkce služby IBM Security Pinpoint Detect Premium popsané v oddílu 4.2 výše a volbu integrace se systémem řízení přístupu.

IBM Trusteer Pinpoint Detect Premium with access management integration se používá při zakoupení se systémy řízení přístupu, například IBM Security Access Management ("ISAM"). V případě zakoupení se službou ISAM je nutné aktivovat obě nabídky. Tato služba Cloud Service zahrnuje volbu integrace se systémem řízení přístupu. Pro systém řízení přístupu však nezahrnuje oprávnění.

Tato služba Cloud Service zahrnuje ochranu pro jednu Aplikaci. Pro každou další Aplikaci by Zákazník měl získat oprávnění pro další aplikace IBM Trusteer Pinpoint Detect Premium.

Podpora Premium je součástí této nabídky.

4.4 Volitelné služby pro IBM Trusteer Pinpoint Detect Standard anebo IBM Trusteer Pinpoint Detect Premium

Pro služby Cloud Service uvedené v tomto oddíle platí prerekvizita oprávnění pro IBM Trusteer Pinpoint Detect Premium for Retail nebo IBM Trusteer Pinpoint Detect Standard for Retail.

4.5 IBM Trusteer Rapport for Mitigation for Retail anebo IBM Trusteer Rapport for Mitigation for Business

Cílem služby IBM Trusteer Rapport for Mitigation je prošetřit, napravit, zablokovat a odstranit infekce malwarem z napadených zařízení (PC/MAC) Vybraných účastníků Zákazníka, kteří přistupují k Maloobchodní aplikaci Zákazníka na ad hoc bázi v případech, kdy data událostí IBM Trusteer Pinpoint Detect Premium nebo IBM Trusteer Pinpoint Detect Standard zjistila napadení malwarem. Zákazník musí mít ve své Maloobchodní aplikaci spuštěnu aktuální registraci produktu IBM Trusteer Pinpoint Detect Premium nebo IBM Trusteer Pinpoint Detect Standard. Zákazník smí tuto službu Cloud Service použít pouze ve spojení s Vybranými účastníky, kteří přistupují k Maloobchodní aplikaci Zákazníka, a výhradně jako nástroj, jehož cílem je prošetřit a opravit konkrétní infikované zařízení (PC/MAC) na ad-hoc bázi. Produkt IBM Trusteer Rapport for Mitigation for Retail musí být na takovém dotčeném zařízení Vybraného účastníka (PC/MAC) spuštěn a takový dotčený Vybraný účastník musí přijmout smlouvu EULA, minimálně jednou se přihlásit k Maloobchodní aplikaci (Maloobchodním aplikacím) Zákazníka a konfigurace Zákazníka musí zahrnovat kolekci ID uživatele. Pro vyloučení pochybností se uvádí, že tato služba Cloud Service nezahrnuje právo na používání Úvodní stránky Trusteer Splash nebo k jiné podpoře klientského softwaru majitele účtu určené pro obecné Vybrané účastníky Zákazníka.

4.5.1 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business anebo IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail anebo IBM Trusteer Pinpoint Detect Premium Additional Applications for Business anebo IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

IBM Trusteer Pinpoint Standard for Business vyžaduje nasazení na jakékoli další Obchodní aplikaci nad rámec první Aplikace oprávnění pro IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.

IBM Trusteer Pinpoint Standard for Retail vyžaduje nasazení na jakékoli další Maloobchodní aplikaci nad rámec první Aplikace oprávnění pro IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.

IBM Trusteer Pinpoint Premium for Business vyžaduje nasazení na jakékoli další Obchodní aplikaci nad rámec první Aplikace oprávnění pro IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

IBM Trusteer Pinpoint Premium for Retail vyžaduje nasazení na jakékoli další Maloobchodní aplikaci nad rámec první Aplikace oprávnění pro IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.

4.5.2 IBM Trusteer Pinpoint Detect Standard Redeployment anebo IBM Trusteer Pinpoint Detect Premium Redeployment

Zákazníci, kteří během období poskytování služby znovu nasadí své aplikace pro online bankovnictví, a vyžadují proto změny svého nasazení služby IBM Trusteer Pinpoint Detect, by si měli zakoupit službu IBM Trusteer Pinpoint Detect Redeployment.

Nové nasazení může být vyžadováno z důvodu změny domény nebo hostující adresy URL Aplikace Zákazníkem, převodu online Aplikace na novou technologii, přechodu na novou platformu online bankovnictví nebo přidání nového postupu přihlašování do stávající Aplikace.

Během přechodového období nového nasazení v délce šesti měsíců má Zákazník nárok na další Aplikace (vždy po jedné aplikaci), které běží na již registrovaných Aplikacích.

5. Služby IBM Trusteer Mobile Cloud Service

5.1 IBM Trusteer Mobile Browser for Business nebo IBM Trusteer Mobile Browser for Retail

Produkt IBM Trusteer Mobile Browser je určen k přidání další úrovně ochrany a slouží k zajištění bezpečného online přístupu mobilních zařízení Vybraných účastníků přistupujících k Maloobchodním nebo Obchodním aplikacím Zákazníka, pro které si Zákazník zaregistroval pokrytí služeb Cloud Service, posouzení rizika mobilních zařízení a ochranu proti phishingu. Zabezpečená detekce Wi-Fi je k dispozici pouze pro platformu Android. Pro účely těchto služeb Cloud Service mobilní zařízení zahrnují mobilní telefony nebo tablety a nezahrnují notebooky a počítače MAC.

Prostřednictvím TMA může Zákazník přijímat data událostí, analýzy a informace o statistikách související se zařízeními, jejichž Vybraní účastníci: (i) si zdarma stáhli Software klienta vlastníka účtu, aplikaci licencovanou veřejnosti v rámci licenční smlouvy pro koncové uživatele („EULA“), která je k dispozici ke stažení do mobilních zařízení Vybraných účastníků, a (ii) uzavřeli smlouvu pro koncové uživatele EULA a minimálně jednou provedli své ověření v Obchodní nebo Maloobchodní aplikaci Zákazníka, pro kterou si Zákazník zaregistroval pokrytí služeb Cloud Service. Zákazník může nabízet Software klienta vlastníka účtu pouze pomocí Úvodní stránky Trusteer Splash a nesmí tento software používat pro své interní obchodní operace.

a. Data události:

   Zákazník (a neomezený počet jeho oprávněných pracovníků) může TMA používat k přijímání dat událostí generovaných v důsledku online interakcí mobilních zařízení s Maloobchodními nebo Obchodními aplikacemi Zákazníka, pro které si Zákazník zaregistroval pokrytí služeb Cloud Service.

b. Úvodní stránka Trusteer Splash:

   Marketingová platforma Úvodní stránky Trusteer Splash identifikuje a prodává Software klienta vlastníka účtu Vybraným účastníkům přistupujícím k Obchodním anebo Maloobchodním aplikacím Zákazníka, pro které si Zákazník zaregistroval pokrytí služeb IBM Cloud Service. Zákazník si může vybrat z dostupných šablon Úvodní stránky ("Šablona úvodní stránky"). Na základě samostatné smlouvy nebo rozsahu prací lze sjednat přizpůsobenou úvodní stránku.

Zákazník může souhlasit s poskytnutím ochranných známek, log nebo ikon k použití v souvislosti s TMA a pouze pro využití Úvodní stránky Trusteer Splash a zobrazení v Softwaru klienta vlastníka účtu nebo na vstupních stránkách hostovaných IBM nebo na webu IBM Trusteer. Každé použití poskytnutých ochranných známek, log nebo ikon bude v souladu s přiměřenými zásadami IBM týkajícími se inzerce a využití ochranných známek.

5.2 IBM Trusteer Mobile SDK for Business nebo IBM Trusteer Mobile SDK for Retail

Služby IBM Trusteer Mobile SDK Cloud Service jsou určeny k přidání další úrovně ochrany a slouží k zajištění bezpečného webového přístupu k Maloobchodním nebo Obchodním aplikacím Zákazníka, pro které si Zákazník zaregistroval pokrytí služeb Cloud Service, posouzení rizika mobilních zařízení a ochranu proti pharmingu. Zabezpečená detekce Wi-Fi je k dispozici pouze pro platformu Android.

Služby IBM Trusteer Mobile SDK Cloud Service zahrnují vlastní mobilní sadu pro vývojáře softwaru ("SDK"), softwarový balík obsahující dokumentaci, programovací vlastní knihovny softwaru a ostatní související soubory a položky známé jako mobilní knihovna IBM Trusteer, a "Komponentu běhového prostředí" nebo "Opakovaně šiřitelný" vlastní kód generovaný sadou IBM Trusteer Mobile SDK, který lze vložit a integrovat do chráněných samostatných mobilních aplikací sytému iOS nebo Android Zákazníka, pro které si Zákazník zaregistroval pokrytí služeb Cloud Service. ("Integrované mobilní aplikace Zákazníka").

Produkt IBM Trusteer Mobile SDK for Retail je k dispozici v balíčcích po 100 Vybraných účastnících nebo balíčcích po 100 Zařízeních Zákazníka a produkt IBM Trusteer Mobile SDK for Business je k dispozici v balíčcích po 10 Vybraných účastnících nebo balíčcích po 10 Zařízeních Zákazníka.

Prostřednictvím TMA může Zákazník (a neomezených počet jeho oprávněných pracovníků) přijímat reporty o datech událostí a hodnocení trendů rizik. Prostřednictvím Integrované mobilní aplikace Zákazníka může Zákazník přijímat analýzy rizik a informace o mobilním zařízení související s mobilními zařízeními Vybraných účastníků, kteří si stáhli Integrovanou mobilní aplikaci Zákazníka. Zákazník tak může vytvořit zásady prevence podvodů, které budou vynucovat zmírňující akce zaměřené na tato rizika. Pro účely této nabídky zahrnují "mobilní zařízení" pouze podporované mobilní telefony, nikoli počítače PC a MAC.

Zákazník může:

a. interně používat sadu IBM Trusteer Mobile SDK výhradně pro účely vývoje Integrovaných mobilních aplikací Zákazníka;

b. vnořit Opakovaně šiřitelný kód (výhradně ve formátu objektového kódu) jako integrální neoddělitelný způsob do Integrované mobilní aplikace Zákazníka. Jakákoli změněná nebo sloučená část Opakovaně šiřitelného kódu v souladu s touto licencí podléhá stejným podmínkám tohoto Popisu služeb; a

c. prodávat Opakovaně šiřitelný kód a distribuovat jej ke stažení do mobilních zařízení Vybraných účastníků nebo vlastníkovi Zařízení Zákazníka za předpokladu, že:

- S výjimkou případů výslovně povolených v této Smlouvě Zákazník nesmí (1) používat, kopírovat, měnit nebo distribuovat sadu SDK; (2) zpětně sestavovat, kompilovat nebo jinak překládat nebo provádět zpětnou analýzu sady SDK s výjimkou případů výslovně povolených zákonem bez možnosti smluvního vzdání se práv; (3) sadu SDK poskytovat v rámci dílčí licence, pronajímat nebo poskytovat na leasing; (4) odstranit soubory, jež jsou předmětem autorských práv, a sdělení obsažená v Opakovaně šiřitelném kódu; (5) používat stejný název cesty jako původní soubory nebo moduly Opakovaně šiřitelného kódu; a (6) používat názvy nebo ochranné známky IBM, jejích poskytovatelů licence a distributorů v souvislosti s marketingem Integrované mobilní aplikace Zákazníka bez předchozího písemného souhlasu těchto stran.
- Opakovaně šiřitelný kód zůstane neoddělitelným způsobem integrovaný do Integrované mobilní aplikace Zákazníka. Opakovaně šiřitelný kód musí být pouze ve formě objektového kódu a musí splňovat všechny pokyny a specifikace v sadě SDK a v příslušné dokumentaci. Licenční smlouva s koncovým uživatelem pro Integrovanou mobilní aplikaci Zákazníka musí koncového uživatele upozornit, že Opakovaně šiřitelný kód nesmí být i) použit k jinému účelu než k povolení Integrované mobilní aplikace Zákazníka, ii) zkopírován (s výjimkou pro účely zálohování), iii) dále distribuován nebo přenesen ani iv) zpětně získán, kompilován nebo jinak přeložen s výjimkou konkrétně povolenou právními předpisy a bez možnosti smluvního vzdání se práv. Licenční smlouva Zákazníka musí zajistit minimálně stejnou ochranu IBM jako podmínky této Smlouvy.
- Sadu SDK lze implementovat pouze v rámci interní implementace Zákazníka a testování jednotky na určených mobilních testovacích zařízeních Zákazníka. Zákazník nesmí sadu SDK používat pro účely zpracování produktivní zátěže, simulace produktivní zátěže nebo testování škálovatelnosti kódu, aplikace nebo systému. Zákazník nesmí používat žádnou část sady SDK k jakýmkoli jiným účelům.

Zákazník nese výhradní odpovědnost za vývoj, testování a podporu Integrované mobilní aplikace Zákazníka. Zákazník nese odpovědnost za veškerou technickou asistenci pro Integrovanou mobilní aplikaci Zákazníka a jakékoli modifikace Opakovatelně šiřitelných kódů provedené Zákazníkem v souladu s tímto dokumentem.

Zákazník je oprávněn instalovat a používat Opakovaně šiřitelné kódy a sadu IBM Security Mobile SDK pouze k podpoře svého používání služeb Cloud Service.

IBM otestovala ukázkové aplikace vytvořené prostřednictvím mobilních nástrojů poskytnutých v sadě IBM Trusteer Mobile SDK ("Mobilní nástroje"), aby zjistila, zda bude možno je řádně spouštět v určitých verzích mobilních platforem OS ze zařízení Apple (iOS) a Google (Android) (společné označení "Mobilní platformy OS"). Mobilní platformy OS jsou však poskytovány třetími stranami, nejsou pod kontrolou IBM a mohou být změněny, aniž by o tom byla IBM informována. Vzhledem k tomu a bez ohledu na jakékoli jiné podmínky IBM nezaručuje, že jakékoli aplikace nebo jiné výstupy, které byly vytvořeny pomocí Mobilních nástrojů, bude možné na jakýchkoli Mobilních platformách OS nebo mobilních zařízeních správným způsobem spouštět, že budou s těmito platformami a nástroji spolupracovat nebo že s nimi budou kompatibilní.

Zdrojové komponenty a vzorové materiály - IBM Trusteer Mobile SDK může zahrnovat určité komponenty ve formě zdrojového kódu ("Zdrojové komponenty") nebo jiné materiály, které jsou označeny jako Vzorové materiály. Zákazník smí kopírovat a upravovat Zdrojové komponenty a Vzorové materiály pouze pro interní účely, za předpokladu, že toto užívání splňuje limity licenčních práv podle této Smlouvy, avšak pod podmínkou, že Zákazník nesmí pozměňovat ani odstraňovat žádné informace o autorských právech nebo výhrady autorských práv, které jsou uvedeny ve Zdrojových komponentách či Vzorových materiálech. IBM poskytuje Zdrojové komponenty a Vzorové materiály bez závazku podpory a "JAK

JSOU", BEZ ZÁRUKY JAKÉHOKOLI DRUHU, VÝSLOVNĚ VYJÁDŘENÉ NEBO KONKLUDENTNÍ, VČETNĚ ZÁRUKY PLYNOUCÍCH Z VLASTNICKÉHO PRÁVA, NEPORUŠENÍ PRÁV NEBO NEZASAHOVÁNÍ DO PRÁV TŘETÍCH STRAN A ZÁRUK A PODMÍNEK PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Upozorňujeme, že Zdrojové komponenty nebo Vzorové materiály jsou poskytovány výhradně jako příklad implementace Integrovatelného obsahu do CIMA; Zdrojové komponenty a Vzorové materiály nemusejí být kompatibilní s vývojovým prostředím Zákazníka a Zákazník nese výhradní odpovědnost za testování a implementaci Integrovatelného obsahu do CIMA.

Zákazník vyjadřuje souhlas, že vytvoří, uchová a IBM a jejím auditorům poskytne přesné písemné záznamy, výstupy ze systémových nástrojů a ostatní informace systému postačující k poskytnutí auditovatelného ověření, že používání sady IBM Trusteer Mobile SDK Zákazníkem je v souladu s ustanoveními tohoto Popisu služeb.

6. Podpora Premium

Zákazník má nárok na podporu Premium pouze v případě služeb Cloud Service, ke kterým si Zákazník zaregistroval související nabídky podpory Premium.

7. Nasazení produktu IBM Trusteer Fraud Protection

Pro každou Aplikaci, kterou si Zákazník zaregistroval, zahrnuje základní registrace Zákazníka požadované činnosti nastavení a počátečního nasazení v cloudu IBM Trusteer, včetně počátečního jednorázového spuštění, konfigurace, šablony úvodní stránky, testování a školení.

Činnosti nasazení nezahrnují činnosti implementace, které jsou vyžadovány v Aplikacích nebo systémech Zákazníka.

Fáze implementace různých služeb Cloud Service je navržena pro časové rámce uvedené v relevantních příručkách implementace.

Provedení těchto fází implementace v rámci přiděleného časového rámce závisí na plné angažovanosti a účasti vedoucích pracovníků a zaměstnanců Zákazníka. Zákazník je povinen poskytnout požadované informace včas. Podmínkou pro plnění ze strany IBM je včasné poskytnutí informací a včasné učinění jakýchkoli rozhodnutí ze strany Zákazníka; jakékoli prodlení může mít za následek dodatečné náklady anebo prodlení s realizací těchto služeb v oblasti implementace.

Pro každou zaregistrovanou Aplikaci zahrnuje základní registrace Zákazníka požadované činnosti nastavení a počáteční implementace v cloudu IBM Trusteer, včetně počátečního jednorázového spuštění, konfigurace, šablony úvodní stránky, testování a školení.

Registrace Zákazníka zahrnuje podporu a testování pro stránky v rámci takové aplikace Zákazníka, která bude označena IBM jako doporučená během počátečního nasazení. IBM nenese odpovědnost za: (i) částečné nasazení, (ii) rozhodnutí Zákazníka nenasadit služby IBM Cloud Service podle doporučení IBM, (iii) za rozhodnutí Zákazníka provést nasazení, nastavení a testování samostatně, ani za (IV) částečné nasazení nebo ochranu v důsledku nedostatečných informací poskytnutých Zákazníkem. Za dodatečný poplatek a na základě samostatné smlouvy mohou být smluvně sjednány dodatečné služby, včetně činností nasazení nad rámec počátečního nasazení.

8. Ochrana osobních údajů a zabezpečení

Tato služba Cloud Service splňuje zásady IBM pro zabezpečení dat a ochranu soukromí IBM SaaS, které jsou k dispozici na adrese http://www.ibm.com/cloud/data-security, a další dodatečné podmínky uvedené v této části. Jakákoli změna zásad zabezpečení a ochrany soukromí IBM nesníží zabezpečení služby Cloud Service.

Tuto službu Cloud Service lze využívat ke zpracovávání obsahu, který zahrnuje osobní údaje, pokud Zákazník jako správce dat rozhodne, že technická a organizační bezpečnostní opatření jsou přiměřená rizikům spojeným se zpracováním a povahou údajů, které je třeba chránit. Zákazník uznává, že tato služba Cloud Service nenabízí funkce pro ochranu citlivých osobních údajů nebo údajů, na něž se vztahují další regulační požadavky.

Tato služba Cloud Service je zahrnuta do certifikace Privacy Shield IBM a uplatní se, pokud si Zákazník zvolí hostování služby Cloud Service v datovém středisku ve Spojených státech, a vztahují se na ni zásady zabezpečení certifikace Privacy Shield IBM dostupné na adrese http://www.ibm.com/privacy/details/us/en/privacy_shield.html.

8.1 Funkce zabezpečení a odpovědnost

Služba Cloud Service zahrnuje následující bezpečnostní funkce:

Služba Cloud Service šifruje obsah během přenosu dat do sítě IBM a z ní, je-li nečinná a čeká na přenos dat z koncového bodu.

8.2 Použití v souladu s právními předpisy a udělení souhlasu

Použití v souladu s právními předpisy

Použití této služby Cloud Service může implikovat různé právní předpisy. Službu Cloud Service lze používat pouze zákonným způsobem a pro účely, které jsou v souladu se zákonem. Zákazník se zavazuje, že službu Cloud Service bude používat v souladu s platnými právními předpisy a zásadami, a v této souvislosti přebírá veškerou odpovědnost.

Oprávnění ke shromažďování a zpracování údajů

Služba Cloud Service bude shromažďovat informace od Vybraných účastníků a Zařízení Zákazníka, která spolupracují s Obchodními nebo Maloobchodními aplikacemi, pro které si Zákazník zaregistroval pokrytí služeb Cloud Service. Služba Cloud Service shromažďuje informace, které mohou být samostatně nebo v kombinaci v určitých jurisdikcích považovány za Osobní údaje. Osobní údaje jsou jakékoli informace, které mohou být použity k identifikaci určité osoby (například jméno, e-mailová adresa, adresa bydliště nebo telefonní číslo) a které byly poskytnuty IBM pro účely uložení, zpracování nebo přenosu jménem Zákazníka.

Postupy shromažďování a zpracování údajů mohou být aktualizovány za účelem zlepšení funkcí služby Cloud Service. Zákazníkovi je na vyžádání k dispozici dokument s kompletním popisem postupů shromažďování a zpracování dat, který je podle potřeby aktualizován. Zákazník opravňuje IBM ke shromažďování těchto informací a jejich zpracování v souladu s oddílem Přenosy přes hranice a oddílem Ochrana osobních údajů tohoto Popisu služeb.

Pro nabídky IBM Trusteer, které zahrnují Trusteer Management Application (TMA):

Následující data jsou shromažďována a ukládána v Trusteer Management Application (TMA) pro správce TMA od sponzorujících podniků: e-mailová adresa (jako přihlašovací jméno), skryté heslo, jméno, příjmení, pozice a oddělení.

Pro služby IBM Trusteer Pinpoint Cloud Services:

Shromažďovaná data mohou zahrnovat:

- identifikátory uživatele nebo koncového bodu, například šifrované nebo jednosměrně hašované ID uživatele, trvalé ID uživatele (PUID), klíč agenta pro produkt Rapport a ID relace Zákazníka;
- data související s chráněnou aplikací, například konkrétní atributy/prvky aplikace pro online bankovnictví zákazníka zobrazené v prohlížeči koncového uživatele, návštěvy webové stránky a historii procházení;
- informace o prostředí nainstalovaného softwaru, atributů a nastavení prohlížeče i zařízení a období historie prohlížeče;
- informace o hardwaru a časové razítko;
- záhlaví prohlížeče a data komunikačního protokolu, například adresa IP uživatele, soubory cookie, záhlaví odkazujícího webu a další záhlaví HTTP;
- pohyby dat myší koncového uživatele, jako jsou souřadnice ukazatele myši, kliknutí a pohyby posunovacího kolečka (a jejich ekvivalenty) a časové razítko během interakce s online bankovní aplikací Zákazníka;
- phishingové weby a informace na tyto weby odesílané; a
- dle výhradního uvážení Zákazníka transakční data (částka transakce, měna transakce a cílové kódy, jednosměrně hašovaný identifikátor cílové banky transakce, jednosměrně hašovaný identifikátor cílového účtu transakce, binární hodnota, pokud transakce zahrnuje nového příjemce platby, a datum/čas transakce) a volitelné skóre dat rizika.
- dle vlastního uvážení Zákazníka rytmus psaní na klávesnici a řada sekvencí klávesových úhozů používané koncovým uživatelem pro zadávání uživatelského jména, hesla a dalšího textu (nicméně nikoliv písmena, číslice či speciální znaky samotné a bez možnosti rozpoznat uživatelské jméno či heslo);

Zákazník bere na vědomí a souhlasí, že IBM neshromažďuje, neuchovává, nespravuje ani nevede úřední knihy ani záznamy Zákazníka.

Když si Zákazník zaregistruje nabídku IBM Trusteer Rapport for Remediation nebo v určitých případech podpory produktu Pinpoint, může IBM doporučit, aby byl za účelem výzkumu a šetření podezření na infekci malwarem na stroji Vybraného účastníka nainstalován klientský software vlastníka účtu pro produkt Rapport. Shromažďovaná data pro nabídky Rapport jsou uvedena níže.

Pro služby IBM Trusteer Rapport Cloud Service (včetně Rapport for Remediation nebo Rapport for Mitigation v případě nasazení ve spojení s nabídkami Pinpoint):

Shromažďovaná data mohou zahrnovat:

- adresy URL a internetové protokoly (IP) webových stránek, které Vlastník účtu navštíví a které IBM považuje za potenciálně podvodné, phishingové nebo zneužívající, a informace o povaze identifikovaných hrozeb;
- adresy URL a adresy IP webových stránek, které Vlastník účtu navštíví, jsou řízeny Zákazníkem a chráněny službou Cloud Service, například weby internetového bankovnictví; adresy IP Vlastníka účtu;
- informace o identifikaci hardwaru, operačních systémech, aplikačním softwaru, periferním hardwaru, konfiguraci zabezpečení, nastavení systému a síťových připojeních koncového bodu, a dále ID, název, vzorce užívání a další identifikovatelné údaje koncového bodu;
- informace týkající se instalace a provozu programu, ID programu, verze programu, události zabezpečení generované z koncového bodu a informace o chybách programu;
- statistiky užívání a statistické informace o hrozbách zjištěných programem; soubory protokolu obsahující pády prohlížeče, datum a čas infekce a informace o povaze zjištěných hrozeb nebo selhání;
- Vztah Zákazníka označovaný také jako Sponzorující podnik. Vztah je navázán, když koncový uživatel stáhne Zprávu z webových stránek Zákazníka, vybere konkrétního Zákazníka při stahování Zprávy ze stránky podpory Trusteer nebo se přihlásí k bankovní aplikaci Zákazníka. Koncový uživatel může mít více než jeden vztah Zákazníka;
- kopii šifrovaného ID uživatele, které Vlastník účtu využívá k interakci se Zákazníkem (volitelné);
- šifrovanou kopii čísla platební karty, které Vlastník účtu zadá na webu poté, co ho program informuje, že daný web považuje za rizikový;
- soubory a další informace z koncového bodu, u nichž mají odborníci na zabezpečení IBM podezření, že mohou souviset s malwarem nebo jinou škodlivou aktivitou, nebo které mohou být spojeny s obecným selháním programu; a
- osobní kontaktní informace, včetně jména a e-mailu, když koncový uživatel kontaktuje Podporu.

Pro nabídky IBM Trusteer Mobile SDK a služby IBM Trusteer Mobile Browser Cloud Service:

Shromažďovaná data mohou zahrnovat:

- identifikátory uživatele, například šifrované nebo jednosměrně hašované ID uživatele,
- informace o zařízení, například adresu IP, hašované ID zařízení, časové razítko, hodnoty nainstalovaného balíčku MD5 a další informace o hardwaru a softwaru zařízení,
- verze a datum instalace sady SDK pro mobilní zařízení nebo prohlížeče pro mobilní zařízení;
- návštěvy chráněných aplikací,
- spojení Zákazníka; a
- data o rizicích zařízení (např. přítomnost malwaru, aplikace pro skrývání kořenových složek, stav šifrování Wi-Fi, zda bylo zařízení chráněno aplikací Jailbreak),
- havárie trasování zásobníku (v případě neočekávaného ukončení aplikace),
- telefonicky sestavená data (např., model, výrobce),
- interakce dotykové obrazovky koncového uživatele včetně souřadnic x, y, typy oblasti dotyku a typ akce (dolu, nahoru a posun);

- data pohybového snímače, využití napájení/zdrojů, nastavení konektivity, snímače prostředí, jako jsou teplota, světlo a tlak vzduchu, jakož i obecná nastavení zařízení (hlasitost, ztišení na omezenou dobu, jas obrazovky atd.).

8.3 Informovaný souhlas od Datových subjektů

Pro služby IBM Trusteer Pinpoint Cloud Service a IBM Trusteer Mobile SDK Cloud Service:

Zákazník vyjadřuje souhlas, že získal nebo získá plně informované souhlasy, oprávnění nebo licence nutné k používání služby Cloud Service v souladu se zákony a k povolení shromažďování a zpracování informací společností IBM prostřednictvím služeb IBM Cloud Service.

Pro služby IBM Trusteer Rapport (včetně Rapport Remediation nebo Rapport for Mitigation v případě nasazení ve spojení se službami Pinpoint Cloud Service) a službami IBM Trusteer Mobile Browser Cloud Service:

Zákazník opravňuje IBM k získání plně informovaných souhlasů nutných k používání služby Cloud Service v souladu s právními předpisy a ke shromažďování a zpracování informací podle popisu v Licenční smlouvě s koncovým uživatelem na adrese https://www.trusteer.com/support/end-user-license-agreement. Pokud Zákazník určí, že on (a nikoli IBM) bude mít na starosti komunikaci s koncovými uživateli týkající se získání souhlasu, vyjadřuje souhlas s tím, že získal nebo získá plně informované souhlasy, oprávnění nebo licence nutné k používání služby Cloud Service v souladu se zákony a k povolení shromažďování a zpracování informací společností IBM prostřednictvím Cloud Service.

8.4 Použití dat zabezpečení

V rámci služby Cloud Service, která zahrnuje činnosti vytváření sestav, bude IBM připravovat a uchovávat neidentifikované anebo agregované informace shromážděné ze služby Cloud Service ("Data zabezpečení"). S výjimkou uvedenou v bodě (d) níže nebudou Data zabezpečení identifikovat Zákazníka, jeho Vybrané účastníky ani jednotlivce. Zákazník souhlasí, že IBM je oprávněna Data zabezpečení trvale používat anebo kopírovat pouze k následujícím účelům:

a. publikování anebo distribuce Dat zabezpečení (např. v kompilacích anebo analýzách týkajících se kybernetické bezpečnosti),

b. vývoj a vylepšení produktů nebo služeb,

c. interní výzkum nebo výzkum realizovaný se třetími osobami, a

d. sdílení informací o potvrzeném pachateli, který je třetí osobou, v souladu se zákonem.

8.5 Přeshraniční přenosy

Zákazník vyjadřuje souhlas, že IBM může zpracovat obsah, včetně jakýchkoli Osobních údajů identifikovaných v oddílu Použití v souladu se zákony a souhlas výše, v souladu s relevantními zákony a požadavky přes státní hranice zpracovatelům a dílčím zpracovatelům v následujících zemích mimo EHS a zemích, které mají podle Evropské Komise odpovídající úrovně zabezpečení: USA.

8.6 Ochrana osobních údajů

Pokud Zákazník poskytuje službě Cloud Service Osobní údaje v členských státech EU, na Islandu, v Lichtenštejnsku, Norsku nebo Švýcarsku nebo pokud má Zákazník v těchto zemích Vybrané účastníky nebo Zařízení Zákazníka, Zákazník jako výhradní kontrolor určí IBM jako zpracovatele ke zpracování (tyto pojmy jsou definovány ve směrnici EU 95/46/ES) Osobních údajů. IBM bude takové Osobní údaje zpracovávat pouze v rozsahu požadovaném ke zpřístupnění nabídky služby Cloud Service v souladu s publikovanými popisy IBM služby Cloud Service a Zákazník vyjadřuje souhlas, že takové zpracování je v souladu s pokyny Zákazníka. IBM poskytne prostřednictvím Zákaznického portálu přiměřeně předem oznámení, pokud provede podstatnou změnu umístění zpracování nebo způsobu, jakým zabezpečuje Osobní údaje v rámci služby Cloud Service. Zákazník smí aktuální období registrace pro dotčenou službu Cloud Service ukončit, a to na základě písemné výpovědi poskytnuté IBM do třiceti (30) dní od okamžiku, kdy IBM změnu Zákazníkovi oznámila.

Strany nebo jejich relevantní příbuzné společnosti mohou uzavřít samostatné standardní a nezměněné smlouvy k Modelovým ustanovením EU z titulu jejich příslušného postavení, a to v souladu s Rozhodnutím EU 2010/87/EU a s odebranými volitelnými klauzulemi. Jakékoli spory nebo nároky vzniklé na základě těchto smluv, a to i v případě, že byly uzavřeny přidruženými společnostmi, budou stranami posuzovány tak, jako by tento spor nebo odpovědnost vznikly mezi nimi podle podmínek této smlouvy.

a. Zákazník vyjadřuje souhlas s tím, že pro služby poskytované datovým střediskem v Německu určeným během procesu zajišťování smí IBM zpracovávat obsah včetně jakýchkoli Osobních údajů přes hranice státu, a to ve vztahu s následujícími zpracovateli a dílčími zpracovateli:

Název zpracovatele/dílčího zpracovatele	Role (zpracovatel nebo dílčí zpracovatel dat)	Umístění
Smluvní subjekt IBM	Zpracovatel	Tak, jak je uvedeno v Transakčním dokumentu
Amazon Web Services (Německo)	Dílčí zpracovatel	Německo
IBM Ireland Ltd.	Zpracovatel	Irsko
IBM Israel Ltd.	Zpracovatel	Izrael

Pro služby poskytované prostřednictvím německého datového střediska mohou být některé služby zákaznické podpory poskytovány zaměstnanci Trusteer v kterékoliv zemi Evropské unie.

b. Zákazník vyjadřuje souhlas s tím, že pro služby poskytované datovým střediskem v Japonsku určeným během procesu zajišťování smí IBM zpracovávat obsah včetně jakýchkoli Osobních údajů přes hranice státu, a to ve vztahu s následujícími zpracovateli a dílčími zpracovateli:

Název zpracovatele/dílčího zpracovatele	Role (zpracovatel nebo dílčí zpracovatel dat)	Umístění
Smluvní subjekt IBM	Zpracovatel	Japonsko, tak, jak je uvedeno v Transakčním dokumentu
Amazon Web Services (Japonsko)	Dílčí zpracovatel	Japonsko
IBM Ireland Ltd.	Zpracovatel	Irsko
IBM Israel Ltd.	Zpracovatel	Izrael

c. Zákazník vyjadřuje souhlas s tím, že pro služby poskytované datovým střediskem v USA smí IBM zpracovávat obsah včetně jakýchkoli Osobních údajů přes hranice státu, a to ve vztahu s následujícími zpracovateli a dílčími zpracovateli:

Název zpracovatele/dílčího zpracovatele	Role (zpracovatel nebo dílčí zpracovatel dat)	Umístění
Smluvní subjekt IBM	Zpracovatel	Tak, jak je uvedeno v Transakčním dokumentu
Amazon Web Services LLC	Dílčí zpracovatel	USA
IBM Ireland Ltd.	Zpracovatel	Irsko
IBM Israel Ltd.	Zpracovatel	Izrael
IBM Corp	Zpracovatel	USA

d. U služeb poskytovaných datovými středisky uvedenými v Oddíle 8.5.c výše "Datové středisko v USA" smí IBM provádět zpracování také prostřednictvím jednoho nebo více z následujících možných dílčích zpracovatelů podle určení během procesu zajišťování:

Název zpracovatele/dílčího zpracovatele	Role (zpracovatel nebo dílčí zpracovatel dat)	Umístění
Amazon Web Services (Austrálie)	Dílčí zpracovatel	Austrálie
Amazon Web Services (Singapur)	Dílčí zpracovatel	Singapur
Amazon Web Services (Irsko)	Dílčí zpracovatel	Irsko

e. Zákazník souhlasí, že IBM je oprávněna po oznámení na Zákaznickém portálu migrovat zpracování ze služeb Amazon Web Services do datových středisek IBM. Po oznámení na Portálu pro zákazníky je IBM dále oprávněna změnit seznam dílčích zpracovatelů uvedený výše.

f. Data Vlastníka účtu budou zpracována v oblasti, ve které Vlastník účtu původně nainstaloval klientský software vlastníka účtu. To znamená, že obsah Vlastníka účtu může být zpracováván v původní oblasti i v oblasti odsouhlasené Zákazníkem.

g. Data zákaznické podpory jsou ukládána na cloudovém serveru Salesforce.com, který je umístěn v Irsku.

h. Pro účely vysvětlení se uvádí, že vzhledem k tomu, že Trusteer Fraud Protection je integrované řešení, pokud Zákazník ukončí některou z těchto služeb Cloud Services, IBM si může uchovat data Zákazníka pro účely poskytování zbývajících služeb Cloud Services Zákazníkovi v souladu s tímto Popisem služby.

9. Dohoda o úrovni služeb

IBM poskytuje pro Cloud Service následující Dohodu o úrovni služeb, jak je uvedeno v Dokumentu o oprávnění (Proof of Entitlement). Dohoda o úrovni služeb nepředstavuje záruku. Dohoda o úrovni služeb je k dispozici pouze pro Zákazníka a vztahuje se pouze na používání v produktivních prostředích.

9.1 Kredity za porušení úrovně dostupnosti služeb

Zákazník musí u IBM střediska technické podpory zaregistrovat tiket podpory se Závažností 1 do 24 hodin od okamžiku, kdy poprvé zjistil, že událost měla dopad na dostupnost služby Cloud Service. Zákazník musí s IBM přiměřeně spolupracovat při diagnostice a řešení problémů.

Nárok na tiket podpory za nesplnění Dohody o úrovni služeb musí být předložen do tří pracovních dní od konce smluvního měsíčního období. Kompenzací za platný nárok týkající se Dohody o úrovni služeb bude kredit vydaný oproti budoucí faktuře za Cloud Service na základě doby, během které nebylo zpracování produktivního systému pro Cloud Service k dispozici ("Odstávka"). Odstávka se měří od okamžiku, kdy Zákazník nahlásí událost, do okamžiku obnovení Cloud Service a nezahrnuje čas související s plánovanou nebo nahlášenou odstávkou v rámci údržby, příčinami mimo kontrolu IBM, problémy s obsahem, technologií Zákazníka nebo třetí osoby, návrhy nebo pokyny, nepodporovanými konfiguracemi systému a platformami nebo jinými chybami Zákazníka či incidentem zabezpečení způsobeným Zákazníkem nebo testováním zabezpečení Zákazníka. IBM bude aplikovat nejvyšší použitelnou kompenzaci vycházející ze souhrnné dostupnosti služby Cloud Service dosažené během každého smluvního měsíčního období, jak je uvedeno v tabulce níže. Celková kompenzace vztahující se k jakémukoliv smluvnímu měsíčnímu období nesmí přesáhnout deset procent z jedné dvanáctiny (1/12) ročního poplatku za Cloud Service.

9.2 Úrovně služeb

Dostupnost Cloud Service v průběhu smluvního měsíčního období

Dostupnost v průběhu smluvního měsíčního období	**Kompenzace (% měsíčního registračního poplatku* za smluvní měsíční období, za které je uplatňován nárok)**
< 99,5 %	2 %
< 98,0 %	5 %
< 96,0 %	10 %

* Pokud byla služba Cloud Service získána od Obchodního partnera IBM, bude měsíční registrační poplatek vypočítán na základě aktuálního ceníku pro Cloud Service, který je platný pro smluvní měsíční období, na které se nárok vztahuje, se slevou 50 %. IBM Zákazníkovi přímo poskytne slevu.

Úrovně služeb a související Kredity služeb jsou měřeny odděleně pro službu Cloud Service a Aplikace Zákazníka.

Při výpočtu kreditů SLA pro službu Cloud Service pro oprávnění Aplikací se Dostupnost vypočte na základě následujících pokynů:

- Každé Aplikaci bude přidělen vážený podíl zjištěného počtu objemu relací během smluvního měsíce.
- Odstávky jednotlivých služeb Cloud Service pro Aplikace se budou akumulovat samostatně pro smluvní měsíc.

Následuje příklad výpočtu za jeden měsíc a souvisejících vah. Slouží pouze k ilustračním účelům:

Maloobchodní aplikace	Podíl celkového počtu relací za příslušný smluvní měsíc	Celková doba odstávky za smluvní měsíc	Vážené minut odstávky
Maloobchodní aplikace A	40 %	300 minut	40 % x. 300 minut = 120 minut
Maloobchodní aplikace B	20 %	250 minut	20 % x 250 minut = 50 minut
Maloobchodní aplikace C	40 %	150 minut	40 % x 150 minut = 60
			Celkový počet vážených minut odstávky = 230

Procento dostupnosti se vypočítá jako: celkový počet minut v rámci smluvního měsíčního období minus celkový počet vážených minut Odstávky za smluvní měsíční období, děleno celkovým počtem minut za smluvní měsíční období. Příklad výpočtu na příkladu výše uvedených vah je následující:

Celkem 43 200 minut za 30denní Smluvní měsíční období - 230 vážených minut odstávky = 42 970 minut _____ Celkem 43 200 minut	Kredity za porušení úrovně dostupnosti služeb = 2 % pro 99,4% dostupnost během smluvního měsíčního období

10. Technická podpora

Technická podpora pro služby Cloud Service je Zákazníkovi a jeho Vybraným účastníkům poskytována s cílem poskytnout jim asistenci při užívání služeb Cloud Service.

Registrace všech nabídek zahrnuje Standardní podporu. Předpokladem pro podporu Premium pro základní registraci Trusteer Rapport je služba Trusteer Rapport Mandatory Service, což je doplněk služby Trusteer Rapport.

Pro každou službu Cloud Service je za dodatečný poplatek k dispozici registrace podpory Premium, a to s výjimkou produktů IBM Trusteer Mobile SDK Cloud Services a IBM Trusteer Rapport Mandatory Service Cloud Services. Obraťte se na Prodejního zástupce nebo Obchodního partnera IBM.

Standardní podpora:

- Podpora poskytovaná od 8:00 do 17:00 místního času.
- Zákazníci a jejich Vybraní účastníci mohou odesílat záznamy požadavku podpory elektronicky podle popisu v příručce podpory Software as a Service [SaaS].
- Zákazníci naleznou oznámení, dokumenty, sestavy jednotlivých případů a časté dotazy na portálu zákaznické podpory na adrese: http://www-01.ibm.com/software/security/trusteer/support/.
- Volby a podrobnosti podpory naleznete v příručce podpory Software as a Service [SaaS]: http://www-01.ibm.com/software/support/handbook.html.

Podpora Premium:

- Nepřetržitá podpora pro všechny úrovně závažnosti.
- Zákazníci mohou podporu získat přímo telefonicky a prostřednictvím zpětného volání.
- Zákazníci a jejich Vybraní účastníci mohou odesílat záznamy požadavku podpory elektronicky podle popisu v příručce podpory Software as a Service [SaaS].
- Zákazníci naleznou oznámení, dokumenty, sestavy jednotlivých případů a časté dotazy na portálu zákaznické podpory na adrese: http://www-01.ibm.com/software/security/trusteer/support/.
- Volby a podrobnosti podpory naleznete v příručce podpory Software as a Service [SaaS]: http://www-01.ibm.com/software/support/handbook.html.

11. Oprávnění a informace o fakturaci

11.1 Metriky poplatků

Služba Cloud Service je poskytována v rámci metriky poplatků uvedené v Transakčním dokumentu:

a. **Vybraný účastník** – je měrnou jednotkou, na jejímž základě lze získat Cloud Service. Vybraným účastníkem je každá fyzická nebo právnická osoba, která je způsobilá k účasti na jakémkoli programu poskytování služeb a který je spravován nebo sledován prostřednictvím služby Cloud Service. Je nutno získat dostatečný počet oprávnění, který bude pokrývat všechny Vybrané účastníky spravované nebo sledované v rámci Cloud Service během období měření specifikovaného v Transakčním dokumentu Zákazníka.

   Všechny programy poskytování služeb spravované službou Cloud Service jsou analyzovány samostatně a následně sloučeny. Fyzické nebo právnické osoby, které jsou oprávněny využívat více programů poskytování služeb, vyžadují samostatné nároky.

   Pro účely oprávnění těchto služeb Cloud Service je Vybraný účastník koncový uživatel Zákazníka s přihlašovacími pověřeními k Obchodní nebo Maloobchodní aplikaci Zákazníka.

b. **Zařízení klienta** – je měrnou jednotkou, na jejímž základě lze získat službu Cloud Service. Zařízení Zákazníka je výpočetní zařízení pro jednoho uživatele nebo senzor či telemetrické zařízení sloužící ke speciálnímu účelu, které vyžaduje spuštění nebo přijímá pro spuštění sadu příkazů, postupů nebo aplikací z jiného počítačového systému nebo poskytuje data do jiného počítačového systému, který je typicky označován jako server nebo je jinak řízen serverem. Více Zařízení Zákazníka může sdílet přístup ke společnému serveru. Zařízení Zákazníka může mít určité funkce v oblasti zpracování nebo může být programovatelné, aby uživateli umožňovalo výkon práce. Zákazník je povinen získat oprávnění pro každé Klientské zařízení, které spouští službu Cloud Service, poskytuje data pro službu Cloud Service, používá služby poskytované službou Cloud Service nebo jinak přistupuje ke službě Cloud Service během období měření uvedeného v Transakčním dokumentu Zákazníka.

c. **Aplikace** – je měrnou jednotkou, na jejímž základě lze získat Cloud Service. Aplikace je softwarový program s jedinečným názvem. Pro každou Aplikaci zpřístupněnou a používanou během období měření uvedeného v Zákazníkově Dokumentu o oprávnění (Proof of Entitlement) nebo Transakčním dokumentu je nutno získat dostatečný počet oprávnění.

   Pro službu Cloud Service představuje aplikace jednu Obchodní nebo Maloobchodní aplikaci Zákazníka.

d. **Sjednaná služba** – je měrnou jednotkou, na jejímž základě lze získat služby. Sjednaná služba sestává z odborných služeb anebo ze služeb v oblasti vzdělávání v souvislosti se službami Cloud Service. Je nutno získat dostatečný počet oprávnění, který bude pokrývat každou Sjednanou službu.

11.2 Poplatky za neúplný měsíc

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

12. Dodržování předpisů a audity

Přístup ke službám IBM Trusteer Fraud Protection Cloud Service podléhá maximálnímu množství Aplikací, Vybraných účastníků anebo Zařízení Zákazníka určenému v Transakčním dokumentu. Zákazník nese odpovědnost za zajištění, že jeho počet Aplikací, Vybraných účastníků anebo Zařízení Zákazníka nepřekročí maximální množství uvedené v Transakčním dokumentu.

Za účelem ověření dodržení maximálního počtu Aplikací, Vybraných účastníků anebo Zařízení Zákazníka může IBM provést audit.

13. Smluvní období a možnost obnovení

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

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

V případě průběžného používání bude služba Cloud Service dále dostupná na měsíční bázi, dokud Zákazník neposkytne 90 dní předem písemnou výpověď. Po ukončení takového 90denního období zůstane služba Cloud Service k dispozici do konce kalendářního měsíce.

14. Aktivační software

Tato Cloud Service zahrnuje aktivační software, který může Zákazník používat pouze ve spojení se svým užíváním Cloud Service a pouze po dobu poskytování služby Cloud Service.

15. Navýšení poplatku za roční registraci produktu IBM Trusteer

IBM si vyhrazuje právo upravit poplatek za registraci pro tuto službu Cloud Services. Úprava poplatku za registraci bude reflektována v cenách stanovených v podmínkách příslušné Cenové nabídky. Další úpravy poplatku za registraci, které lze uplatnit maximálně jednou za dvanáct (12) měsíců o procento stanovené IBM, které nesmí překročit 3 %, se mohou uplatnit, jestliže je prodloužena doba platnosti služby Cloud Services na základě automatického prodloužení nebo pokračování používání. Tyto úpravy poplatků nezmění nárok Zákazníka na služby Cloud Service ani metriku poplatků, na základě které je služba Cloud Service získána. Obchodní partneři IBM jsou nezávislí na IBM a sami si určují své ceny a podmínky.