SMLOUVA O DÍLO - č. j.: MV-62520-4/SIK5-2019

(dále jen „smlouva“)

Objednatel:

Česká republika - Ministerstvo vnitra, se sídlem: Praha 7, Nad Štolou 936/3, PSČ 170 34; IČ: 00007064 zastoupená Mgr. Bohdanem Urbanem, ředitelem odboru provozu informačních technologií a komunikací

Poskytovatel:	**Spis. zn. :**
T-Mobile Czech Republic a.s.	**Vyřizuje :**
Tomíčkova 2144/1	**Telefon :**
148 00 Praha 4	**Fax :**
DIČ: CZ64949681 IČO: 64949681	**Mobil :**
Bankovní spojení: KB a.s., **č. ú:** 19-2235200217/0100	**ID dat. schr. :**
	e-mail :
Zapsaný v obchodním rejstříku vedeném Městským soudem v Praze oddíl B, vložka 3787	**http :**
Zastoupený:	

Objednatel a poskytovatel jsou společně nazýváni „smluvní strany“.

Kontaktní údaje objednatele:	**Vyřizuje : Mgr. Kateřina Obešlová**
Česká republika - Ministerstvo vnitra (OPITK)	**Telefon : 974 841 729**
nám. Hrdinů 1634/3	**Fax : 974 841 055**
140 21 PRAHA 4	**e-mail : katerina.obeslova@mvcr.cz**
Bankovní spojení:	***Fakturace:***
Název : ČNB Praha	**Způsob úhrady : převodním příkazem**
Směr. numer. kód : 0710	**Účtujte : fakturou s DPH**
Číslo účtu : 3605881	**Fakturace na adresu:** MV (OPITK), nám. Hrdinů 1634/3, 140 21 PRAHA 4
Místo plnění:	***Osoba oprávněná k předání/převzetí předmětu plnění a podpisu akceptačního protokolu:***
Olšanská 1951/4	
130 27 Praha 3	**Za objednatele:** Mgr. Bohdan Urban
Způsob dopravy: Poskytovatelem	**E-mail:** bohdan.urban@mvcr.cz **Telefon: 974 841 789**
Dodání je možné pouze v pracovních dnech v době: pondělí-čtvrtek 8:00-16:00, pátek 8:00-14:30	Z důvodu připravenosti k předání a převzetí předmětu plnění žádáme o telefonické vyzvání před dodáním v pracovní době (pondělí-pátek 7:30-15:00)

Předmět plnění	**DDoS ochrana vnějšího připojení do internetu** spočívající v jednovrstvé DDoS ochraně konektivity objednatele IP transit 4 Gbps, GN 111403 a GN 111404, v období voleb do Evropského parlamentu 2019 (dále jen „předmět plnění“).

Počet listů: -1-	Přílohy: -1-	**Počet položek předmětu plnění: -1-**
Termín plnění: neprodleně po nabytí účinnosti smlouvy		**Celková cena:** 325.890,00 Kč bez DPH **394.326,90 Kč s DPH**

Platba po akceptaci předmětu plnění. ***Na fakturu uveďte číslo jednací této smlouvy. Součástí faktury musí být akceptační protokol potvrzený osobou oprávněnou k převzetí předmětu plnění - bez tohoto dokladu nelze fakturu proplatit.***. Smluvní strany se dohodly, že jejich závazkový vztah se řídí zákonem č. 89/2012 Sb. v platném znění a s použitím § 1746 a následujících tohoto zákona uzavírají na veřejnou zakázku malého rozsahu podle § 31 a § 6 zákona č. 134/2016 Sb. v platném znění tuto smlouvu. Dílčí plnění se nepřipouští. Poskytovatel poskytuje záruku na předmět plnění po dobu poskytování předmětu plnění. Smlouvu lze měnit nebo doplňovat pouze dohodou smluvních stran a to pouze formou písemných dodatků ke smlouvě. Smlouva se vyhotovuje ve třech výtiscích s platností originálu, z nichž objednatel obdrží jeden výtisk a poskytovatel obdrží dva výtisky. Smluvní strany prohlašují, že jejich označení ve smlouvě odpovídá aktuálnímu zápisu v obchodním rejstříku či na roveň postavenému jinému zápisu (dále jen „OR“). Údaje ve smlouvě uvedené nejsou dotčeny změnami již uskutečněnými, avšak ještě nezapsanými v OR, uzavření smlouvy je v souladu s právním řádem České republiky a interními akty řízení, jakož v plném zájmu smluvních stran, smlouvu si před podepsáním pečlivě přečetly a smlouva byla uzavřena podle jejich svobodné vůle, vážně a nikoliv v tísni ani za jednostranně nevýhodných podmínek pro některou smluvní stranu, určitě a srozumitelně a na důkaz toho připojují své podpisy. Smlouva je platná po podepsání oprávněnými zástupci smluvních stran uvedenými ve smlouvě a účinná dnem uveřejnění v registru smluv (http://smlouvy.gov.cz/).

Poskytovatel:	Objednatel:
Datum :	

Po vzájemném potvrzení smluvního vztahu objednatel předá jeden podepsaný výtisk smlouvy poskytovateli.

Nedílnou součástí této smlouvy jsou Platební a obchodní podmínky MV uvedené na druhé straně listu smlouvy a nabídka poskytovatele připojená v příloze.

Platební a obchodní podmínky MV

Cena, platební podmínky a fakturace

1. Celková cena uvedená ve smlouvě je sjednána dohodou smluvních stran podle zákona č. 526/1990 Sb., o cenách, v platném znění a **je konečná a nepřekročitelná** (vyjma případného zaokrouhlení výše DPH na celé haléře nahoru) pro předmět plnění (dále jen "PP") podle specifikace ve smlouvě. Celková cena zahrnuje veškeré náklady včetně nákladů spojených s celními poplatky a dopravou do místa plnění.
2. Prodávající má právo fakturovat PP po jeho převzetí a potvrzení dodacího listu, předávacího/přejímacího protokolu nebo akceptačního protokolu (dále jen „DL", typ dokladu uveden ve smlouvě) oprávněným zástupcem kupujícího v místě plnění.
3. Prodávající je povinen, po vzniku práva fakturovat, vystavit a kupujícímu předat fakturu **ve dvojím vyhotovení** s rozepsáním položek PP přesně dle smlouvy a uvedením jejich jednotkových cen. Faktura musí obsahovat označení (faktura), číslo jednací smlouvy, číslo účtu prodávajícího a všechny údaje uvedené v § 29 a § 29a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění a v § 435 zákona č. 89/2012 Sb., občanský zákoník.
4. **Společně s fakturou prodávající dodá kopii DL podepsaného pověřenými zástupci obou smluvních stran.**
5. Kupující je povinen uhradit fakturovanou částku v době splatnosti faktury, která je stanovena **na 30 kalendářních dní ode dne prokazatelného doručení faktury** kupujícímu na adresu: Ministerstvo vnitra OPITK, nám. Hrdinů 1634/3, 140 21 Praha 4. Osobní doručení je možné na adrese: Ministerstvo vnitra, podatelna, nám. Hrdinů 1634/3, 140 21 Praha 4 (tel.: 974 816 295-9).
6. V roce, v němž bylo uskutečněno plnění, musí být faktura doručena nejpozději **do 5. 12.** do 15^{OO} hod. Při doručení faktury po termínu uvedeném v předchozí větě nelze fakturu v daném roce proplatit, sjednaná lhůta splatnosti faktury se stanovuje na 60 kalendářních dní ode dne doručení faktury.
7. Kupující je oprávněn do data splatnosti vrátit (tj. odeslat zpět kupujícímu) fakturu, která není vystavena v souladu se smlouvou, neobsahuje požadované náležitosti, není doložena kopií potvrzeného DL, nebo obsahuje jiné cenové údaje nebo jiný druh či množství PP než dohodnuté ve smlouvě. Doba splatnosti nové (opravené) faktury začíná znovu běžet ode dne jejího prokazatelného doručení kupujícímu (i v tomto případě musí být bezpodmínečně dodržen bod 8 těchto „Platebních a obchodních podmínek MV").
8. Uhrazením ceny PP se rozumí odepsání oprávněně fakturované finanční částky za PP z účtu kupujícího ve prospěch účtu prodávajícího.

Sankce

9. V případě prodlení s úhradou faktury se smluvní strany dohodly, nebude-li ve smlouvě stanoveno jinak, že kupující uhradí prodávajícímu úrok z prodlení ve výši **0,05 %** z fakturované částky včetně DPH za každý i započatý den prodlení. Výše sankce není omezena.
10. V případě prodlení prodávajícího s dodáním PP se smluvní strany dohodly, nebude-li ve smlouvě stanoveno jinak, že prodávající je povinen uhradit kupujícímu smluvní pokutu ve výši **0,05 %** z celkové ceny PP včetně DPH za každý i započatý den prodlení **(minimálně však 250 Kč za každý i započatý den prodlení)**. Výše sankce není omezena.

Závěrečná ustanovení

11. Za datum prokazatelného oznámení prodávajícímu, že došlo k uzavření smlouvy, je smluvními stranami považováno datum odeslání e-mailové zprávy se sdělením, že smlouva byla uzavřena, na e-mailovou adresu prodávajícího uvedenou ve smlouvě. Informaci o uzavření smlouvy NEN zasílá prodávající.
12. V případě, že mezi vybraným účastníkem a zadavatelem bude uzavřen smluvní závazek formou smlouvy o dílo, nahrazuje se v těchto „Platebních a obchodních podmínkách MV" slovo „kupující" slovem „objednatel", slovo „prodávající" slovem „poskytovatel".

NABÍDKA
telekomunikačních služeb

ZPRACOVÁNO PRO:

Ministerstvo vnitra

VYTVOŘENO DNE:

29. 4. 2019

NÁZEV SLUŽBY:

DDoS ochrana – operátorská vrstva

Obsah

1 Úvodní ustanovení

1.1 Důvěrnost informací

Tento dokument obsahuje informace důvěrného charakteru a je určen výhradně pověřeným pracovníkům společnosti **Ministerstvo vnitra.** Jako takový nesmí být bez předchozího souhlasu T-Mobile Czech Republic a.s. citován, kopírován nebo předán třetí fyzické nebo právnické osobě.

1.2 Identifikační údaje

Plné obchodní jméno:	**T-Mobile Czech Republic a.s.**
Právní forma podnikání:	akciová společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze v oddíle C, vložka č. 145533
Přesná adresa sídla:	**Tomíčkova 2144/1, 148 00 Praha 4**
Telefon /Fax/Poruchy:	**800 737 333 / 603 604 646 / 800 737 373**

1.3 Kontaktní osoba

Pověřený zástupce zodpovědný za jednání jménem T-Mobile Czech Republic a.s.

Jméno a příjmení:	**Ing. Pleštil Viktor**
Mobilní telefon:	**602 108 222**
E-mail:	**viktor.plestil@t-mobile.cz**

1.4 Doplňující informace k předložené nabídce

Cílem této nabídky je předat Vaší společnosti informace o možnostech řešení IT a telekomunikačních služeb T-Mobile Czech Republic. V případě požadavku na jakékoliv doplňující informace se prosím obraťte na pověřeného zástupce T-Mobile Czech Republic.

2 Profil Společnosti

Společnost T-Mobile Czech Republic je členem skupiny Deutsche Telekom AG a v České republice je předním operátorem, poskytujícím jak mobilní služby pro rezidentní klientelu a podnikatele, tak i IT služby pro firemní zákazníky. Integrací společnosti T-Systems zajišťujeme současně nabídku úplného portfolia komplexních služeb a péče o ICT i pro ty největší firemní zákazníky a to ve všech oborech – od automobilového průmyslu přes telekomunikace, finančnictví, obchod, služby, energetiku, až po veřejnou správu a zdravotnictví.

Našim hlavním mottem při poskytování ICT služeb v oblasti B2B je podpora zvýšení konkurenceschopnosti zákazníků; proto k nim přistupujeme s maximální flexibilitou, respektující jejich konkrétní situaci, ať už technologickou nebo finanční. Vždy jim nabízíme řešení, jež nejlépe vyhovují jejich potřebám a řeší je v celé šíři problematiky, se kterou se zákazníci setkávají. Jedinečná symbióza IT a telekomunikačních služeb, podpořená širokým know-how mateřské společnosti Deutsche Telekom, nám dovoluje realizovat komplexní ICT projekty i v oblasti systémové integrace. Díky trvalé kontrole nad všemi komponenty tak poskytujeme záruku vysoké kvality a spolehlivosti celého řetězce služeb až po jednotlivé aplikace u konkrétních uživatelů.

2.1 Proč spolupracovat s T-Mobile

- **Zkušenost a znalost procesů.** Máme významné referenční zákazníky v klíčových odvětvích a důkladné znalosti jejich obchodních modelů a procesů.
- **Nedělitelná odpovědnost.** Šíře našeho portfolia umožňuje dodávat konvergentní řešení jako celek.
- **Ucelená nabídka.** Naše portfolio ICT služeb pokrývá potřeby podniků v celé jejich šíři.
- **Cílená řešení.** Nabízíme vybrané služby infrastruktury a aplikace, stejně jako správu obchodních procesů.
- **Jeden kontakt.** Zákazník má přidělenu osobu zodpovědnou za jeho projekty a řešení.
- **Globální služby.** Celosvětově zaručujeme konzistentní, vysoce kvalitní služby.
- **Důvěra.** S našimi klienty budujeme trvalou spolupráci.
- **Jistota.** Jsme součástí silné korporace.

3 Problematika DDoS útoků

DDoS útoky jsou v současné době považovány za jednu z nejagresivnějších forem počítačové kriminality na internetu. Při velmi nízkých nákladech na straně útočníka dokážou způsobit obětem útoků citelné finanční škody, které mohou dosáhnout stovek tisíc korun za hodinu.

Odborné studie společnosti Arbor Networks (WISR) z oblasti DDoS útoků dokládají následující fakta:

Průměrná velikost útoku za rok 2017: **~1 Gbps**

- **95,9%** útoků je **do 5 Gbps**
- **99,96%** útoků je do **50 Gbps**
- **Trvale roste počet útoků mezi 2 a 5 Gbps.**

Průměrná doba trvání DDoS útoku v roce 2017: **46 min**

- **96%** útoků **do 3 hod.**

Síla největšího útoku (03/2018): **~1,35 Tbps**

Nejčastěji se objevují útoky **volumetrické (76%)** a jejich počet nadále **roste.**

- Aplikační útoky tvoří **12%**.
- Útoky na infrastrukturní prvky, jako jsou load ballancery, firewally, IPS sondy i vlastní aplikační servery, tvoří **12%**.

K vytvoření **reflexních/amplifikačních** DDoS útoků se nejčastěji používají **DNS a NTP protokoly (77%)**

- **10%** z nich tvoří útoky **multi-vektorové,** které kombinují volumetrické útoky s aplikačními a infrastrukturními. **Počet** multi-vektorových útoků nadále **roste**.

Z těchto informací poměrně zřetelně vyplývá, že hrozba DDoS útoku je naprosto reálnou hrozbou současného kybernetického světa. DDoS útok může velmi zásadně ovlivnit chod celé řady organizací, závislých v menší či větší míře na komunikaci prostřednictvím internetu.

Mezi časté cíle DDoS útoků patří obchodní společnosti ze segmentu bankovnictví a finančních služeb, nebo elektronické komerce (typicky např. e-shopy). Hrozba DDoS útoků se ale týká celé řady dalších, které se z různých důvodů mohou stát atraktivním cílem hackerů.

Doposud nejběžněji používané metody ochrany proti kybernetickým útokům, jako je firewall či IPS, proti DDoS útokům bohužel neochrání.

Specializovaná zařízení, která si dokáží s DDoS útokem poradit na úrovni samotného připojení do internetu, jsou poměrně nákladná a jejich cena roste úměrně objemu provozu, který je během DDoS útoku nutno vyčistit. Tato zařízení poskytují velmi dobrou ochranu proti DDoS útokům různého typu. Jsou však zpravidla vhodným typem DDoS ochrany pouze pro útoky v řádu jednotek Gbps.

Proti masivním útokům hrubou silou tzv. volumetrickým, které se zpravidla pohybují v řádu desítek Gbps, je již nutno použít zcela odlišné řešení na úrovni poskytovatele. Poskytovatel má díky vysokým přenosovým kapacitám své vlastní sítě a vysokokapacitní platformě pro potlačování DDoS útoků, zcela jiné možnosti ochrany než jednotlivé společnosti. Nutno zdůraznit, že kromě vlastní technologie je pro úspěšné potlačování DDoS útoků klíčové její správné a především průběžně aktualizované nastavení. Pouze tímto způsobem je možno zajistit dlouhodobou účinnou ochranu, která je schopna reagovat na stále nové typy a formy DDoS útoků.

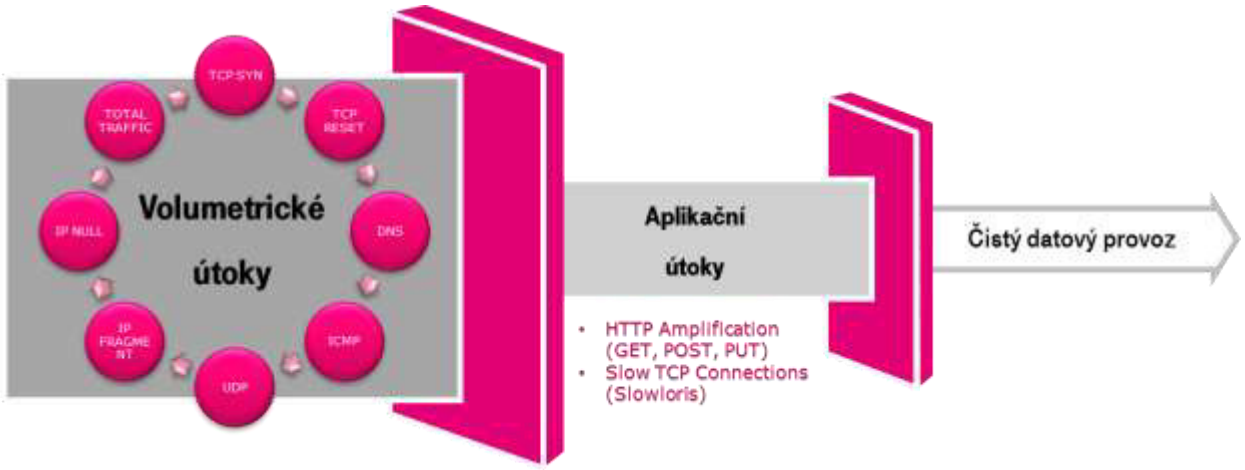
Nabídky jednotlivých poskytovatelů se mohou poměrně zásadně lišit. Při výběru toho správného je vhodné se neorientovat pouze na cenu nabízené služby, ale především na její reálnou a dlouhodobou účinnost.

4 Řešení od T-Mobile Czech Republic

Jako provozovatel vysokokapacitních sítí a technologických řešení, jejichž cílem je chránit síťový provoz a odhalit útoky, nabízí T-Mobile Czech Republic svým zákazníkům řadu komplexních opatření pro zabezpečení sítě.

Jedním z těchto opatření je ochrana sítí zákazníků před DDoS útoky. T-Mobile Czech Republic se problematikou řešení DDoS útoků zabývá již mnoho let. Za tuto dobu nasbíral celou řadu cenných zkušeností, které využil pro vytvoření služby ochrany proti DDoS útokům.

S cílem poskytnout zákazníkům skutečně komplexní ochranu proti DDoS útokům, navrhnul T-Mobile Czech Republic řešení, které se skládá ze dvou vzájemně provázaných ochranných vrstev: operátorské a In-Line. Každá z vrstev je zaměřena na jiný typ útoku a jako celek fungují jako velmi efektivní štít odolávající širokému spektru DDoS útoků. Princip vícevrstvé architektury řešení zachycuje obrázek níže.



Mezinárodní spolupráce v rámci skupiny Deutsche Telekom

T-Mobile Czech Republic, jako součást skupiny Deutsche Telekom, při potlačování DDoS útoků úzce spolupracuje s dalšími členy této skupiny.

V případě skutečně masivních útoků v řádech stovek Gbps, které není možné kapacitně zvládnout lokálními prostředky T-Mobile Czech Republic, a přesahují i kapacitní limity připojení T-Mobile Czech Republic do mezinárodních peeringových uzlů, se do řešení zapojuje rovněž systém DDoS ochrany mateřské společnosti Deutsche Telekom.

- Přestože k útokům, které nejsme schopni zvládnout lokálně, dochází jen velmi výjimečně, za dobu naší dlouholeté praxe jsme se již s několika takovými případy setkali a můžeme prohlásit, že jsme byli schopni je ve spolupráci se skupinou Deutsche Telekom úspěšně odrazit.

Pro případy, kdy síla útoku přesahuje možnosti DDoS ochrany celé skupiny Deutsche Telekom, máme připraveny krizové postupy, které umožní odblokovat komunikaci za cenu dočasného omezení provozu z některých částí Internetu. Pro tyto účely se používá technik selektivního blokování nežádoucího provozu (blackhole).

Ochrana prostředků zákazníka mimo síť T-Mobile

V případě, že zákazník potřebuje před DDoS útoky chránit např. webové servery, které jsou hostovány u jiného poskytovatele než T-Mobile, doporučujeme tyto přemístit do hostingových center T-Mobile a tyto chránit spolu s dalšími prostředky zákazníka službou DDoS ochrana od T-Mobile. Pouze tato varianta je schopna zajistit komplexní ochranu jak aplikační vrstvy, tak i kompletní přenosové infrastruktury, která připojuje prostředky zákazníka do prostředí Internetu.

Pokud migrace není z nějakého důvodu možná, doporučujeme primárně požádat o zajištění ochrany proti DDoS útokům přímo stávajícího poskytovatele hostingových služeb.

SOC

V případě, že monitorovací sondy na některé z vrstev ochrany zaznamenají potenciální DDoS útok, vygenerují alarm, na který neprodleně reaguje tým security specialistů SOC (Security Operation Center) zajišťujících pohotovost v režimu 24x7x365. Dle aktuální situace a průběžného vývoje DDoS útoku nasazuje SOC tým vhodná protiopatření, která jsou předem schválena zákazníkem.

On-line uživatelské rozhraní (pouze varianta Gold)

Zákazník má možnost sledovat celý průběh potlačování DDoS útoku v reálném čase prostřednictvím webového uživatelského rozhraní. To mu umožňuje včas a efektivně komunikovat se SOC týmem, vzájemně se koordinovat a zvyšovat tak účinnost DDoS ochrany.

Odbornost a zkušenosti

T-Mobile Czech Republic disponuje týmem security specialistů, kteří jsou připraveni u zákazníka provést analýzu současného stavu ochrany proti kybernetickým útokům, konzultovat vhodná ochranná opatření, následně je implementovat a průběžně je přizpůsobovat dynamicky se měnícím okolnostem.

ATLAS – Threat Intelligence

T-Mobile Czech Republic v rámci operátorské varianty služby ochrany proti DDoS útokům využívá unikátní globální systém pro analýzu a sledování hrozeb na internetu – ATLAS od společnosti Arbor Networks.

Tento systém je založen na sdílení nejnovějších informací o hrozícím nebezpečí DDoS útoků od provozovatelů sítí po celém světě. V současné době ATLAS zahrnuje více než 330 poskytovatelů internetu, mezi které patří i T-Mobile Czech Republic.

Zúčastnění ISP průběžně dodávají do systému ATLAS anonymně statistiky síťového provozu a útoků, které jsou využity k provedení analýzy hrozeb z botnetů, malware a DDoS útoků.

Zjištěné poznatky slouží jako zdroj pro tvorbu pravidel k identifikaci nejnovějších typů útoků. Nová pravidla jsou následně distribuována formou aktualizací na technologické platformy jednotlivých operátorů. Významně se tak zvyšují jejich ochranné schopnosti proti nejnovějším DDoS útokům.

Doporučení:

- Zákazníkům, kteří ještě DDoS ochranu nemají, doporučujeme zřídit minimálně 1. vrstvu, která je schopna ochránit proti celé řadě aplikačních a pomalých útoků. Tato vrstva je schopna ochránit rovněž proti volumetrickým útokům v řádech jednotek Gbps. V nabídce T-Mobile se jedná o službu DDoS ochrany ve variantě In-Line.
- Pro ty, kteří již mají 1. vrstvu ochrany vybudovánu, doporučujeme nasazení DDoS ochrany na operátorské úrovni. Tato vrstva je schopna ochránit proti útokům v řádech stovek Gbps. V nabídce T-Mobile se jedná o službu DDoS ochrany na operátorské úrovni. Nasazení 2. vrstvé DDoS ochrany je velmi robustní řešení, které poskytuje zákazníkům ochranu před naprostou většinou DDoS útoků a minimalizuje riziko nedostupnosti chráněných komunikačních prostředků zákazníka.

T-Mobile je připraven se zákazníkem blíže diskutovat jeho konkrétní požadavky a navrhnout nejlepší možné řešení, které bude optimálně vyladěné dle jeho aktuálních potřeb.

Výhody řešení od T-Mobile Czech Republic

- Použití vícevrstvé architektury a špičkových technologií pro zajištění komplexní ochrany
- Operátorská vrstva proti volumetrickým DDoS útokům
- In-Line vrstva proti aplikačním DDoS útokům
- Technická a provozní podpora zajišťovaná operátory SOC v režimu 24×7×365
- Rychlá detekce a potlačení útoku garantovaná parametry SLA
- Přizpůsobení služby skutečným potřebám a možnostem zákazníka
- Několik funkčních variant služby
- Několik fakturačních modelů
- Vysoká kompetence a dlouholetá zkušenost
- Garance dlouhodobé stability a dalšího rozvoje služby
- Schopnost efektivně čelit největším a nejnovějším DDoS útokům díky aktivní mezinárodní spolupráci

5 Nabídka - DDoS ochrana TMCZ - operátorská vrstva

Předmětem této nabídky je operátorská vrstva DDoS ochrany TMCZ.

V tomto odstavci jsou popsány základní komponenty služby, funkční varianty, provozní fáze stejně jako detaily služby jako takové, ochranný plán, SLA a detail nabízeného řešení.

Operátorská vrstva DDoS ochrany je v principu postavena na průběžném monitoringu vzorku datových paketů směřujících do IP adresního rozsahu, který zákazník určí. Monitorován je jak datový provoz přicházející do sítě T-Mobile Czech Republic z internetu, tak i provoz pocházející z vybraných segmentů vlastní sítě T-Mobile Czech Republic. Operátorská vrstva DDoS ochrany je zaměřena především na potlačení útoků vedených hrubou silou tzv. volumetrické útoky.

5.1 Základní komponenty

Operátorská vrstva DDoS ochrany sestává ze dvou komponent: Monitoringu a Ochrany

Komponenta	Detail
DDoS Monitoring	Monitoring (Flow-based Monitoring), který běží na úrovni sítě T-Mobile Czech Republic, spočívá v analýze vzorků datových toků shromážděných od okrajových směrovačů sítě T-Mobile Czech Republic. Náš systém analyzuje příchozí provoz, který je přesměrován do vaší sítě prostřednictvím sítě T-Mobile Czech Republic i přes naše propojení se sítěmi jiných operátorů. Současně používáme tři metody pro detekci DDoS útoku: • analýza zneužití vybraných síťových protokolů • analýza vzorků provozu • signatury útoků získané z databáze ATLAS V případě detekce chybové události, nebo překročení hranice datového toku, systém automaticky pošle oznámení a zahájí proces analýzy a klasifikace, který následně dokončují pracovníci security dohledového operačního centra T-Mobile Czech Republic (SOC). Monitorovací služba dokáže odhalit útoky na druhé až čtvrté vrstvě (L2-4) ISO/OSI modelu a částečně i na vrstvě aplikační (L7).
DDoS Ochrana	DDoS Ochrana je služba, která zajišťuje aktivní ochranu a zahájí protiopatření, které čistí provoz a zmírní dopady útoku. Díky vysokokapacitní síti a specializované DDoS technologii, může T-Mobile Czech Republic poskytnout vysokou účinnost čištění, filtrování a potlačení nežádoucích datových toků. Tato služba je spuštěna v souladu s dohodnutým **plánem ochrany**, který definuje rozsah vlastních činností a postupů, které mají být použity za specifických okolností. V případě hrozby útoku je veškerý příchozí provoz prostřednictvím sítě T-Mobile Czech Republic přesměrován na Threat Management System (TMS), který analyzuje a identifikuje legitimní provoz a odstraní falešný. Legitimní komunikace je pak směrována zpět k zákazníkovi.

5.2 Funkční varianty

Operátorská vrstva DDoS ochrany je k dispozici ve 3 funkčních variantách: Bronze, Silver a Gold

Funkce / parametr	Bronze	Silver	Gold
DDoS Monitoring	+	-	+
DDoS Ochrana	-	+	+
Počet konzultačních hodin určených pro stanovení specializovaného Plánu Ochrany	2	6	8
Neomezený počet ochranných akcí	-	+	+
Nezávislost poplatku na velikosti DDoS útoku	-	+	+
Service Level Agreement (SLA)	+	+	+
Dostupnost techniků Centra síťového provozu T-Mobile Czech Republic v režimu 24×7×365	+	+	+

Monitoring a detekce útoků na L3 a L4	+	-	+
Proaktivní ohlašování událostí (mobilní sms a email)	+	-	+
On-line uživatelské rozhraní	-	-	+

Varianta **Bronze** je vhodná pro organizace, které potřebují zajistit detekci DDoS útoků a proaktivní informování v případě útoku. Tato varianta nezahrnuje aktivní ochranu. Tuto je možno si doplatit. Doplatek za aktivní ochranu se je kalkulován za každý započatý den čištění provozu.

Varianta **Silver** je vhodná pro organizace, které již mají své vlastní řešení detekce DDoS útoku instalované a vyžadují aktivní ochranu v případě útoku bez ohledu na počet či délku útoků.

Varianta **Gold** je určena organizacím, které potřebují kompletní služby, zahrnující kontrolu, přístup k analýze datových toků a krátkou dobu odezvy při nasazení proaktivní ochrany.

5.3 Provozní fáze

Služba samotná v sobě zahrnuje 3 provozní fáze (etapy):

Analýza situace a parametrizace řízení

- do 14 dnů od podpisu smlouvy.

Implementace a testy dohodnutých postupů

- do 7 dnů od jejich schválení.

Údržba plánu ochrany po dobu trvání smlouvy

- T-Mobile Czech Republic umožňuje zákazníkům bezplatně ověřit postupy dvakrát v průběhu 12 měsíců.

5.4 Popis služby

V rámci Služby poskytovatel monitoruje datový provoz na lince zákazníka. Provoz je monitorován pomocí technologie umístěné v páteřní síti poskytovatele. Služba spočívá v detekci a ochraně před internetovými útoky typu DDoS.

Detekce útoku

Použitá Technologie umožňuje detekovat většinu známých Volumetrických útoků, některé Aplikační útoky a některé Pomalé útoky, přičemž se vždy vychází ze současného stavu a úrovně vývoje komunikačních a IT technologií.

Ochrana před útokem

Použitá Technologie umožňuje v případě útoku na Chráněné cíle uvedené ve Specifikaci služeb na základě znalosti datového provozu Zákazníka odfiltrovat podstatnou část škodlivého Provozu - útoku DDoS.

Standardní provoz Zákazníka

Technologie získává znalosti datového provozu Zákazníka (učí se) na „standardním provozu Zákazníka“. Během Provozu, kdy neprobíhá útok DDoS, Technologie analyzuje pouze hlavičky datových paketů, obsah paketu - data Zákazníka tedy nejsou součástí analýzy.

Při zahájení poskytování Služby a po každé podstatné změně struktury Provozu zákazníka, potřebuje Technologie alespoň tři týdny na získání potřebných znalostí o novém profilu standardního Provozu zákazníka. V tomto období zavedení Služby je Technologie méně citlivá pro detekci útoku DDoS.

Security Operation Center

Technologie v případě detekce útoku nebo podezření na útok DDoS poskytne informaci Security Operation Center (SOC) - dohledovému týmu poskytovatele.

SOC analyzuje výstrahy Technologie a na základě dohody se zákazníkem zahájí nasazení protiopatření, dokud není Provoz vyčištěn.

Schválení nasazení protiopatření

V případě, že SOC vyhodnotí údaje z Technologie jako podezření na volumetrický útok DDoS, bez zbytečného prodlení telefonicky kontaktuje Zákazníkem uvedené osoby ve stanoveném pořadí prostřednictvím telefonního čísla uvedeného ve

Specifikaci služby a určeného k autorizaci nasazení protiopatření (v tomto dokumentu jako „**autorizační kontakt**“). Zákazník bere na vědomí a souhlasí s tím, že tyto hovory jsou poskytovatelem nahrávány. Pokud se SOC nedovolá žádnému z autorizačních kontaktů, pak všem třem pošle e-mail.

Poskytovatel následně postupuje v souladu s pokyny zákazníka, které obdržel prostřednictvím autorizačního kontaktu. V případě souhlasu autorizačního kontaktu zahájí poskytovatel bez zbytečného prodlení nasazení protiopatření. V případě, že autorizační kontakt neudělí souhlas s protiopatřením, nebudou ze strany poskytovatele činěny žádné úkony a tato skutečnost bude zaznamenána do Service Desku poskytovatele.

V případě, že zákazník vyhodnotí alarmy týkající se aplikační infrastruktury jako podezření na Aplikační útok, Autorizační kontakt to oznámí na SOC poskytovatele, který nasadí protiopatření na základě jeho požadavku. Podobně se postupuje v případě Pomalého útoku.

Protiopatření

V rámci Protiopatření a s ohledem na Chráněné cíle uvedené zákazníkem ve Specifikaci služby poskytovatel přesměruje Provoz zákazníka nebo jeho část do zařízení, které odstraní Provoz považovaný za škodlivý. Nastavení Protiopatření primárně zohledňuje zprovoznění Chráněných cílů dle Specifikace služeb. Vyčištěný Provoz je doručen k Chráněnému cíli.

V případě vícenásobného útoku, kdy útoky běží paralelně, bude výše uvedený proces Protiopatření opakován, dokud se nevyčistí všechny útoky a nebude obnoven běžný Provoz.

Ukončení nasazení Protiopatření

V případě, že SOC vyhodnotí údaje z Technologie jako ukončení útoku DDoS, oznámí to autorizačnímu kontaktu zákazníka a ukončí nasazení Protiopatření.

5.5 Ochranný plán – specifikace vybraných akcí

Předdefinovaný rozsah ochrany zahrnuje následující kroky.

Služba	Rozsah činností
DDoS Monitoring	• Sledování příchozího provozu na L3 a L4 v režimu 24/7. • Definice zákaznického detekčního modelu pro Managed Object. • Zajištění proaktivního datového provozu pomocí sms/email upozornění na události. • Smluvně zaručená doba pro doručení oznámení v nejvyšší úrovni hrozeb od okamžiku detekce. • Přístup k NIP (Network Intelligence Portal), který poskytuje report a statistiky příchozích datových toků a historii zaznamenaných událostí. (pouze u varianty Gold)

DDoS Ochrana	• Analýza a klasifikace síťové události zaznamenané monitorovacím systémem, oznamuje klientovi typ události a domluvených ochranných opatření pro nejnebezpečnější události.
	• Přesměrování datového provozu do Traffic Mitigation Systém (TMS).
	• Sada dalších ochranných postupů neomezeně zahrnuje:
	  ○ blokování IP adresy na základě doporučení z monitorovacího systému,
	  ○ omezení vysílání rozsahů sítí (pro klienty s BGP routingem)
	  ○ blokování zdrojové a cílové adresy,
	  ○ filtrování/zakázání datového provozu pro vybrané protokoly (UDP)
	  ○ Navýšení šířky pásma pro připojení k Internetu [1].

[1] Dočasné zvýšení šířky pásma je předmětem technické proveditelnosti takového opatření provozovatelem síťové infrastruktury. Příprava síťové infrastruktury pro toto opatření může vyžadovat linku a / nebo infrastrukturu modernizovat a podléhá dodatečným nákladům.

5.6 SLA (Service Level Agreement)

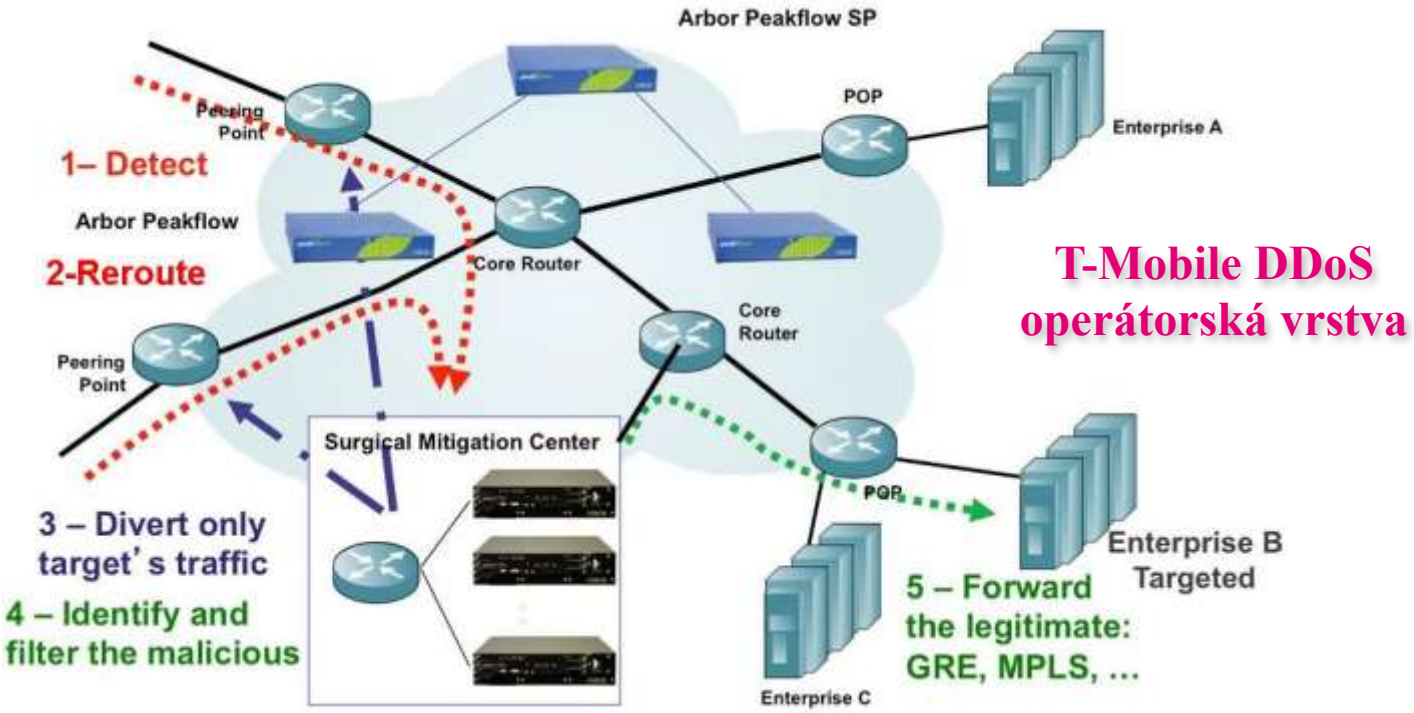
Služba je poskytována nepřetržitě všechny dny v roce 24 hodin denně. Parametry SLA zachycuje tabulka níže.

SLA parametr	Bronze	Silver	Gold
Dostupnost Monitoringu	99.9%	-	99.9%
Dostupnost Ochrany	-	99.99%	99.99%
Reakční doba pro oznámení potenciálního útoku	15 minut	-	15 minut
Reakční doba pro aktivaci ochrany (nasazení protiopatření)	-	do 30 minut	do 15 minut

6 Popis nabízeného řešení

Nabízené řešení se je založeno na využití ochranného DDoS štítu, vybudovaném T-Mobile na technologii ARBOR.

Schéma operátorské vrstvy T-Mobile DDoS ochrany zachycuje obrázek níže.



V peeringových bodech sítě T-Mobile jsou umístěny monitorovací sondy (Arbor Peakflow SP), které monitorují procházející provoz s cílem detekovat DDoS útoky směřující na chráněné objekty zákazníků využívajících operátorskou vrstvu služby T-Mobile DDoS Ochrana.

V případě, že sondy detekují DDoS útok, posílají varovný signál specialistům SOCu, kteří jsou schopni přesměrovat DDoS útok do mitigačního (čistícího) centra (na obrázku výše červená přerušovaná čára). Vyčištěný provoz je z mitigačního centra následně směrován do sítě zákazníka (na obrázku výše zelená přerušovaná čára).

6.1 Nabízené varianty služby

Základem této nabídky operátorské vrstvy DDoS ochrany je funkční **varianta Gold**, která obsahuje:

- Monitoring (Flow based)
- Proaktivní upozornění na detekované události
- Technickou podporu 24×7×365
- On-line uživatelské rozhraní, přes které je možno sledovat průběh mitigace DDoS útoku a které rovněž umožňuje získat zákazníkovi on-line reporty ve formátu pdf.

Vzhledem k požadavku zákazníka na expresní nasazení, které sebou přináší rizika zvýšeného počtu false-positive alarmů je služba nabídnuta ve variantě „Gold **Unlimited**“, **u** které **c**ena za službu není závislá na počtu DDoS útoků, ani na jejich velikosti.

6.2 Předmět nabídky

Předmětem nabídky je jednovrstvá DDoS ochrana (operátorská vrstva) následující konektivity zákazníka:

1. IP transit **4 Gbps** (GN111403), Na Vápence 14/915, Praha 3
2. IP transit **4 Gbps** (GN111404), Sazečská 598/7, Praha 10 - Malešice

V případě záplavového (volumetrického) útoku na Internet Access T-Mobile vyšle monitorovací část operátorské vrstvy DDoS ochrany alarm na SOC T-Mobile.

Pokud bude zákazníkem dopředu povoleno aplikovat čistící protiopatření, dojde k aktivaci signalizace pro přesměrování provozu do čistícího centra. Pokud povolení k přesměrování nebude zákazníkem uděleno dopředu, dojde ke komunikaci mezi SOC T-Mobile a pověřenou osobou na straně zákazníka.

Řešení počítá s tím, že DDoS útok může být nahlášen zákazníkem na základě jeho vlastní detekce na in-line vrstvě ochrany. V takovém případě T-Mobile SOC převezme požadavek zákazníka a aktivuje operátorskou vrstvu TMCZ DDoS ochrany.

In-line vrstva DDoS ochrany není předmětem nabídky (zákazník si řeší sám).

7 Cenová nabídka

Ceny jsou uvedeny bez DPH.

Ceny jsou platné pro využití služby v následujícím období:

- 13. až 27. května 2019

7.1 Zřizovací poplatek

Zřizovací poplatek pokrývá

- Zřízení služby
- Několik iteračních cyklů pro odladění konfigurace

Hodnota zřizovacího poplatku činí **89 000 Kč** a platí se pouze jednou při zřízení služby.

7.2 Platba za službu

Tabulka níže obsahuje ceny za službu pro nabízenou variantu a požadované období.

Varianta	Fakturační položka	13. až 27. května 2019
Gold Unlimited	Cena za službu	236 890 Kč

8 Implementační plán

Tabulka níže zobrazuje implementační plán, který byl vytvořen na základě požadavku zákazníka na expresní zřízení služby. Tento plán je potřeba vnímat jako optimistickou variantu, která je postavena na předpokladu hladké součinnosti obou stran a absenci jakékoliv časové rezervy.

Aktivita	Termín	Datum	Poznámka
Dodání vyplněného zadávacího dokumentu zákazníkem (Tabulka chráněných cílů)	T0	3. 5. 2019	Zákazník poskytne TMCZ veškeré potřebné technické informace (rozsahy chráněných cílů – ip adresy, protokoly, služby, kontaktní matice, eskalační kontakty…)
Analýza požadavků a příprava konfigurace	T0 + 3 dny	6. 5. 2019	V rámci zřízení služby na straně TMCZ
Nastavení bezpečnostních politik v systému, základní provozní testy	T0 + 4 dny	7. 5. 2019	V rámci zřízení služby na straně TMCZ
Postupné odladění konfigurace. Vytvoření dokumentace k danému nastavení.	T0 + 7 dnů	10. 5. 2019	Na základě průběžné analýzy provozních charakteristik chování chráněných služeb bude v rámci několika iterací odladěna konfigurace systému tak, aby se výrazně snížilo riziko výskytu false-positive alarmů.
Provedení komunikačních testů	T0 + 7 dnů	10. 5. 2019	Vyžaduje další součinnost ze strany zákazníka.
Spuštění služby	T0 + 10 dnů	13. 5. 2019	Služba je schopna plnohodnotně ochránit specifikované cíle zákazníka.

9 Slovník použitých pojmů:

Managed Object

Zákaznická síť, která je monitorována a/nebo chráněna je definována jako Service Availability Point (SAP) a přiřazeným rozsahem IP adres

Clean Traffic

Příchozí datový tok, který je směrován do zákaznické sítě během standardního provozu.

Commited Clean Traffic Plan (CCTP)

Definuje velikost příchozího datového toku směrovaného do sítě zákazníka, který je chráněn službou proti DDoS útokům. Hodnota CCTP a její možné překročení se stanoví pomocí metody 95. percentilu na základě podmínek stanovených v technické specifikaci služby. Prvotně schválená hodnota CCTP je uvedena v objednávce (specifikaci služby).

Plán Ochrany

Sada postupů plánu ochrany dohodnutých mezi Provozovatelem a Účastníkem v příloze k technické specifikaci.

Škodlivý provoz

Internetový provoz generovaný a směrovaný do sítě Účastníka a na jeho IP adresy, který narušuje legitimní provoz zařízení Účastníka nebo jakéhokoliv jiného zařízení na konci u odběratele.

SOC - Security Operation Center

Specializovaný tým poskytovatele, zajišťující technickou podporu služby v režimu 24x7x365

Denial of Service (DoS)

Česky odmítnutí služby - je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a pádu nebo minimálně nefunkčnosti a nedostupnosti pro ostatní uživatele.

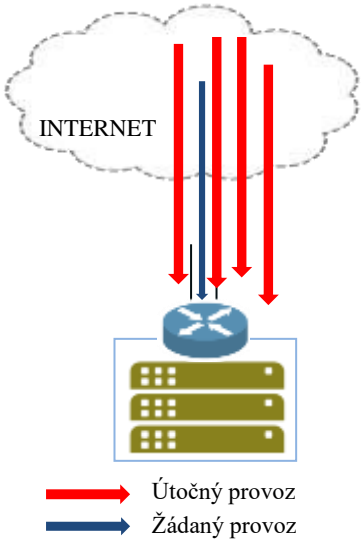
Během útoku je čistý, legitimní provoz potlačen obrovským počtem požadavků, který generují útočící stroje. Proto hlavním smyslem obrany je ochránit legitimní provoz a zajistit jeho doručení k cíli, ale přitom odstranit datový tok útočníků, kteří přetěžují linky a cílové počítače – servery.

Cíle takového útoku jsou v zásadě dva:

- Vnucení opakovaného resetu cílového počítače
- Narušení komunikace mezi serverem a obětí tak, aby jejich komunikace byla buď zcela nemožná, nebo alespoň velmi pomalá.

Distributed Denial of Service (DDoS)

bývá konstruován tak, že jeho cílem je v jednom čase útok velkého počtu koncových počítačů na jednu konkrétní službu. Existují také softwarové principy, které umožňují distribuované útoky na více služeb v jednom čase (a nikoliv jen na jednu). I proti těmto typům útoků existují možnosti řešení.



Typicky je objem škodlivého útočného provozu mnohonásobně větší než provozu žádaného (10× - 100×).

10 Odpovědnost T-Mobile Czech Republic

Jako součást služby **DDoS ochrana** zaručuje včasné provádění ochranných postupů a zajišťuje Váš přístup k vědomostem a dovednostem síťových inženýrů T-Mobile Czech Republic. Ačkoliv se T-Mobile Czech Republic zavazuje vynaložit přiměřené úsilí na omezení dopadu DDoS útoků, kvůli složité celkové povaze a špatné předvídatelnosti rozsahu takových útoků T-Mobile Czech Republic nemůže zaručit, že Plán Ochrany nebo aplikovaných opatření jsou vždy a bezpodmínečně plně efektivní. T-Mobile Czech Republic nenese odpovědnost za případné škody, které jste utrpěli v důsledku jakéhokoli útoku DDoS nebo jakýmkoliv opatřením přijatém T-Mobile Czech Republic pro ochranu příchozího provozu do Vaší sítě

11 Závěrečná ustanovení

11.1 Platnost nabídky

Tato nabídka má platnost po dobu 30 kalendářních dnů ode dne jejího vydání. Po uplynutí této lhůty, musí být návrh aktualizován.

11.2 Závěr

Ve společnosti T-Mobile Czech Republic jsme připraveni s vámi spolupracovat tak, abychom Vám poskytli nejlepší možné řešení, které bude optimálně vyladěné dle Vašich aktuálních potřeb a umožnilo budoucí růst Vaší firmy. Prosím, neváhejte nás kontaktovat pro jakékoliv vysvětlení nebo doporučení týkající se tohoto návrhu. Rádi Vám také poradíme alternativní řešení, které Vám můžeme nabídnout.