Smlouva o poskytování služeb č. 23/600/0429

Níže uvedeného dne, měsíce a roku byla mezi smluvními stranami uzavřena podle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., Občanský zákoník, ve znění pozdějších předpisů (dále jen „OZ"), smlouva níže uvedeného znění na akci

„Operátorská DDOS ochrana"

Smluvní strany

T-Mobile Czech Republic a.s.

Se sídlem: Tomíčkova 2144/1, 148 00 Praha 4
IČ: 64949681
DIČ: CZ64949681

Zastoupená: [redacted]
Spojení:
ID datové schránky: ygwch5i

Bankovní spojení: Komerční banka, a.s., Praha 2
Číslo účtu: 19-2271190247/0100
Adresa pro doručování korespondence: Tomíčkova 2144/1, 148 00 Praha 4

Společnost je zapsána v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl B, vložka 3787

(dále jen „poskytovatel")
a

Česká republika – Generální ředitelství cel

Se sídlem: Budějovická 7, 140 96 Praha 4
Jednající: [redacted]

Spojení: [redacted]

IČ: 71214
DIČ: CZ71214011
Bankovní spojení: ČNB Praha 1
Číslo účtu: 1020011/0710
Adresa pro doručování korespondence: Budějovická 7, 140 96 Praha 4

(dále jen **„objednatel")**

Smluvní strany prohlašují, že údaje uvedené v tomto odstavci jsou v souladu s platnými zápisy v obchodním, popř. jiném rejstříku.

[redacted]

Smluvní strany se zavazují, že změny ve výše uvedených údajích oznámí bez prodlení druhé straně (případně upozorní na důsledky z toho vyplývající). Pokud tak včas neučiní, uhradí druhé straně veškerou škodu, která jí tímto opomenutím vznikla.

Objednatel a poskytovatel též společně jako „**smluvní strany**“ uzavírají tuto smlouvu o poskytování služeb s názvem „**Operátorská DDOS ochrana**“ (dále jen „**smlouva**“).

Smluvní strany se dohodly, že se jejich závazkový vztah řídí OZ s použitím příslušných ustanovení zákona č.121/2000 Sb., ve znění pozdějších předpisů (dále jen ”autorský zákon”) a zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění.

I. Předmět smlouvy

Předmětem smlouvy je závazek:

A. poskytovatele

Poskytnout služby DDOS ochrany na operátorské vrstvě ve variantě služby Gold unlimited. Služba DDoS ochrana bude ze strany poskytovatele zajišťovat neustálou ochranu a bude minimalizovat negativní dopady útoků díky proaktivní kontrole a realizaci technických a procesních protiopatření pro rychlé snížení rizik. Zkušení odborníci poskytovatele v bezpečnostním centru (SOC) v úzké spolupráci s objednatelem budou blokovat závadný tok dat a propouštět dále jen bezpečný obsah. Detailní popis a specifikace služby jsou uvedeny v dokumentech Popis služby, SLA a eskalační matice (příloha č. 3 této smlouvy) a Podmínky poskytování Služby DDoS ochrana (příloha č. 4 této smlouvy), kterými se tato služba řídí.

(Dále jen „**služba**“ nebo „služby“)

B . objednatele

v souladu s ustanovením smlouvy službu převzít a za řádnou a včasnou realizaci služby poskytovateli zaplatit dle této smlouvy.

II. Povinnosti smluvních stran

2.1. Povinnosti poskytovatele:

a) Poskytovatel je povinen poskytovat řádně a včas službu dle této smlouvy bez faktických a právních vad.

b) Poskytovatel je povinen zajistit ochranu dokumentů a dokumentace, v datové anebo listinné podobě, které od objednatele obdržel pro potřebu plnění předmětu smlouvy nebo které vytvořil v rámci plnění předmětu smlouvy. Poskytovatel je povinen takové dokumenty a dokumentaci po ukončení smlouvy objednateli prokazatelně předat, nebo je se souhlasem objednatele prokazatelně zlikvidovat či je vést a prokazatelně evidovat. Poskytovatel je povinen zajistit, že takové dokumenty a dokumentace nebudou poskytnuty třetí straně nebo užity ve prospěch třetí strany.

c) Veškeré podklady, které byly objednavatelem poskytovateli předány, zůstávají v jeho vlastnictví a poskytovatel za ně odpovídá od okamžiku jejich převzetí jako skladovatel a je povinen je vrátit objednavateli po splnění svého závazku (ukončení služby), pokud není ujednáno jinak.

d) Poskytovatel je povinen bez zbytečného odkladu oznámit objednateli všechny okolnosti, které zjistil při zařizování záležitostí, a které mohou mít vliv na změnu pokynů nebo zájmů objednatele, dále je povinen upozornit objednatele na nevhodnost předaných dokumentací, případně nevhodnost pokynů objednatele.

e) Poskytovatel je povinen zachovávat mlčenlivost o všech záležitostech, o nichž se dozvěděl v souvislosti s prováděním předmětných činností.

f) Poskytovatel po dobu plnění poskytne oprávněným osobám objednatele přístup do webového rozhraní, kde oprávněné osoby objednatele mohou sledovat průběh potlačení DDoS útoků, což umožňuje včas efektivně koordinovat a komunikovat kroky se SOC týmem poskytovatele a zvyšovat účinnost DDoS ochrany.

g) Poskytovatel je povinen zajistit plnění povinností ze zákona o kybernetické bezpečnosti uvedené v Příloze č. 5 této smlouvy.

2.2. Zaměstnanci poskytovatele podílející se na plnění předmětu smlouvy jsou povinni:

a) zachovávat mlčenlivost ve vztahu k informacím, se kterými jakýmkoliv způsobem přijdou do styku při plnění předmětu smlouvy,

b) zdržet se pokusů o neoprávněný fyzický přístup do objektů anebo prostor objektů objednatele, které nesouvisejí s plněním předmětu smlouvy,

c) zdržet se pokusů o neoprávněný logický přístup k objektům Informačního systému Celní správy České republiky (dále jen „ISCS“), které nesouvisejí s plněním předmětu smlouvy,

d) zdržet se jakýchkoliv aktivit v objektech objednatele, které nesouvisejí s plněním předmětu smlouvy, pokud nejsou vázání jiným smluvním závazkem s objednatelem.

2.3. Poskytovatel služby může pověřit jeho provedením jinou osobu (subdodavatele). V tomto případě má poskytovatel odpovědnost jako by službu prováděl sám. Poskytovatel má povinnost neprodleně informovat objednatele o tom, že pověřil poskytováním služby nebo jejich části subdodavatele.

2.4. Pracovníci poskytovatele nebudou kromě odpovědné osoby objednatele navazovat žádné další pracovní kontakty s jinými pracovníky objednatele pro řešení předmětu této smlouvy ani tyto jiné pracovníky seznamovat se stavem řešení projektu bez předchozího rozhodnutí oprávněné osoby na straně objednatele.

2.5. Povinnosti objednatele:

a) převzít řádně poskytnutou službu ve smyslu této smlouvy a podepsat příslušné dokumenty v souladu s ustanoveními této smlouvy,

b) dodržovat provozní podmínky užívání prokazatelně dodané poskytovatelem a písemná doporučení poskytovatele, zaslaná elektronicky – cestou datové schránky s následujícím parametrem: ID datové schránky „Generální ředitelství cel“: **7puaa4c**

c) realizovat příslušnou součinnost v rozsahu této smlouvy,

d) realizovat případnou další součinnost odsouhlasenou zástupci smluvních stran.

2.6. Pokud objednatel neposkytne poskytovateli řádně a včas veškerou součinnost vyplývající z této smlouvy, má poskytovatel v takovém případě právo posunout termín poskytování služby o dobu trvající nejméně počet dní, po které poskytovatel nemohl řádně smlouvu plnit.

2.7. Vyžaduje-li plnění závazků poskytovatele dle této smlouvy uskutečnění právních či jiných úkonů jménem objednatele, je objednatel povinen vystavit včas poskytovateli písemně potřebnou plnou moc.

2.8. Objednatel je oprávněn neprodleně po ukončení poskytování služby odebrat fyzická a logická přístupová práva, která byla poskytnuta zaměstnancům poskytovatele podílejících se na plnění smlouvy, včetně práv privilegovaných a práv vzdáleného přístupu do ISCS.

2.9. Objednatel je oprávněn schvalovat změny zaměstnanců poskytovatele podílejících se na díle, a to formou číslovaného dodatku smlouvy, prvotní seznam takových zaměstnanců je uveden ve čl. XII této smlouvy. Pro doplňování dodatků platí pravidla uvedená v čl. XVI. – Závěrečná ustanovení.

2.10. Objednatel je oprávněn při porušení nebo nedodržení bezpečnostních podmínek uvedených v odst. 1 až 2 tohoto článku uplatnit vůči poskytovateli sankce podle čl. IX. – Smluvní sankce podle této smlouvy.

2.11. Zaměstnanci objednatele určení podle odst. 9 tohoto článku jsou uvedeni v čl. XII. této smlouvy.

2.12. Zaměstnancem poskytovatele odpovědným za plnění bezpečnostních podmínek specifikovaných objednatelem je [redacted]

2.13. Zaměstnancem objednatele odpovědným za dohled nad plněním bezpečnostních podmínek uvedených v odst. 1 až 2 tohoto článku specifikovaných objednatelem a plněných poskytovatelem je [redacted]

III. Způsob poskytování služeb

3.1. Poskytovatel bude poskytovat službu dle podmínek stanovených v této smlouvě, zejména v souladu s Podmínkami poskytování Služby DDoS Ochrana (příloha č. 4) a Popisem služby, SLA a eskalační matice (příloha č. 3). O zahájení poskytování služby v souladu s touto smlouvou se vyhotoví „Předávací protokol“ (příloha č. 1), který bude podepsán oprávněnými osobami objednatele a poskytovatele uvedenými ve článku XII. této smlouvy. V případě rozporu mají dokumenty mezi sebou přednost v tomto pořadí: 1. Podmínky poskytování Služby DDoS Ochrana (Příloha č. 4) 2. Popis služby, SLA a eskalační matice (Příloha č. 3), a 3. ustanovení této smlouvy.

IV. Převzetí služeb

4.1. Místem převzetí služeb je sídlo objednatele, tj. Budějovická 7, 140 96 Praha 4.

V. Místo poskytování služeb

5.1. Místem poskytování služeb je Primární informační centrum GŘC (PIC) umístěné v sídle objednatele, tj. Budějovická 7, 140 96 Praha 4 a Záložní informační centrum GŘC umístěné v SP CSS, Na Vápence 915/14, 130 00 Praha 3 Žižkov. S ohledem na typ a charakter poskytované služby může být služba poskytována rovněž v lokalitách poskytovatele, resp. vzdáleným přístupem poskytovatele k zařízením a síti objednatele.

VI. Cena služeb

6.1. Cena za předmět této smlouvy podle článku I. je dohodnuta oběma stranami ve výši 83.250 Kč (slovy: osmdesát tři tisíc dvě stě padesát korun českých) měsíčně. Ceny uvedené ve smlouvě neobsahují DPH, které bude stanoveno na základě platných právních předpisů v den uskutečnění zdanitelného plnění.

6.2. Celková cena za poskytovatelem dodané a objednatelem převzaté služby za celou dobu trvání této smlouvy, resp. dobu platnosti této smlouvy, nepřekročí částku bez DPH:

1.998.000 Kč

(slovy: jeden milion devět set devadesát osm tisíc korun českých),

to je s 21 % DPH ve výši **419.580,- Kč celkem**

2.417.580,- Kč

(slovy: dva miliony čtyři sta sedmnáct tisíc pět set osmdesát korun českých).

6.3. Celková cena je stanovena jako cena nejvýše přípustná a konečná. Cena za poskytování služby zahrnuje veškeré související náklady poskytovatele, např. náklady na dopravu, pojištění, předání a záruční servis. Celková cena může být změněna pouze v souvislosti se změnou daně z přidané hodnoty dle příslušných právních předpisů.

VII. Platební podmínky

7.1. Poskytovatel bude fakturovat cenu za službu měsíčně. Částka je stanovena v čl. VI. bod 6.1. této smlouvy.

7.2. Daňový doklad (faktura) musí obsahovat všechny náležitosti daňového dokladu podle § 435 OZ, podle § 7 zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), podle zákona č. 563/1991 Sb. o účetnictví, ve znění pozdějších předpisů a podle § 21 a § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a odkaz na tuto smlouvu a identifikaci zástupce poskytovatele. Faktura včetně příslušných výkazů práce musí být zaslána elektronicky - cestou datové schránky s následujícím parametrem: ID datové schránky „Generální ředitelství cel": **7puaa4c**

7.3. Faktura musí obsahovat evidenční číslo této Smlouvy a u první faktury bude přiložena kopie předávacího protokolu podepsaného oběma smluvními stranami. Pokud faktura nebude obsahovat stanovené náležitosti dle této Smlouvy, nebo v ní nebudou správně uvedené údaje, je objednatel oprávněn vrátit ji ve lhůtě 10 (slovy: deseti) pracovních dnů od jejího obdržení poskytovateli s uvedením chybějících náležitostí nebo nesprávných údajů. V takovém případě bude faktura poskytovatelem opravena a nová lhůta splatnosti začne plynout doručením opravené faktury zpět objednateli. V případě,

že objednatel fakturu vrátí, přestože faktura je správná a předepsané náležitosti obsahuje, zůstává v platnosti původní lhůta splatnosti faktury a pokud objednatel fakturu nezaplatí v původním termínu splatnosti, je v prodlení.

7.4. Doba splatnosti faktury je sjednána na 30 (slovy: třicet) kalendářních dnů od data doručení faktury na adresu objednatele. Takto sjednaná doba splatnosti, není-li průkazně dohodnuto jinak, nahrazuje den splatnosti uvedený na faktuře. V případě, že poslední den splatnosti faktury připadne na den pracovního klidu, resp. volna, bude se za den splatnosti považovat nejblíže následující pracovní den.

7.5. Peněžní závazek objednatele se považuje za včas splněný dnem připsání příslušné částky ve prospěch účtu poskytovatele. Platba faktury bude provedena bezhotovostním převodem na bankovní účet poskytovatele, jenž je uvedený na faktuře.

7.6. Smluvní strany si dojednaly, že objednatel je oprávněn provést zajišťovací úhradu daně z přidané hodnoty ve smyslu ust. § 109a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, na účet příslušného správce daně, jestliže se poskytovatel stane ke dni poskytnutí úplaty za uskutečněné zdanitelné plnění nespolehlivým plátcem daně ve smyslu ust. § 106 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

VIII. Odstraňování závažných technických problémů

8.1. V případě, že dojde ke vzniku závažného technického problému v poskytování služby uvedeném v čl. I této smlouvy, oznámí objednatel tuto skutečnost bezodkladně poskytovateli prokazatelným způsobem s uvedením, jak se závažný technický problém projevuje. Závažný technickým problémem se rozumí skutečnosti způsobující nefunkčnost služeb uvedených v čl. I této smlouvy.

8.2. Poskytovatel je povinen poskytovat službu v souladu se sjednaným SLA (viz Příloha č. 3 této smlouvy).

IX. Smluvní sankce

9.1. V případě nedodržení garantovaného parametru Dostupnosti služby stanoveného v příloze č. 3 této smlouvy z důvodů na straně poskytovatele, je objednatel oprávněn požadovat po poskytovateli zaplacení smluvní sankce ve výši 188,- Kč (slovy: sto osmdesát osm korun českých) za každou hodinu prodlení.

9.2. Ustanoveními o smluvních sankcích není dotčeno právo objednatele na náhradu vzniklé škody v souladu s čl. X. této smlouvy. Smluvní sankce je splatná do 10 dnů ode dne doručení jejího vyúčtování poskytovateli.

9.3. V případě, že objednatel bude v prodlení s jakoukoli platbou dle článku VII. Platební podmínky o více než 30 (slovy:třicet) dnů a nedoloží prokazatelně, že zpoždění spočívá v systémových překážkách objednatelem neovlivnitelných, je poskytovatel oprávněn žádat po objednateli zaplacení úroku z prodlení ve výši stanovené nařízením vlády č. 351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměna likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku, veřejných rejstříků právnických a fyzických osob a evidence svěřenských

fondů a evidence údajů o skutečných majitelích, ve znění pozdějších předpisů. Smluvní strany výslovně sjednávají, že v případě porušení dle tohoto odstavce odpovídá výše úroků z prodlení náhradě škody.

9.4. V případě porušení nebo nedodržení bezpečnostních podmínek uvedených ve čl. II odst. 2.1. a/nebo 2.2. této smlouvy je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 15 000,- Kč (slovy: patnáct tisíc korun českých) za každý prokázaný případ.

9.5. Vznikne-li objednateli neplněním povinností ze strany poskytovatele uvedených v čl. II odst. 2.1. až 2.5. této smlouvy škoda, uhradí ji poskytovatel v prokázané výši.

9.6. V případě porušení povinnosti mlčenlivosti je objednatel oprávněn požadovat po poskytovateli zaplacení smluvní pokuty ve výši 50.000,- Kč (slovy: padesát tisíc korun českých) za každý jednotlivý případ porušení. Tímto ustanovením není dotčeno právo na náhradu škody.

9.7. Smluvní pokuty je objednatel oprávněn započítat proti pohledávce poskytovatele.

9.8. Výslovně se touto smlouvou sjednávají smluvní sankce stanovené v tomto článku. Smluvní strany si výslovně ujednaly, že se k jiným než zde uvedeným a dále např. ústně sjednaným smluvním sankcím sjednaným dodatečně nebude přihlíženo.

9.9. Smluvní strany si výslovně ujednaly vyloučení aplikace ust. § 1806 OZ, tzn. že úroky z úroků nelze požadovat.

X. Náhrada škody a vlastnické právo

10.1. Poskytovatel ručí společně a nerozdílně se subdodavatelem za škody způsobené v rámci plnění této smlouvy. Smluvní strany si dojednaly vyloučení ust. § 2914 OZ.

10.2. Ačkoliv se poskytovatel zavazuje vynaložit přiměřené úsilí na omezení dopadu DDoS útoků, kvůli složité celkové povaze a špatné předvídatelnosti rozsahu takových útoků, poskytovatel nemůže zaručit, že Plán Ochrany nebo aplikovaných opatření budou vždy a bezpodmínečně plně efektivní. Poskytovatel nenese odpovědnost za případnou újmu, která může vzniknout v důsledku jakéhokoli útoku DDoS nebo jakýmkoliv opatřením přijatým poskytovatelem pro ochranu příchozího provozu do sítě objednatele.

XI. Omezení odpovědnosti poskytovatele, mlčenlivost

11.1. Poskytovatel neodpovídá za nemožnost plnit předmět této smlouvy a případnou škodu z toho vzniklou v případě, že objednatel:

a) neposkytl poskytovateli potřebnou součinnost a informace,

b) ani po písemné výzvě poskytovatele nepředal poskytovateli pravdivé a úplné podklady nebo poskytl poskytovateli nevhodné podklady a tyto nedoplnil či nenahradil na základě oznámení dle čl. II. odst. 2.1. písm. d) vhodnými podklady,

c) nerespektoval písemná doporučení a pokyny poskytovatele vydaná v souladu se zákonem.

11.2. Poskytovatel se zavazuje po celou dobu trvání této smlouvy, jakož i po jejím uplynutí respektovat a dodržovat mlčenlivost o skutečnostech dle čl. II. odst. 2.1. písm. e).

11.3. V této souvislosti se zejména zavazuje:

a) nesdělit údaje, které objednatel označil jako důvěrné či neveřejné, ani jiné údaje, které se od objednatele při plnění této smlouvy dozvěděl, třetím osobám, s výjimkou osob uvedených v čl. XII. odst. 12.1. této smlouvy,

b) zajistit, aby uvedené údaje nebyly zpřístupněny třetím osobám, s výjimkou osob uvedených v čl. XII. odst. 12.1. této smlouvy,

c) zabezpečit listiny včetně fotokopií obsahující uvedené údaje před zneužitím třetími osobami.

11.4. Smluvní strany se zavazují, že obchodní a další údaje, s nimiž se při plnění závazků z této smlouvy seznámily, nezpřístupní třetím osobám, mimo osob uvedených v čl. XII. odst. 12.1. této smlouvy, bez písemného souhlasu druhé smluvní strany.

11.5. V případě přístupu k osobním údajům, které jsou v rámci Celní správy ČR zpracovávány, se tímto poskytovatel zavazuje k tomu, že při své činnosti bude postupovat v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 a zákonem č. 110/2019 Sb., o zpracování osobních údajů, zejména:

a) přijme taková opatření, která zajistí náležité zabezpečení zpřístupněných osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a náhodnou ztrátou, zničením nebo poškozením,

b) bude se zpřístupněnými osobními údaji nakládat pouze v rozsahu nezbytně nutném k plnění předmětu díla,

c) bude zachovávat mlčenlivost ohledně zpřístupněných osobních údajů.

d) V případě zapojení třetí strany do plnění předmětu díla je poskytovatel povinen tuto stranu smluvně zavázat k plnění výše uvedených povinností v oblasti ochrany osobních údajů.

XII. Součinnost a komunikace smluvních stran

12.1. Při plnění této smlouvy jsou na straně objednatele pověřeni rolí **oprávněné osoby**:

ve věcech smluvních: [redacted]

ve věcech technických: [redacted]

Tyto oprávněné osoby budou vyvíjet součinnost s poskytovatelem při plnění předmětu smlouvy, a to ve věcech smluvních (s právem předávat poskytovateli všechny informace potřebné pro plnění smluvního závazku poskytovatele, o které ke splnění závazků v souladu s touto smlouvou požádá, a přebírat od něho všechna plnění uskutečněná dle této smlouvy).

12.2. Při plnění této smlouvy jsou na straně poskytovatele pověřeni rolí **oprávněné osoby**:

ve věcech smluvních: [redacted]

ve věcech technických [redacted]

Tyto oprávněné osoby budou vyvíjet součinnost s objednatelem při plnění předmětu smlouvy, a to ve věcech smluvních (s právem přebírat všechny informace potřebné pro plnění tohoto smluvního závazku od objednatele, o které ke splnění závazků v souladu s touto smlouvou požádá a předávat mu všechna plnění uskutečněná dle této smlouvy).

XIII. Platnost a účinnost smlouvy

13.1. Smlouva se uzavírá na dobu určitou na 24 měsíců plynoucích ode dne nabytí její účinnosti.

13.2. Tato smlouva nabývá platnosti podpisem statutárních zástupců obou smluvních stran a účinnosti dnem jejího uveřejnění v registru smluv.

13.3. Tuto smlouvu je možno ukončit písemnou dohodou obou smluvních stran.

13.4. Shledá-li objednatel nebo poskytovatel podstatné porušení plnění předmětu smlouvy druhou stranou, má právo na okamžité odstoupení od smlouvy, jehož písemné vyhotovení musí být druhé straně doručeno.

13.5. Za podstatné porušení smlouvy ze strany objednatele se zejména považuje, pokud objednatel :

a) nevystaví pro poskytovatele plnou moc dle čl. II. odst. 2.7. této smlouvy,

b) bude v prodlení s úhradou ceny déle než 30 dní,

c) poruší obchodní tajemství nebo jiný závazek mlčenlivosti dle této smlouvy.

13.6. Za podstatné porušení smlouvy ze strany poskytovatele se zejména považuje, pokud poskytovatel:

a) poruší kterékoliv ustanovení čl. II. této smlouvy,

b) poruší obchodní tajemství nebo jiný závazek mlčenlivosti dle této smlouvy.

13.7. Odstoupení od smlouvy je platné dnem doručení oznámení o odstoupení. Strana, kvůli jejímuž porušení smlouvy došlo k odstoupení od smlouvy, je povinna zaplatit odstupující straně na základě faktury vystavené odstupující stranou do 14 (slovy: čtrnácti) dnů ode dne doručení takové faktury veškeré náklady odstupující strany jakožto přímý důsledek odstoupení od smlouvy.

13.8. Obě smluvní strany mají možnost tuto smlouvu kdykoliv bez udání důvodu vypovědět s výpovědní dobou 3 měsíce. Výpovědní doba začne běžet od počátku měsíce následujícího po měsíci, v němž byla výpověď doručena druhé smluvní straně.

13.9. Ustanovení článků této smlouvy, jejichž cílem je upravit vztahy mezi smluvními stranami po ukončení účinnosti této smlouvy, zůstanou platná i po ukončení této smlouvy.

XIV. Zvláštní ujednání

14.1. Objednatel souhlasí s tím, že poskytovatel má právo zmiňovat tuto smlouvu jako referenci vůči třetím stranám, avšak za podmínky dodržení závazků mlčenlivosti dle čl. XI. této smlouvy.

14.2. Žádná ze smluvních stran není odpovědná za škodu způsobenou okolnostmi vylučujícími odpovědnost ve smyslu § 2913 odst. 2 OZ.

14.3. Poskytovatel výslovně prohlašuje, že je v plném rozsahu pojištěn minimálně do výše 10 mil. Kč pro případ škody způsobené porušením závazků poskytovatele dle této smlouvy. Tuto pojistnou ochranu se poskytovatel zavazuje udržovat po celou dobu možnosti trvání této smlouvy a po celou dobu možnosti kontroly ze strany finančního úřadu nebo jiného kompetentního orgánu, viz ust. § 44a odst.8 zákona č.218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů, ve znění pozdějších právních předpisů.

14.4. Poskytovatel souhlasí s tím, že obsah této smlouvy není obchodním tajemstvím a objednatel jej může zveřejnit, zejména v rozsahu a za podmínek vyplývajících ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. V souladu se zákonem č. 340/2015 Sb., o registru smluv, se strany dohodly, že objednatel zašle tuto smlouvu správci registru smluv k uveřejnění ve lhůtě, stanovené tímto zákonem. Osobní údaje stran před odesláním budou anonymizovány v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů.

14.5. Poskytovatel je povinen poskytnout objednateli veškeré doklady související s realizací projektu a plněním závazných ukazatelů v rámci předmětu činnosti zhotovitele, které si vyžádají příslušné kontrolní orgány, zejména příslušný finanční úřad, Ministerstvo financí ČR, Nejvyšší kontrolní úřad.

XV. Okolnosti vylučující odpovědnost

15.1. Pro účely této smlouvy „okolnosti vylučující odpovědnost“ znamenají událost, vymezenou v § 2913 odst. 2 OZ.

15.2. Jestliže vznikne situace zaviněná okolnostmi vylučujícími odpovědnost, dotčená strana okamžitě uvědomí druhou smluvní stranu písemně o takových podmínkách a jejich příčině. Pokud není jinak stanoveno písemně ze strany dotčené, bude druhá smluvní strana pokračovat v realizaci svých závazků podle smlouvy tak, jak je to možné a bude hledat veškeré rozumné alternativní prostředky pro realizaci části, kde nebrání okolnosti vylučující odpovědnost.

15.3. Žádná ze smluvních stran nebude odpovídat za nesplnění kteréhokoliv ze svých smluvních závazků dle této smlouvy či jejich dodatků v důsledku okolností vylučujících odpovědnost. Platební závazky vzniklé před okolností vylučující odpovědnost nebudou okolností vylučující odpovědnost prominuty. Žádná ze smluvních stran není oprávněna požadovat zaplacení smluvní sankce druhou smluvní stranou za porušení povinností z této smlouvy okolnostmi vylučujícími odpovědnost.

15.4. Trvají-li okolnosti vylučující odpovědnost déle než 3 (slovy: tři) měsíce, smluvní strany mohou odstoupit od Smlouvy písemně s účinností ke dni doručení odstoupení druhé smluvní straně.

15.5. Smluvní strany si výslovně ujednaly vyloučení aplikace ust. § 2914 OZ.

XVI. Závěrečná ujednání

16.1. Veškerá právní jednání směřující ke změně i části této smlouvy, jakož i k jejímu zrušení, musí mít formu vzestupně číslovaných písemných dodatků, schválených statutárními zástupci smluvních stran. Dodatek se po schválení stává nedílnou součástí této smlouvy.

16.2. Stanou-li se některá ustanovení této smlouvy zcela nebo zčásti neplatná nebo pokud by některá ustanovení chyběla, není tím dotčena platnost zbývajících ustanovení. Místo neplatného ustanovení platí jako dohodnuté takové ustanovení, které odpovídá smyslu a účelu neplatného ustanovení. Schází-li ustanovení zcela, platí za dohodnuté takové ustanovení, které odpovídá tomu, co by podle smyslu a účelu této Smlouvy bylo ujednáno, kdyby tato skutečnost byla známa od počátku. Totéž platí, vyskytnou-li se ve smlouvě či jejích dodatcích případné mezery.

16.3. Tato smlouva a veškeré záležitosti z ní vyplývající nebo s ní související se řídí právním řádem České republiky a spadá pod jurisdikci soudů České republiky. Smluvní strany se zavazují, že případné rozpory vzniklé při realizaci této smlouvy budou řešit korektním způsobem a v souladu s právními předpisy a pravidly slušnosti. Každá ze smluvních stran se dále zavazuje, že k soudnímu řešení uvedených sporů přistoupí až po vyčerpání možností jejich vyřízení mimosoudní cestou.

16.4. Smluvní strany podle § 89a zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů určují jako místně příslušný soud Obvodní soud pro Prahu 1; v případě, že podle procesních předpisů je k rozhodování věci v prvním stupni příslušný krajský soud, určují smluvní strany jako místně příslušný soud Městský soud v Praze.

16.5. Pokud se jedna ze smluvních stran vzdá určitého nároku na nápravu v případě porušení nebo nedodržení ustanovení této smlouvy ze strany druhé smluvní strany nebo se zdrží či opomene uplatnit či využít kteréhokoli práva nebo výsady, jež jí podle této smlouvy náleží nebo náležet může, nesmí být takový úkon, a to bez výjimky, považován nebo uplatňován jako precedens do budoucna pro jakýkoli další případ, ani nelze považovat takové jednání za vzdání se jakéhokoli nároku, práva či výsady jednou pro vždy.

16.6. Poskytovatel výslovně souhlasí s tím, že objednatel tuto smlouvu uveřejní na svém profilu v plném znění v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění.

16.7. Smluvní strany si ujednaly, že závazky vyplývající z této smlouvy se promlčují ve lhůtě deset let ode dne, kdy smluvní strana mohla poprvé toto právo uplatnit.

16.8. V souladu se zákonem č. 340/2015 Sb., o registru smluv, se strany dohodly, že nabyvatel zašle tuto smlouvu správci registru smluv k uveřejnění ve lhůtě, stanovené tímto zákonem. Osobní údaje stran před odesláním budou anonymizovány v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů.

16.9. Smluvní strany si výslovně ujednaly, že tuto smlouvu nelze postoupit na řad. Žádná ze smluvních stran není oprávněna vtělit jakékoliv právo plynoucí jí ze smlouvy nebo z jejího porušení do podoby cenného papíru.

16.10. Smluvní strany výslovně vylučují, aby nad rámec ustanovení této smlouvy byla jakákoliv práva a povinnosti dovozovány z dosavadní či budoucí praxe zavedené mezi stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění této

smlouvy, ledaže je ve smlouvě výslovně sjednáno jinak. Vedle shora uvedeného si smluvní strany potvrzují, že si nejsou vědomy žádných dosud mezi nimi zavedených obchodních zvyklostí či praxe.

16.11. Smluvní strany prohlašují, že si tuto smlouvu přečetly, že byla uzavřena po vzájemném projednání. Autentičnost této smlouvy potvrzují svým podpisem.

16.12. Tato smlouva může být smluvními stranami podepsána vlastnoručně, nebo elektronicky se zaručeným elektronickým podpisem. Bude-li smlouva podepsána vlastnoručně, musí být vyhotovena ve dvou (2) výtiscích s platností originálu, z nichž jeden (1) výtisk obdrží objednatel a jeden (1) výtisk obdrží poskytovatel. V případě, že smlouva bude podepsána elektronicky, zavazuje se smluvní strana, která smlouvu podepíše jako poslední, zaslat její elektronickou podobu bez zbytečného odkladu druhé smluvní straně.

16.13. Přílohy jsou nedílnou součástí této smlouvy. V případě rozporu mezi touto smlouvou a jejími přílohami platí smlouva.

16.14. Tato smlouva obsahuje následující přílohy:

Příloha 1 Formulář „Předávací protokol“
Příloha 2 Krycí list nabídky
Příloha 3 Popis služby, SLA a eskalační matice
Příloha 4 Podmínky poskytování Služby DDoS Ochrana
Příloha 5 Bezpečnostní pravidla pro významné a pro běžné dodavatele ISCS ČR

16.15. Smluvní strany na důkaz svého souhlasu připojují své podpisy.

za poskytovatele	za objednatele
V Praze dne: _____	V Praze dne: _____
[redacted]	

Příloha č.1

PŘEDÁVACÍ PROTOKOL

Objednatel:	**Generální ředitelství cel**	**Číslo smlouvy:**	
Poskytovatel:	**T-Mobile Czech Republic a.s.**		

Předmět předání a převzetí **(Specifikace rozsahu předávaného plnění včetně uvedení verzí předávaných dokumentů nebo software)**
1. DDOS ochrana na operátorské vrstvě ve variantě služby Gold unlimited
2.
3.
4.
Předáno dne:

Podpisem tohoto Předávacího protokolu potvrzuje Oprávněná osoba Poskytovatele, že uvedený předmět k uvedenému dni řádně předala Oprávněné osobě Objednatele.
Podpisem tohoto Předávacího protokolu potvrzuje Oprávněná osoba Objednatele, že uvedený předmět k uvedenému dni řádně převzala v souladu s ustanoveními smlouvy.

Objednatel:		
Oprávněná osoba:	Telefon, E-mail:	Datum:

Poskytovatel:		
Oprávněná osoba:	Telefon, E-mail:	Datum:

Příloha č.2

Krycí list nabídky

Veřejná zakázka na dodávky zadaná jako veřejná zakázka malého rozsahu dle zákona č. 137/2006 Sb., o veřejných zakázkách, v platném znění

„Operátorská DDOS ochrana“

Uchazeč	
Obchodní firma:	T-Mobile Czech Republic, a.s.
Adresa a sídlo/místo podnikání uchazeče:	Tomíčkova 2144/1, 148 00 Praha 4 - Chodov
Jméno/a a příjmení člena/ů statutárního orgánu:	1. OLGA NEVSKA 2. ARMIN SUMESGUTNER 3. JOSE SEVERINO PERDOMO LORENZO
IČO:	64949681
DIČO:	CZ64949681
Bankovní spojení:	19-2235210247 / 0800
Kontaktní osoba:	[redacted]
Telefonní spojení:	
FAX:	
e-mailová adresa:	
Datová schránka:	ygwch5i

Nabídková cena:

Celková nabídková cena za 1 měsíc	**cena bez DPH**	**cena včetně DPH**
	83.250,-	**100.732,5**

V……dne……..

[redacted]

Podpis/y člena/ů statutárního orgánu

Příloha č. 3 **Popis služby, SLA a esklalační matice**

V této části 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.

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 TMobile 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.

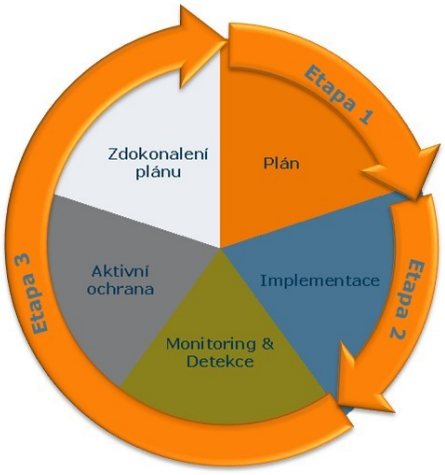
Funkční varianty

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

Funkce / parametr	Bronze	Silver	Gold

DDoS Monitoring	+	-	+
DDoS Ochrana	-	+	+
Funkce / parametr	**Bronze**	**Silver**	**Gold**
Počet konzultačních hodin určených pro stanovení specializovaného Plánu Ochrany	-	6	8
Neomezený počet ochranných akcí	-	+	+
Nezávislost poplatku na velikosti napadení	-	+	+
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)	+	-	+

Varianta **Silver** je vhodná pro organizace, které již mají své vlastní řešení detekce DDoS útoku instalované a vyžadují aktivní ochranu v případě útoku.
Varianta **Gold** je určena organizacím, které potřebují kompletní služby, zahrnující kontrolu, přístup k analýze datových toků a krátkou dobu odezvy při nasazení proaktivní ochrany.



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.

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.

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. • Definovat zákaznický detekční model pro Managed Object. • Zajišťuje proaktivní datový provoz pomocí sms/email upozornění na události. • Smluvně zaručená doba pro doučení oznámení v nejvyšší úrovni hrozeb: do 15 minut od okamžiku detekce. • Přístup k NIP (Network Intelligence Portal), který poskytuje report a statistiky příchozích datových toků a historii zaznamenaných událostí.
Služba	**Rozsah činností**
DDoS Ochrana	• Analyzuje a klasifikuje síťové události zaznamenané monitorovacím systémem, oznamuje klientovi typ události a domluvených ochranných opatření pro nejnebezpečnější události. • Přesměrovává datový provoz do Traffic Cleaning System. • 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].

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

Veškeré zde uvedené lhůty počínají běžet okamžikem doručení příslušného požadavku (na odstranění vady služby nebo na zákaznickou a technickou podporu služby na místě) sjednaným způsobem poskytovateli ze strany objednatele.

„Doba reakce pro oznámení potenciálního útoku" je maximální doba měřená od okamžiku zjištění chybové události nebo překročení hranice datového toku ze strany poskytovatele do okamžiku, kdy systém automaticky/poskytovatel pošle oznámení o této skutečnosti objednateli, jejíž doba je stanovená výše, pokud objednatel sám prokazatelně neodsouhlasil prodloužení této doby.

„Doba reakce pro aktivaci ochrany" je maximální doba měřená od okamžiku odsouhlasení nasazení protiopatření proti zjištěné chybové události nebo překročení datového toku ze strany objednatele do okamžiku nasazení odsouhlaseného protiopatření ze strany poskytovatele, jejíž doba je stanovená výše, pokud objednatel sám prokazatelně neodsouhlasil prodloužení této doby.

[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.

Doba reakce pro oznámení potencionálního útoku a doba reakce pro aktivaci ochrany jsou pouze dobami obvyklými, které mohou být v konkrétních případech ze strany poskytovatele překročeny bez jakékoliv odpovědnosti poskytovatele vůči objednateli.

ATLAS

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. Tento systém je založen na sdílení nejnovějších informací o hrozícím nebezpečí DDoS útoků od provozovatelů sítí po celém světě. V současné době je tato skupina zahrnuje více než 270 poskytovatelů internetu.

Provozovatelé průběžně dodávají do systému ATLAS důležité informace, 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.

Eskalační matice

Tato eskalační matice může být použita kdykoliv, když není Zákazník spokojen se standardní procedurou řešení.

Úroveň	1	2	3
Jméno	[redacted]		
Pozice			
Telefon			

Mobilní	[redacted]		
Fax			
E-mail			
Dostupnost	24x7	8x5	8x5

8x5 – dostupnost v pracovní dny od 9:00 do 17:00.

Příloha č. 4 **Podmínky poskytování Služby DDoS Ochrana**

Podmínky poskytování Služby DDoS Ochrana

Tyto podmínky se uplatní v případě, že není pro Službu ve smluvním vztahu mezi T-Mobile Czech Republic a.s. (dále jen „Poskytovatel“) a jeho zákazníkem/Účastníkem (dále jen „Smluvní partner“) (dále pro smluvní vztah jen „Dokumentace“) sjednáno jinak.

Služba DDoS ochrana (dále jen „Služba“) slouží k ochraně sítě (určených chráněných cílů) Smluvního partnera před útoky typu DoS a DDoS. Chráněné cíle Smluvního partnera jsou definovány v aktuálním formuláři DDoS ochrana - Konfigurační formulář (dále jen „Zadání“) a mohou být dále upraveny postupem uvedeným níže.

Podmínkou Služby je užívání služby datového připojení od Poskytovatele (dále jen „přípojka“).

Tyto podmínky se uplatní v případě, že není pro Službu ve smluvním vztahu mezi T-Mobile Czech Republic a.s. (dále jen „Poskytovatel“) a jeho zákazníkem (dále jen „Smluvní parter“) (dále pro smluvní vztah jen „Dokumentace“) sjednáno jinak. V případě rozporu mezi ujednáním Smluvní dokumentace a těmito Podmínkami poskytování Služby DDoS Ochrana se použijí přednostně ujednání sjednaná v Dokumentaci.

1. Charakteristika Služby

Součástí Služby je analýza, vstupní konzultace a vlastní implementace síťově orientované ochrany telekomunikačních systémů proti DDoS útokům, a to prostřednictvím Služby DDoS Ochrana. Tato Služba je založena na technologii ARBOR od společnosti NetScout Systems, Inc. (dále jen „Platforma“) a na znalostech a zkušenostech specialistů Poskytovatele.

Služba čistí datový tok směřovaný na IP adresy definované jako chráněné cíle Smluvního partnera, a to již na úrovni páteřní sítě a snižuje tak dopady útoku díky rychlé detekci a nasazení předdefinovaných pravidel.

Během útoku je čistý legitimní provoz standardně potlačen obrovským počtem požadavků, který generují útočící zařízení. Hlavním smyslem obrany je tak ochránit legitimní provoz Smluvního partnera směřující na chráněné cíle a zajistit jeho doručení k chráněnému cíli, a přitom odstranit datový tok útočníků, kteří přetěžují linky a cílové počítače (servery) Smluvního partnera.

2. Základní součásti Služby

Operátorská vrstva DDoS ochrany v rámci Služby sestává ze dvou nedílných částí: Monitoringu a vlastní Ochrany (Mitigace).

DDoS Monitoring

Monitoring (Flow-based Monitoring), který běží na úrovni páteřní sítě Poskytovatele, spočívá v analýze vzorků datových toků shromážděných od okrajových směrovačů sítě TMCZ. Systém Poskytovatele analyzuje příchozí provoz (provoz na chráněné cíle), který je přesměrován na koncový bod přípojky Smluvního partnera. Při tom v rámci Služby Platforma v páteřní síti Poskytovatele používá tři metody pro detekci DDoS útoku:

- analýzu zneužití vybraných síťových protokolů
- analýzu vzorků metadat provozu (netflow) směrovaného na chráněné cíle Smluvního partnera
- obecné signatury útoků ukládané v databázi Platformy.

V případě detekce chybové události nebo výrazné překročení obvyklé hranice datového toku Služba automaticky pošle oznámení o podezření na útok v rozsahu uvedeném v Zadání a zahájí proces analýzy a klasifikace, který podle sjednané varianty Služby buď následně dokončují pracovníci Security dohledového operačního centra Poskytovatele (dále jen „SOC“) nebo Platforma Poskytovatele sama automaticky. Monitoring dokáže odhalit útoky na druhé až čtvrté vrstvě (L2-L4) dle ISO 7498 a jeho aktualizace/OSI modelu a částečně i na vrstvě aplikační (L7).

DDoS Mitigace

DDoS Mitigace je součást Služby, která zajišťuje aktivní ochranu a zahájení nasazení protiopatření, která čistí provoz a zmírní dopady útoku na chráněné cíle.

Tato část Služby je spuštěna podle sjednané varianty Služby automaticky nebo v souladu se Zadáním dohodnutým se Smluvním partnerem, které definuje mj. rozsah vlastních činností a postupů, které mají být použity při identifikaci nežádoucího provozu.

V případě hrozby útoku je veškerý příchozí provoz přímo z páteřní sítě Poskytovatele přesměrován na Platformu, která analyzuje a identifikuje legitimní provoz a odstraní (zlikviduje) provoz nežádoucí. Nežádoucím provozem, je provoz, který byl Platformou vyhodnocen jako neobvyklý či nenaučený nebo provoz vykazující škodlivé signatury. Ostatní provoz, který byl Platformou vyhodnocen jako legitimní komunikace, je pak směrován dále na určený chráněný cíl.

3. Parametry Služby

Základní charakteristika Služby – DDoS Ochrana **Gold:**

- Předpokládá dostupnost znalých pracovníků na straně Smluvního partnera, kteří jsou během útoku připraveni efektivně spolupracovat se SOC na mitigaci útoku.
- Umožňuje zajistit detekci a mitigaci volumetrických DDoS útoků na úrovni jednotlivých chráněných aplikací, individuální přístup a maximální flexibilitu mitigace s cílem minimalizovat dobu nedostupnosti chráněných cílů Smluvního partnera
- Součinnost týmu SOC v režimu 24x7
  - Proaktivní monitoring výskytu bezpečnostních událostí a dle potřeby nasazení protiopatření ve spolupráci se Smluvním partnerem
- Plán ochrany je tvořen individuálně dle potřeb Smluvního partnera
  - Způsob ochrany lze nastavit individuálně pro jednotlivé chráněné skupiny aplikací (web, dns, vpn…) či jednotlivé servery.
  - Mitigace probíhá za plné asistence SOC a umožňuje flexibilní ladění / modifikaci mitigačních pravidel v průběhu útoku pro jejich maximální účinnost
- Pravidelný měsíční reporting
- Čas bezpečnostních konzultantů SOC v ceně Služby
- Možnost rozšíření Služby o In-line ochranu (samostatné zákaznické řešení) a vzájemnou integraci obou služeb

3.1.1 Režimy varianty Gold

Unlimited

Pravidelný měsíční poplatek není závislý na počtu DDoS mitigací, ani na jejich délce.

On-Demand

Pravidelný měsíční poplatek zahrnuje nasazení DDoS mitigace po dobu 2 dnů v kalendářním měsíci. V případě, že je požadováno nasazení DDoS mitigace ve větším rozsahu, bude cena Služby navýšena o jednorázový poplatek za každý další započatý den mitigace. Pokud v rámci kalendářního měsíce suma všech poplatků přesáhne hodnotu maximálního měsíčního poplatku pro variantu GOLD On-Demand, je v daném kalendářním měsíci fakturován pouze maximální měsíční poplatek pro variantu GOLD OnDemand.

4. Princip fungování Služby

V rámci Služby Poskytovatel monitoruje datový provoz na přípojce Smluvního partnera. Provoz je monitorován pomocí Platformy umístěné v páteřní síti Poskytovatele. Služba spočívá v detekci a ochraně před internetovými útoky typu DDoS.

4.1 Detekce útoku

Technologie Platformy 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.

4.2 Ochrana před útokem

Technologie Platformy umožňuje v případě útoku na chráněné cíle na základě znalosti (naučených vzorců chování) datového provozu Smluvního partnera odfiltrovat podstatnou část nežádoucího provozu.

Standardní provoz Smluvního partnera

Platforma získává znalosti datového provozu Smluvního partnera (učí se) na „standardním provozu Smluvního partnera“. Během standardního provozu, kdy neprobíhá útok DDoS, použitá technologie analyzuje pouze hlavičky datových paketů, obsah paketu - data Smluvního partnera tedy nejsou součástí analýzy.

Při zahájení poskytování Služby a po každé nikoli bezvýznamné změně struktury provozu Smluvního partnera, jsou nezbytné alespoň tři týdny, aby Platforma získala potřebné znalosti o novém profilu standardního provozu Smluvního partnera. V tomto období je použitá technologie méně citlivá pro detekci či vyhodnocení útoku.

4.2.1 Způsob nasazení protiopatření

Schválení nasazení protiopatření

Platforma v případě detekce útoku nebo podezření na útok DDoS poskytne informaci SOC. SOC analyzuje výstrahy technologie. V případě, že SOC vyhodnotí údaje Platformy jako podezření na volumetrický útok DDoS, kontaktuje telefonicky Osobu oprávněnou pro schvalování mitigace (u více osob ve stanoveném pořadí) prostřednictvím telefonního čísla uvedeného v Zadání (v tomto dokumentu také jako „autorizační kontakt“). Smluvní partner bere na vědomí a souhlasí s tím, že tyto hovory jsou Poskytovatelem nahrávány. Pokud se SOC nedovolá autorizačnímu kontaktu uvedenému v Zadání, pak všem autorizačním kontaktům pošle e-mail.

Poskytovatel následně postupuje v souladu s pokyny Smluvního partnera, 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 proti útoku a tato skutečnost bude zaznamenána v rámci evidence Poskytovatele.

V případě, že Smluvní partner vyhodnotí alarmy týkající se aplikační infrastruktury jako podezření na aplikační útok, autorizační kontakt to oznámí SOC, který nasadí protiopatření na základě požadavku autorizačního kontaktu.

4.2.2 Protiopatření

V rámci protiopatření a s ohledem na chráněné cíle uvedené Smluvním partnerem v Zadání Poskytovatel přesměruje provoz Smluvního partnera nebo jeho část do platformy ARBOR, které odstraní provoz považovaný za škodlivý. Nastavení protiopatření primárně zohledňuje zprovoznění chráněných cílů dle Zadání. Vyčištěný provoz je doručen k chráněnému cíli.

V případě vícenásobného útoku, kdy útoky běží paralelně, bude výše uvedený proces protiopatření opakován, dokud se nevyčistí všechen nežádoucí provoz a/nebo nebude obnoven běžný provoz Smluvního partnera (provoz hodnocený Službou jako běžný).

Pokud SOC při útoku nezastihne ani jeden autorizační kontakt (popř. žádný z nich neuvede identifikaci služby formou short ID) a není ohrožena infrastruktura Poskytovatele, je Poskytovatel oprávněn zavést tzv. nouzový režim – tj. neprovést žádnou mitigaci.

4.3 Ukončení nasazení Protiopatření

V případě, že SOC vyhodnotí údaje z Platformy jako ukončení útoku DDoS, oznámí to autorizačnímu kontaktu Smluvního partnera, a ukončí nasazení protiopatření či dále řeší útok dle pokynu Smluvního partnera. Po ukončení útoku SOC odešle na osobu oprávněnou pro přijímání reportu po útoku PDF report

5. Konfigurace Služby a její změna

5.1 Konfigurace Služby

Konfigurace Služby je zachycena v dokumentu s názvem Konfigurační formulář (dále také jen „Zadání“), který tvoří nedílnou součást Dokumentace. V Zadání Smluvní partner specifikuje zejména chráněné cíle, kontaktní osoby a notifikační cíle pro Službu a plán ochrany (pokud se liší od plánu ochrany uvedeného v kapitole 8 tohoto Popisu služby).

Kontaktní osoby uvedené v Zadání jsou kontaktními osobami určenými výhradně pro Službu a výhradně pro určené úkony.

Notifikačním cílem je Smluvním partnerem určený typ kontaktu (volání, SMS, e-mail) u příslušného typu kontaktní osoby s tím, že Poskytovatel dále neověřuje aktuálnost daného notifikačního cíle a skutečnost, zda byla zpráva na notifikační cíl doručena (toto je v odpovědnosti Smluvního partnera). Povinnost Poskytovatele je splněna odesláním zprávy na určený notifikační cíl.

V případě změny typu či kapacity přípojky Poskytovatel doporučuje pro správné fungování Služby revizi plánu ochrany ze strany Smluvního partnera

5.2 Změna konfigurace Služby

Změnu parametrů Služby zadává Smluvní partner prostřednictvím nového Zadání nebo jinou změnou Dokumentace, podle toho, které parametry jsou změnou ovlivněny.

O změnu konfigurace Služby žádá příslušná kontaktní osoba Smluvního partnera SOC formou emailového požadavku na změnu. Tento požadavek musí obsahovat

- jedinečný identifikátor Služby (také ShortID), které se požadovaná změna týká
- na žádost SOC Zadání s vyznačením požadované změny formou revize

Změnu konfigurace Služby spočívající ve změně (vč. Doplnění) Kontaktních osob Smluvního partnera sjednávaných v Zadání může Smluvní partner provést jednostranně. Ostatní požadavky na změnu konfigurace Služby podléhají posouzení technické realizovatelnosti ze strany Poskytovatele.

Poskytovatel se zavazuje provést požadovanou změnu Kontaktních osob nebo posoudit technickou realizovatelnost ostatních požadavků bez zbytečného odkladu po doručení požadavku na změnu konfigurace Služby SOC.

Pokud Poskytovatel nejpozději do 14 dnů od doručení informace o změně nevyzve Smluvního partnera k úpravě požadavku, požadavek Smluvního partnera se považuje za akceptovaný a konfigurace Služby se mění ke dni, kdy Poskytovatel začne postupovat v souladu se změnou, nejpozději však uplynutím uvedené lhůty.

Změny Zadání či jiné změny Dokumentace jsou prováděny v rámci hodin technické podpory Služby uvedené pro konkrétní variantu Služby ve Specifikaci služby. Pokud je rozsah a pracnost změny požadovaných parametrů náročnější než příslušný rozsah hodin technické podpory sjednaný v rámci Služby, jsou tyto změny zpoplatněny dle platného Ceníku služby DDoS ochrana.

6. Kontaktní osoby Smluvního partnera

Kontaktní osoby Smluvního partnera pro Službu jsou sjednány v aktuálním Zadání či jinde v Dokumentaci, a to s těmito kompetencemi:

6.1 Kontaktní osoba uvedená v Dokumentaci (zejména smlouvě či objednávce Služby) - ADSR

- může provést změnu Dokumentace s výjimkou samostatné změny konfigurace Služby

6.2 Osoba pověřená pro schvalování mitigace (autorizační kontakt)

- může provést změnu konfigurace Služby
- jménem Smluvního partnera vydává pokyny pro SOC při mitigaci, pokyny lze vydat pouze z telefonního čísla či e-mailu uvedeného pro danou kontaktní osobu a musí SOC sdělit jedinečný identifikátor Služby (také ShortID).

6.3 Osoba pověřená pro příjem reportů a notifikací

- je příjemcem reportů po útoku a pravidelných měsíčních reportů, které jsou doručovány prostřednictvím e-mailu
- notifikace o zachycených událostech jsou doručovány prostřednictvím e-mailu a/nebo SMS
- tento typ kontaktní osoby nemůže provádět změnu konfigurace Služby ani změnu Kontaktních osob

6.4 Osoba pověřená pro přístup na Portál

- může provádět změnu konfigurace Služby
- jménem Smluvního partnera přistupuje na Portál z IP adresy určené v Zadání (z jiných IP adres nelze na Portál přistupovat)
- přihlašovací údaje pro přístup na portál získá od Poskytovatele v rámci zřízení Služby

Pro vyloučení pochybností se stanoví, že Službu na straně Smluvního partnera s výjimkou změny Specifikace služby nemohou obsluhovat Kontaktní osoby uvedené ve Specifikaci služby ani Kontaktní osoby uvedené ve formuláři Kontaktní osoby, který tvoří nedílnou součást Smlouvy. Osoby pověřené na straně Smluvního partnera k obsluze Služby je tedy třeba vždy uvést v Zadání.

7. Kontaktní středisko Poskytovatele - SOC

Kontakty na Securit

Primární tel. linka:	[redacted]
Mobilní linka:	
E-mail:	
Dostupnost	

Eskalační matice

Pokud není Smluvní partner spokojen se standardní procedurou řešení události, může použít následující eskalační matici (v uvedeném pořadí):

Úroveň	**1**	**2**
Jméno	[redacted]	
Pozice		
Mobilní telefon		
E-mail		

Dostupnost	8x5	8x5

8 x 5 – znamená dostupnost v pracovní dny od 9:00 do 17:00.

8. Plán ochrany

Výchozí rozsah ochrany, který lze upravit v aktuálním Zadání, zahrnuje následující kroky.

Služba	Rozsah činností
DDoS Monitoring	○ Sledování příchozího provozu na L3 a L4 v režimu 24/7. ○ Definování detekčního modelu pro chráněné cíle Smluvního partnera. ○ Zajištění proaktivního dohledu datového provozu pomocí emailového upozornění na události
	○ Smluvně zaručená doba pro doručení oznámení v nejvyšší úrovni hrozeb od okamžiku detekce ○ Přístup k Portálu, který poskytuje report a statistiky příchozích datových toků a historii zaznamenaných událostí
DDoS Mitigace	○ Analýza a klasifikace síťové události zaznamenané Platformou ○ Oznámení typu události a domluvených protiopatření při útoku Smluvnímu partnerovi ○ Přesměrování datového provozu do Platformy ○ Sada dalších protiopatření může zahrnovat: ○ blokování podezřelé IP adresy, která je vyhodnocena jako zdroj útoku, ○ omezení vysílání rozsahů sítí (pro klienty s BGP routingem) ○ blokování zdrojové a cílové IP adresy, ○ filtrování / zakázání datového provozu pro vybrané protokoly (UDP)

9. Zpracování osobních údajů

V rámci Služby dochází ke zpracování osobních údajů a dalších informací.

Poskytovatel zpracovává osobní údaje vždy transparentně, korektně, v souladu s nařízením Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“) a zákonem č. 110/2019 Sb., o zpracování osobních údajů (dále jen „Zákon o zpracování osobních údajů“), a to v rozsahu nezbytném pro příslušný účel zpracování. Osobní údaje jsou bezpečně uchovávány po dobu nezbytně nutnou.

Osobní údaje jsou zpracovávány za účelem zajištění Služby v rozsahu uvedeném níže. Zpracovávány jsou osobní údaje administrátorů Služby a Kontaktních osob Smluvního partnera.

Účel zpracování	Účel zpracování spočívá v: - zajištění Služby: - přihlášení do Portálu Služby dle údajů konfiguračního formuláře (Zadání); - komunikace se zákazníkem (Smluvním partnerem) v souvislosti s nastalým incidentem (tickety a e-mailová komunikace).
Právní titul	Plnění smlouvy podle 6 odst. 1 písm. b) GDPR.
Subjekty osobních údajů	Smluvní partneři (fyzické osoby jednající za zákazníka), administrátoři a Kontaktní osoby Smluvního partnera.

Rozsah zpracovávaných osobních údajů	Smluvní partner: - komunikace se Smluvním partnerem v souvislosti s nastalým incidentem. Administrátoři: V rámci Zadání dochází ke zpracování následujících osobních údajů: - jméno a příjmení; - telefonní číslo; - e-mailová adresa; - firma, kterou zastupují (zaměstnavatel). Kontaktní osoby Smluvního partnera: - jméno a příjmení; - telefonní číslo;
	- e-mailová adresa; - společnost, kterou zastupují, (zaměstnavatel). V rámci Služby dochází rovněž ke zpracování provozních dat. Jedná se o vzorky metadat provozu „netflow“. To znamená, že se jedná o hlavičky IP paketů, které neobsahují uživatelské údaje. Vzorky netflow se standardně sbírají se vzorkováním 1:2000, tzn., že se z směrovače do Platformy pošle pouze jeden ze 2000 netflow. Vzorkování lze provádět v rozmezí 1:1000 až 1:5000.
Způsob zpracování	Manuální či automatizované zpracování.
Doba zpracování	- Zajištění Služby: po dobu poskytování Služby a záznamů o ní (zálohy aplikací systémů a konfigurací). - přihlášení do Portálu: po dobu existence Služby. - komunikace se Smluvním partnerem v souvislosti s nastalým incidentem (tickety a e-mailová komunikace): po dobu existence Služby, případně po dobu existence tiketů v IT nástrojích Poskytovatele a záznamů o ní (zálohy aplikací systémů a konfigurací) Vzorky netflow se ukládají na Platformě umístěné v DC TMCZ a STSK. Z daných vzorků Platforma (strojově) generuje grafy a statistiky provozu. Tyto předpřipravené údaje se ukládají na Platformě v DC TMCZ a STSK. Vzorky provozu a předpřipravené grafy jsou uchovávány na Platformě maximálně po dobu 5 let a následně jsou automaticky vymazány.
Přístup k datům v rámci TMCZ	Oprávnění zaměstnanci TMCZ a zaměstnanci dodavatele.

Dodavatel/Zpracovatel	NETSCOUT SYSTEMS, INC. Corporate office at: 310 Littleton Road Westford, MA 01886-4105 United States Incorporated in the State of Delaware, USA, Tax ID No (TIN): 04-2837575

Při zajištění Služby dochází rovněž k zaznamenání alertů, které byly vyhlášeny při provozu Smluvního partnera. Jedná se o informace spojené se útokem na konkrétního Smluvního partnera včetně jejich strojového rozboru. Alerty, tj. informace spojené s útokem na Smluvního partnera jsou uchovávány maximálně po dobu 13 měsíců a následně dochází k jejich automatickému výmazu.

Nahrávání hovorů

Poskytovatel informuje Smluvního partnera/Oprávněnou osobu, že telefonní hovory Smluvního partnera (jeho zaměstnanců a pracovníků) uskutečněné v rámci Služby jsou nahrávány. Poskytovatel nahrává příchozí a odchozí hovory uskutečněné na telefonní lince mezi Smluvním partnerem/Oprávněnou osobou a zaměstnanci SOC Poskytovatele (dohledové centrum T-Mobile).

K nahrávání telefonních hovorů dochází za účelem plnění smlouvy – Dokumentace uzavřené se Smluvním partnerem, tj. za účelem zajištění poskytování Služby sjednané Dokumentací. Poskytovatel nahrává telefonní hovory rovněž za účelem zajištění projevu vůle Smluvního partnera a z důvodu oprávněných zájmů Poskytovatele.

Nahrávky telefonních hovorů jsou uchovávány ze strany Poskytovatele po dobu 3 měsíců.

Smluvní partner se zavazuje, že své zaměstnance, pracovníky a osoby s obdobným postavením informuje o tom, že jejich komunikace na telefonní linku Poskytovatele bude nahrávána za účely uvedenými výše. Smluvní partner odpovídá za případnou újmu způsobenou tím, že by z jeho strany nedošlo k informování subjektů údajů Smluvního partnera/Oprávněné osoby o skutečnosti, že telefonní hovory jsou nahrávány.

Poskytovatel volajícího na telefonní lince se zaměstnanci SOC dále informuje prostřednictvím info hlášky, že telefonní hovor je nahráván. Volající, kteří s nahráváním hovoru nesouhlasí, mají možnost zavěsit a obrátit se na zaměstnance SOC formou e-mailu

10. SLA

Pokud není v Dokumentaci výslovně sjednáno jinak, platí, že: - Informace týkající se definice a dodržování parametru SLA Služby jsou uvedeny v příslušných Smluvních dokumentech, zejm. v platných Obchodních podmínkách Smlouvy o firemním řešení společnosti T-Mobile Czech Republic a.s.

- Podrobné podmínky týkající se úrovně garance Služby (SLA) jsou stanoveny v platném Popisu Služby SLA.

11. Lhůta pro zřízení Služby

Standardní lhůta pro zřízení Služby činí obvykle 30 pracovních dní ode dne podpisu Smlouvy (Specifikace služby) Poskytovatelem a Smluvním partnerem. Tato lhůta neplatí v případě, kdy je společně se Službou DDoS ochrana zřizována i jiná služba Poskytovatele a zřízení těchto Služeb je navzájem provázáno. Nezbytnou podmínkou pro dodržení sjednaného termínu Služby je poskytnutí nezbytné součinnosti ze strany Smluvního partnera a rovněž i existence (zprovoznění) konektivních Služeb, k nimž je tato Služba DDoS ochrana zřizována.

Předání Služby po jejím zřízení (zprovoznění)

Služba je zřízena a předána Smluvnímu partnerovi do provozu následně po nastavení výchozí konfigurace Služby na Platformě dle požadavků Dokumentace a Zadání, uvedení do provozu, provedení testů a předání Předávacího protokolu Služby, který je zaslán na kontaktní osobu Smluvního partnera.

Následně má Smluvní partner 2 pracovní dny na odzkoušení funkčnosti, konfigurace nastavení parametrů, porovnání souladu Služby s parametry uvedenými v příslušné Specifikaci služby a potvrzení převzetí Služby Poskytovateli v souladu s dále uvedeným.

V uvedené lhůtě je Smluvní partner povinen potvrdit Poskytovateli písemně (formou e-mailu) převzetí Služby, resp. může uplatnit připomínky nebo reklamovat funkčnost a parametry Služby, jinak se má za to, že uplynutím uvedené lhůty, tzn. dvou (2) celých pracovních dnů se Služba považuje za řádně předanou v souladu s Dokumentací. Okamžikem doručení potvrzení převzetí Služby ze strany Smluvního partnera Poskytovateli bez připomínek a reklamace, resp. marným uplynutím uvedené lhůty, je Služba považována za řádně zřízenou ve smyslu příslušné Specifikace služby ze strany Poskytovatele vůči Smluvnímu partnerovi.

12. Odpovědnost TMCZ při poskytování Služby DDoS ochrana

V rámci Služby garantuje Poskytovatel Smluvnímu partnerovi včasnou implementaci standardních ochranných postupů (scénářů) dle Zadání a zajišťuje přístup ke znalostem a dovednostem SOC týmu Poskytovatele a nejnovějším poznatkům inženýrského týmu NETSCOUT.

Poskytovatel se zavazuje poskytovat službu DDoS ochrany na základě Good Practice principů s využitím aktuálně dostupné sady funkcí Platformy.

Přestože se Poskytovatel zavazuje vynaložit přiměřené úsilí k omezení dopadu DDoS útoků, vzhledem k neustálému vývoji nových typů útoků, jejich kombinací a modifikací a rozsahu, nemůže Poskytovatel zaručit, že Ochranný plán nebo uplatňovaná opatření budou vždy a bezpodmínečně plně účinná.

Poskytovatel nenese odpovědnost za případné škody, které Smluvní partner utrpí v důsledku jakéhokoli útoku DDoS nebo jakýmkoliv opatřením přijatým Poskytovatelem pro ochranu příchozího provozu do sítě Smluvního partnera.

Poskytovatel upozorňuje Smluvního partnera, že v souladu se zák. č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), v platném znění, je povinen poskytovat přednostní připojení pro určené subjekty, zajišťovat bezpečnost a integritu své sítě elektronických komunikací a bezpečnost služeb, které poskytuje, a plnit další zákonné povinnosti či povinnosti uložené mu na základě zákona soudním či správním rozhodnutím či opatřením. Za účelem zachování integrity a bezpečnosti sítě T-Mobile, služeb poskytovaných prostřednictvím této sítě a koncových zařízení koncových Uživatelů, může Poskytovatel uplatňovat dočasná opatření spočívající v blokování IP adres a jejich rozsahů, blokování síťových portů, protokolů a doménových jmen, dále pak aktualizaci firmware a řízení konfigurace koncových zařízení, které má Poskytovatel ve své správě, jsou-li tyto známým zdrojem nebo cílem útoků a nebo představují hrozbu pro bezpečnost a integritu sítě.

Za účelem zabránění hrozícímu přetížení sítě T-Mobile nebo zmírnění účinků výjimečného přetížení sítě T-Mobile může dojít k dočasnému plošnému omezení datových toků všech koncových uživatelů. Výše uvedená opatření jsou vždy aplikována po nezbytně nutnou dobu a pouze v nezbytné míře k naplnění sledovaného účelu a jejich vliv na poskytování Služby může být různorodý – Smluvní partner je nemusí v některých případech ani zaznamenat, avšak v některých případech může dojít i k dočasnému znepřístupnění poskytované Služby. Poskytovatel garantuje uplatnění takové intenzity opatření, která má nejmenší zásah do zákaznické zkušenosti. V souvislosti s plněním výše uvedených povinnosti Poskytovatele není Smluvní partner oprávněn požadovat jakoukoliv kompenzaci či náhradu újmy po Poskytovateli.

Poskytovatel není odpovědný za neposkytnutí nebo vadné poskytnutí Služby, resp. za újmu, vzniklou v důsledku následujících skutečností, které pokud nastanou, nejsou považovány za Poruchu Služby a Služba není v jejich důsledku považována za nedostupnou (resp. vadně poskytnutou):

- V případech, kdy za poruchu Služby neodpovídá Poskytovatel v souladu s příslušnými právními předpisy;
- Poruchy Služby vzniklé vnitřní chybou operačního systému a dalšího programového vybavení třetích stran. Případnou odpovědnost nesou tyto třetí strany dle jejich licenčních ujednání; • Poruchy Služby vzniklé v důsledku nefunkčnosti služeb Smluvního partnera. Případnou odpovědnost nese Smluvní partner;
- Nesprávné a nepovolené užívání Služby ze strany Smluvního partnera;
- Poruchy Služby zapříčiněné počítačovými viry, červy, spamy apod., pokud není způsobeno zanedbáním povinností Poskytovatele sjednaných ve Smluvním dokumentu;
- Doba, po kterou je Smluvní partner v prodlení s poskytnutím součinnosti,
- Nesprávné užití Služby ze strany Smluvního partnera – např. nevhodné nastavení parametrů software, síťového prvku, či nevhodná volba software nebo síťového prvku apod.,
- Plánované výpadky a údržba či update Služby, popř. jiné služby se Službou provázané, ze strany Poskytovatele,
- Doba, po kterou Smluvní partner nemůže přistoupit přes webové rozhraní Portálu, pokud je Portál prokazatelně dostupný.

13. Slovník použitých pojmů

Managed Object (MO) (chráněný cíl)

Konfigurační položka ze systému ochrany proti DDoS útokům, která obsahuje, mimo jiné, IP dresy chráněných cílů. Pro správné fungování Služby je důležité, aby byly podchyceny všechny Smluvním partnerem používané IP adresy.

Clean Traffic Příchozí datový tok, který je směrován do sítě Smluvního partnera během standardního provozu, kdy neprobíhá DDoS útok

Commited Clean Traffic Plan (CCTP)

Definuje velikost příchozího datového toku směrovaného do sítě Smluvního partnera, který je chráněn Službou proti DDoS útokům. Hodnota CCTP a její možné překročení se stanoví pomocí metody 95. percentilu. Iniciální hodnota CCTP je sjednána ve Specifikaci služby.

Denial of Service (DoS) / Distributed DoS (DDoS)

Technika útoku na internetové nebo webové služby, při níž dochází k přehlcení požadavky a pádu nebo minimálně nefunkčnosti a nedostupnosti konektivních služeb či IT infrastruktury Smluvního partnera.

Příloha č. 5 **Bezpečnostní pravidla pro významné a pro běžné dodavatele ISCS ČR**

(dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti)
(dle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti)
(Minimální bezpečnostní standard, podpůrný materiál NÚKIB, verze 1.0, ke dni 17.července 2020)

ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI				
Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti				
		Významný dodavatel (vč. KII, VIS)	Běžný dodavatel	Odkaz na ref. dok.
1.	***Řízení dodavatelů***			
1.1.	Dodavatel má povinnost se seznámit s pravidly objednatele, která zohledňují jeho požadavky systému řízení bezpečnosti informací a plnit je.	Ano	Ano	VKB, §8, odst. 1, a),d)
1.2.	Dodavatel bere na vědomí, že objednatel pravidelně přezkoumává plnění smluv s významnými dodavateli z hlediska systému řízení bezpečnosti informací.	Ano	Ne	VKB, §8, odst. 1, g)
1.3.	U významných dodavatelů v rámci uzavírání smluvních vztahů stanoví způsoby a úrovně realizace bezpečnostních opatření a určí obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.	Ano	Ne	VKB, §8, odst. 2, b)
1.4.	Dodavatel bere na vědomí, že objednatel provádí pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany.	Ano	Ne	VKB, §8, odst. 2, c)
2.	***Zvládání kybernetických bezpečnostních událostí a incidentů***			
2.1.	Dodavatel má povinnost oznamovat objednateli neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti.	Ano	Ano	VKB, §14, odst. 1, f)
3..	***Příloha č. 7 - Řízení dodavatelů – bezpečnostní opatření pro smluvní vztahy***			VKB, Příloha č. 7.

3.1.	Obsah smlouvy uzavírané s významnými dodavateli: a) ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity),	Ano	zvážit, zda je relevantní a zohlednit ve smlouvě	a)
3.2.	b) ustanovení o oprávnění užívat data,	Ano	zvážit, zda je relevantní a zohlednit ve smlouvě	b)
3.3.	c) ustanovení o autorství programového kódu, popřípadě o programových licencích, **) platí pouze pro dodavatele zakázkového SW, příp. dodavatele krabicového SW.*	Ano	zvážit, zda je relevantní a zohlednit ve smlouvě	c)
3.4.	d) ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu), **) platí pouze pro dodavatele zakázkového SW a pro dodavatele služby.*	Ano	zvážit, zda je relevantní a zohlednit ve smlouvě	d)
3.5.	e) ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem a nebudou v rozporu s požadavky povinné osoby na dodavatele,	Ano	zvážit, zda je relevantní a zohlednit ve smlouvě	e)
3.6.	f) ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou, **) platí pouze pro dodavatele zakázkového SW a pro dodavatele služby.*	Ano	zvážit, zda je relevantní a zohlednit ve smlouvě	f)
3.7.	g) ustanovení o řízení změn, **) platí pouze pro dodavatele zakázkového SW a pro dodavatele služby.*	Ano	zvážit, zda je relevantní a zohlednit ve smlouvě	g)
3.8.	h) ustanovení o souladu smluv s obecně závaznými právními předpisy,	Ano	zvážit, zda je relevantní a zohlednit ve smlouvě	h)

3.9.	i) ustanovení o povinnosti dodavatele informovat povinnou osobu o 1. kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy, 2. způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy, 3. významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy se správcem, **) platí pro všechny dodavatele, pokud součástí dodávky je i maintenance.*	Ano	zvážit, zda je relevantní a zohlednit ve smlouvě	i)
3.10.	j) specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně),	Ano	zvážit, zda je relevantní a zohlednit ve smlouvě	j)
3.11.	k) specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností), **) platí pro všechny dodavatele, pokud součástí dodávky je i maintenance.*	Ano	zvážit, zda je relevantní a zohlednit ve smlouvě	k)
3.12.	l) specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem,	Ano	zvážit, zda je relevantní a zohlednit ve smlouvě	l)
3.13.	m) pravidla pro likvidaci dat,	Ano	zvážit, zda je relevantní a zohlednit ve smlouvě	m)
3.14.	n) ustanovení o právu jednostranně odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy a **) platí pro všechny dodavatele, pokud součástí dodávky je i maintenance.*	Ano	zvážit, zda je relevantní a zohlednit ve smlouvě	n)
3.15.	o) ustanovení o sankcích za porušení povinností.	Ano	zvážit, zda je relevantní a zohlednit ve smlouvě	o)

	P04 Politika řízení dodavatelů			
5.1.	Dodavatel bere na vědomí, že objednatel provádí pravidelnou kontrolu a roční hodnocení dodavatelů.	Ano	Ne	Kap. 6.
5.2.	Dodavatel bere na vědomí, že objednatel u významných dodavatelů ve spolupráci s auditorem kybernetické bezpečnosti připravuje a realizuje plán pro provádění kontrol zavedení bezpečnostních opatření na straně dodavatele. Tento plán musí obsahovat alespoň jednu kontrolní návštěvu u dodavatele za 3 roky.	Ano	Ne	Kap. 18.
5.3.	Dodavatel bere na vědomí, že objednatel v rámci hodnocení významných dodavatelů provádí každoročně přezkoumání, zda služby, které dodavatel poskytuje, jsou dodávány v souladu se sjednanými požadavky a podmínkami, a že jsou řádně řízeny kybernetické bezpečností incidenty a související problémy.	Ano	Ne	Kap. 19.
	P07 Politika řízení přístupu			
6.1.	Dodavatel bere na vědomí, že přístup k jednotlivým aplikacím a datům systému ICT	Ano	Ano	Kap. 6.1.

	smí být povolen pouze na základě úspěšné autentizace a autorizace uživatele.			
6.2.	Přístupy musí být přidělovány identitě uživatele identifikované uživatelským jménem; identifikátory identity uživatele musí být jednoznačné a vždy spojitelné s konkrétní fyzickou osobou.	Ano	Ano	Kap. 6.1.
6.3.	Identita a její platnost musí být zavedena/měněna/rušena během procesu vzniku/změny/ukončení pracovního vztahu zaměstnance nebo na základě smluvního vztahu s dodavatelem.	Ano	Ano	Kap. 6.1.
	P22 Politika zvládání kybernetických bezpečnostních incidentů			
7.1.	Dodavatel bere na vědomí, že zhotovitel je oprávněn při přípravě a provedení testů Za přípravu a zvládání kybernetických bezpečnostních incidentů provedení testů součinnost potřebných zaměstnanců CS i dotčených dodavatelů externích služeb.	Ano	Ano	Kap. 9.1.
	Ostatní bezpečnostní dokumentace objednatele			

8.1.	Dodavatel má povinnost se seznámit s pravidly objednatele, která jsou obsažena v níže uvedeném seznamu ostatní bezpečnostní dokumentace objednatele, a která zohledňují jeho požadavky systému řízení bezpečnosti informací a plnit je:	Ano	Ano	
	a) P00 Politika kybernetické bezpečnosti ISCS	Ano	Ano	
	b) P03 Politika organizační bezpečnosti	Ano	Ano	
	c) P04 Politika řízení dodavatelů	Ano	Ano	
	d) P05 Politika bezpečnosti lidských zdrojů	Ano	Ano	
	e) P07 Politika řízení přístupu	Ano	Ano	
	f) P22 Politika zvládání kybernetických bezpečnostních incidentů	Ano	Ano	
	Minimální bezpečnostní standard, NÚKIB, (ve vztahu k dodavatelům)			
9.1.	Dodavatel bere na vědomí, že objednatel je povinen poučit relevantní osoby dodavatele o jejich povinnostech, teoreticky a prakticky je školit, seznámit je s platnými bezpečnostními politikami a kontrolovat jejich dodržování.	Ano	Ano	Kap. 5.
9.2.	V případě vyvíjeného informačního nebo komunikačního systému dodavatelem musí být definovány a dokumentovány následující požadavky:	Ano	Ano	Kap. 17.3.
	a) požadavky na licenční ujednání, vlastnictví kódu a práv duševního vlastnictví,	Ano	Ano	
	b) požadavky na osvědčení kvality a správnosti provedených prací,	Ano	Ano	
	c) požadavky na uložení zdrojového kódu,	Ano	Ano	
	d) požadavky na právo přístupu k vývoji pro audit bezpečnosti a správnosti provedené práce,	Ano	Ano	
	e) požadavky na smluvní podmínky na bezpečnost a zabezpečení kódu,	Ano	Ano	
	f) požadavky na provedení testů zranitelnosti před instalací v produkčním prostředí.	Ano	Ano	
10.1.	V případě webových aplikací je dodavatel povinen zajistit vývoj dle principů definovaných ve standardu OWASP v aktuálním znění.	Ano	Ano	Kap. 17.3.

10.2.	Pro informační nebo komunikační systém vyvíjený externím dodavatelem musí být smluvně zajištěno právo auditu zdrojového kódu a dodržování požadavků na bezpečnost. Smluvně též musí být zajištěno uložení zdrojových kódů u důvěryhodné třetí strany (code escrow) v případě, že dodavatel nepředává zdrojový kód jako součást dodávky vyvíjeného programového vybavení (informačního nebo komunikačního systému systému).	zvážit, zda je relevantní a zohlednit ve smlouvě	zvážit, zda je relevantní a zohlednit ve smlouvě	Kap. 17.3.

PRO SPOLEČNÉ ZÁŽITKY

POVĚŘENÍ

Jose Severino Perdomo Lorenzo, člen představenstva a současně generální ředitel společnosti T-Mobile Czech Republic a.s., se sídlem v Praze 4, Tomíčkova 2144/1, PSČ 148 00, IČ 64949681 (dále jen „Společnost"), oprávněný jednat za Společnost samostatně, tímto **pověřuje** níže uvedeného zaměstnance Společnosti:

, aby za Společnost jednal a vykonával:

- veškeré úkony, které souvisí se smlouvami o poskytování služeb elektronických komunikací a o prodeji komunikačních zařízení a jejich příslušenství firemním zákazníkům a se smlouvami o zprostředkování anebo spolupráci při uzavírání uvedených smluv; zejména se jedná o uzavírání, změny a ukončování takových smluv;
- veškeré úkony, které souvisí se smlouvami, které upravují komplexní řešení ProfiNet, tedy zejména, nikoli však výlučně Smlouvy o firemním řešení, Smlouvy o poskytování služeb pro veřejnou zakázku atd., či obdobné smlouvy, předložené zadavatelem, v obdobném rozsahu; prodej jakýchkoli nehlasových služeb a služeb s přidanou hodnotou; zejména se jedná o uzavírání, změny a ukončování takových smluv;
- veškeré úkony, které souvisí se smlouvami o poskytování ICT řešení, jež upravují podmínky pronájmu komunikačních zařízení a souvisejícího vybavení vč. požadované softwarové podpory; zejména se jedná o uzavírání, změny a ukončování takových smluv,
- veškeré úkony a jednání dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů; to znamená, aby podával nabídky a prováděl veškerá právní jednání ve veřejných zakázkách a výběrových řízeních, zejména svým čestným prohlášením prokazoval základní i další kvalifikační předpoklady pro plnění veřejné zakázky; rovněž aby Společnost zastupoval ve správním řízení konaném v souvislosti s jakoukoli veřejnou zakázkou nebo výběrovým řízením, a rovněž aby Společnost zastupoval v řízení před Úřadem pro ochranu hospodářské soutěže.

Pověřený zaměstnanec v takto vymezeném rozsahu a po dobu pracovního poměru ve Společnosti jedná za Společnost samostatně a je oprávněn v uvedeném rozsahu podepisovat příslušné písemnosti. Společnost výslovně prohlašuje a pověřený zaměstnanec bere na vědomí, že jakákoliv jeho jednání, která by byla v rozporu s právními předpisy, nejsou v zájmu Společnosti a nejsou ani považována za jednání v rámci činnosti Společnosti.

Pověřený zaměstnanec je dále oprávněn zmocnit jiného zaměstnance Společnosti, aby místo něho prováděl za Společnost v individuálně určených veřejných zakázkách a výběrových řízeních úkony, které nevedou ke změně práv a povinností sjednaných závazně s účinky vůči Společnosti. Pověřený zaměstnanec je zejména oprávněn zmocnit jiného zaměstnance Společnosti, aby místo něho nahlížel do protokolu o otevírání obálek, protokolu o posouzení kvalifikace nebo zprávy o posouzení a hodnocení nabídek, podával žádosti o vysvětlení zadávací dokumentace, zastupoval Společnost v elektronické aukci nebo aby se účastnil na prohlídce místa plnění nebo při ústním vysvětlení nabídky v termínech stanovených zadavateli veřejných zakázek v jednotlivých výběrových řízeních. Pověřený zaměstnanec však není oprávněn zmocnit jiného zaměstnance Společnosti, aby místo něho podepsal za Společnost smlouvu se zadavatelem, podal námitky či Společnost zastupoval v řízení před Úřadem pro ochranu hospodářské soutěže.

Podepisování pověřeného zaměstnance se děje tak, že k napsané nebo vytištěné obchodní firmě Společnosti či otisku razítka Společnosti připojí pověřený zaměstnanec svůj podpis.

V Praze, dne 13. 1. 2021

[redacted]

za T-Mobile Czech Republic a.s.

Toto pověření přijímám:

[redacted]

PROHLÁŠENÍ O PRAVOSTI PODPISU NA LISTINĚ NESEPSANÉ ADVOKÁTEM

Běžné číslo knihy o prohlášeních o pravosti podpisu **010807/446/2020/C**.

Já, níže podepsaný Mgr. Ondřej Koláček, advokát se sídlem v Praze, Jankovcova 1518/2, zapsaný v seznamu advokátů vedeném Českou advokátní komorou pod ev. č. 15742, prohlašuji, že tuto listinu přede mnou vlastnoručně ve 2 vyhotoveních podepsal **Jose Severino Perdomo Lorenzo,** [redacted]

Podepsaný advokát tímto prohlášením o pravosti podpisu nepotvrzuje správnost ani pravdivost údajů uve[redacted]ad s právními předpisy.

Praha 13. 1. 2021

[redacted]

Doložka konverze do dokumentu obsaženého v datové zprávě

Tento dokument, který vznikl převedením vstupu v listinné podobě do podoby elektronické pod pořadovým číslem **104149_006722**, skládající se z **2** listů, se doslovně shoduje s obsahem vstupu.

Vstup bez viditelného prvku.

Jméno a příjmení osoby, která konverzi provedla [redacted]

Vystavil: **Česká pošta, s.p.**
Pracoviště: **Praha 414**
Česká pošta, s.p. dne **15.01.2021**

135059931-194847-210115103706