SMLOUVA O POSKYTOVÁNÍ SLUŽEB

evid. č. ČSÚ: 059-2016-S

Níže uvedeného dne, měsíce a roku uzavřely smluvní strany:

Česká republika – Český statistický úřad
se sídlem: Na padesátém 81, Praha 10, PSČ 100 82
IČO: 000 25 593
bankovní spojení: ČNB, č. ú.: 2923001/0710
zastoupena: Mgr. Radoslavem Bulířem, ředitelem sekce ekonomické a správní na základě pověření předsedkyně ČSÚ ze dne 16. 3. 2015
(dále jen „objednatel" nebo „ČSÚ") na straně jedné

a

T-Mobile Czech Republic a.s.
se sídlem: Tomíčkova 2144/1, 148 00 Praha 4
IČ: 64949681
bankovní spojení:
zastoupena: Ing. Liborem Komárkem a Ing. Miroslavem Kláskem, na základě pověření
(dále jen „poskytovatel") na straně druhé

(objednatel a poskytovatel společně dále též jen „smluvní strany")

tuto

smlouvu o poskytování služeb

podle ust. § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „občanský zákoník"):

Preambule

Tuto smlouvu uzavírají smluvní strany na základě výběrového řízení na nadlimitní veřejnou zakázku zadávanou objednatelem jako zadavatelem ve smyslu zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „zákon o veřejných zakázkách") pod názvem „Zajištění datových služeb pro ČSÚ", interní číslo objednatele 012/2016, uveřejněnou ve Věstníku veřejných zakázek pod evidenčním číslem VZ 634803 (dále jen „veřejná zakázka").

Článek I.
Účel smlouvy, úvodní ustanovení

1. Účelem této smlouvy je zajištění datových a souvisejících služeb pro ČSÚ včetně poskytnutí ochrany proti DDoS útokům a vymezení vzájemných práv a povinností smluvních stran při poskytování služeb poskytovatelem objednateli.

3. Pro plnění předmětu této smlouvy jsou závazné rovněž všechny dokumenty vztahující se k veřejné zakázce, a to zadávací dokumentace včetně všech příloh vztahujících se k předmětu této smlouvy a nabídka poskytovatele k veřejné zakázce.

4. Poskytovatel výslovně prohlašuje, že se seznámil se zadávací dokumentací k veřejné zakázce, přičemž mu nejsou známy žádné nejasnosti či pochybnosti, které by znemožňovaly řádné plnění jeho závazků podle této smlouvy. Poskytovatel se zavazuje, že bude služby na základě této smlouvy poskytovat v souladu se zadávacími podmínkami veřejné zakázky a v souladu se svou nabídkou.

5. Poskytovatel prohlašuje, že se detailně seznámil s rozsahem a povahou předmětu plnění této smlouvy, že jsou mu známy podmínky nezbytné pro její realizaci, a že disponuje takovými kapacitami a odbornými znalostmi, včetně technického a personálního zázemí, které jsou nezbytné pro realizaci této smlouvy za dohodnutou maximální smluvní cenu uvedenou ve smlouvě, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění veřejné zakázky.

6. Poskytovatel se zavazuje plnit své závazky plynoucí z této smlouvy v souladu s platnými právními předpisy, jakož i v souladu se všemi normami obsahujícími technické specifikace a technická řešení, technické a technologické postupy nebo jiná určující kriteria k zajištění, že materiály, výrobky, postupy a služby vyhovují předmětu smlouvy a veškerým zadávacím podmínkám veřejné zakázky.

Článek II.
Výklad pojmů

Pro vyloučení pochybností smluvní strany sjednávají, že pojmy použité v této smlouvě budou mít následující význam:

DATOVÁ LINKA: soubor technických a technologických prostředků poskytovatele umožňující obousměrný přenos datových signálů

DDoS ÚTOKY: distribuované síťové útoky proti datovým linkám

SLUŽBY: služby poskytované objednateli poskytovatelem při provozu datových linek pro ČSÚ, které zahrnují: datové služby podle článku III. odst. 1. písm. a) této smlouvy a služby přeložení datových linek podle článku III. odst. 1. písm. b) této smlouvy v souvislosti se změnami adres míst plnění dle určení a požadavků objednatele. Rozsah, technická specifikace a podmínky poskytování služeb jsou uvedeny v příloze č. 1 této smlouvy.

DATOVÉ SLUŽBY: služby poskytované objednateli poskytovatelem, uvedené v článku III. odst. 1. písm. a) této smlouvy, tj. služby přenosu dat včetně ochrany proti DDoS útokům, instalace datových linek, změny kapacity nebo zrušení určených datových linek podle určení a požadavků objednatele, jejichž rozsah, technická specifikace a podmínky poskytování jsou uvedeny v příloze č. 1 této smlouvy, které zahrnují zejména: zajištění trvalého připojení do IP VPN prostřednictvím MPLS sítě včetně potřebných koncových zařízení; zajištění ochrany datových linek ČSÚ proti DDoS útokům; provozování zákaznického portálu poskytovatele; stálý monitoring všech přípojek datových linek poskytovatelem; poskytování služeb HelpDesku; migrace stávajících služeb a datových linek ČSÚ včetně implementace, ladění, testování a komunikace s předchozím operátorem; součinnost poskytovatele s objednatelem při sestavení a průběžné aktualizaci mitigačního plánu, pravidelné reporty

poskytovatele o dodržování SLA formou on-line poskytovaných údajů, jakož i další související činnosti k zajištění řádného provozu datových linek ČSÚ.

ZMĚNA KAPACITY: navýšení kapacity určených datových linek dle požadavku objednatele včetně případné změny použité technologie poskytovatelem.

PARAMETRY SLUŽEB: technické a technologické vlastnosti koncových zařízení datových linek a podmínky poskytování služeb, které jsou popsány v příloze č. 1 této smlouvy.

VÝPADEK SLUŽEB: nedodržení dostupnosti/SLA služeb podle přílohy č. 1 této smlouvy.

SOC TÝM: Security operations center team, tj. bezpečnostní tým poskytovatele zodpovědný za ochranu datových linek, jehož kvalifikaci, profesionální složení a počet členů uvedl poskytovatel v nabídce k veřejné zakázce.

PLÁN OCHRANY: Souhrn pravidel ochrany datových linek před útoky a navazující konfigurace prvků. Plán ochrany vytvoří poskytovatel na základě parametrů nastavených a definovaných objednatelem bezodkladně po podpisu této smlouvy.

Článek III.
Předmět smlouvy

1. Poskytovatel se touto smlouvou zavazuje poskytovat objednateli za sjednaných podmínek služby zahrnující:
   a) datové služby, tj. služby přenosu dat včetně ochrany proti DDoS útokům, instalace datových linek, změny kapacity nebo zrušení určených datových linek podle určení a požadavků objednatele (dále jen „datové služby");
   b) přeložení datových linek v souvislosti se změnami adres míst plnění, dle určení a požadavků objednatele,

   to vše v rozsahu a za podmínek uvedených v příloze č. 1 této smlouvy (dále jen „služby").

2. Objednatel se zavazuje poskytovateli platit za řádně poskytované služby sjednané ceny ve výši a za podmínek uvedených v článku V. této smlouvy.

Článek IV.
Místa plnění

1. *Místy plnění podle této smlouvy jsou objednatelem určená pracoviště ČSÚ, která se ke dni* podpisu smlouvy nacházejí na těchto adresách:
   - Praha 10 Na padesátém 81
   - Praha 3 Vinohradská 190
   - Brno Jezuitská 2
   - České Budějovice Žižkova 1
   - Pardubice V Ráji 872
   - Hradec Králové Myslivečkova 914
   - Jihlava Ke Skalce 30
   - Karlovy Vary Sportovní 28
   - Liberec nám. Dr. E. Beneše 585/26
   - Olomouc Jeremenkova 1142/42
   - Plzeň Slovanská alej 36

- Ostrava Repinova 2661/17
- Ústí nad Labem Špálova 2684/1
- Zlín Třída Tomáše Bati 1565

2. Případné změny v adresách míst plnění je objednatel povinen prokazatelně oznámit poskytovateli v dostatečném časovém předstihu, nejméně 40 (slovy: čtyřicet) dnů předem.

Článek V.
Ceny služeb a platební podmínky

1. Za poskytované datové služby podle čl. III. odst. 1 písm. a) této smlouvy, tj. služby přenosu dat včetně ochrany v příloze č. 1 specifikovaných datových linek před DDoS útoky, instalace datových linek a zrušení datových linek podle určení a požadavků objednatele se objednatel zavazuje uhradit poskytovateli paušální měsíční cenu ve výši uvedené v příloze č. 2 této smlouvy (dále jen „cena datových služeb"). Dojde-li v průběhu trvání této smlouvy ke změně kapacity datových linek na základě požadavku objednatele, bude cena datových služeb odpovídajícím způsobem navýšena na částku, která je uvedena v příloze č. 2 této smlouvy.

2. Za poskytované služby podle čl. III. odst. 1 písm. b) této smlouvy, tj. za přeložení datových linek podle určení a požadavků objednatele, se objednatel zavazuje uhradit poskytovateli cenu ve výši uvedené v příloze č. 2 této smlouvy.

3. K cenám služeb podle odst. 1. a 2. tohoto článku smlouvy bude připočtena DPH v sazbě podle platných právních předpisů ke dni uskutečnění zdanitelného plnění.

4. Ceny služeb jsou sjednány jako ceny nejvýše přípustné a nepřekročitelné a zahrnují veškeré náklady poskytovatele spojené s poskytováním služeb podle této smlouvy, tj. zejména:
   - v případě služeb podle článku III. odst. 1 písm. a) smlouvy: náklady spojené s přenosem dat a ochranou před DDoS útoky, náklady na dodávky koncových či jiných zařízení, práce na zprovoznění přípojek, konzultace, cla, dopravu apod., náklady na migraci datových linek včetně implementace, ladění, testování a komunikace s předchozím poskytovatelem služeb objednatele, poplatky za zrušení určených datových linek a nákladů na případnou změnu technologie v případě změny kapacity datových linek;
   - v případě služeb podle článku III. odst. 1 písm. b) smlouvy: náklady na dodávky koncových či jiných zařízení, práce na zprovoznění přeložených přípojek, konzultace, cla, dopravu apod., náklady na migraci přeložených linek včetně implementace, ladění, testování a, poplatků za zřízení určených datových linek,

   jakož i náklady na související služby a dodávky, které nejsou výslovně uvedeny v zadávací dokumentaci k veřejné zakázce nebo v této smlouvě, ale poskytovatel jako odborník o nich ví anebo má vědět, že jsou nezbytné pro řádné poskytování služeb.

5. Poskytovatel ve smyslu ust. § 1765 odst. 2 občanského zákoníku přebírá nebezpečí změny okolností po uzavření smlouvy.

6. Poskytovatel se zavazuje informovat objednatele o aktuálním cenovém vývoji služeb a aktualizovat ceny služeb dle aktuálního cenového vývoje tak, že v případě, kdy se výrazně sníží ceny za služby odpovídající službám poskytovaným podle této smlouvy, bude mezi smluvními stranami uzavřen dodatek smlouvy, na základě kterého budou ceny služeb v odpovídajícím poměru sníženy. Výrazným snížením cen se pro účely tohoto ujednání rozumí jejich snížení o více než 20%.

7. Cenu datových služeb uvedených v článku III. odst. 1. písm. a) této smlouvy bude objednatel hradit poskytovateli v paušální sjednané výši měsíčně zpětně, na základě daňových dokladů – faktur, které je poskytovatel oprávněn vystavit objednateli po akceptaci služeb za předchozí kalendářní měsíc objednatelem bez výhrad podle ustanovení článku VI. této smlouvy.

8. Cenu za služby podle článku III. odst. 1 písm. b) této smlouvy bude objednatel hradit poskytovateli na základě daňových dokladů – faktur, které je poskytovatel oprávněn vystavit objednateli po akceptaci příslušných služeb objednatelem bez výhrad podle ustanovení článku VI. této smlouvy.

9. *Každá faktura vystavená poskytovatelem na základě této smlouvy musí obsahovat* veškeré podstatné náležitosti daňového dokladu podle příslušných právních předpisů, zejména podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění a zákona č. 563/1991 Sb., o účetnictví v platném znění. Kromě těchto podstatných náležitostí musí faktury poskytovatele obsahovat evidenční číslo smlouvy objednatele, číslo účtu poskytovatele a všechny údaje uvedené v ust. § 435 odst. 1 občanského zákoníku. Fakturovaná cena musí být vyjádřena výlučně v Kč.

10. Splatnost cen vyúčtovaných fakturami poskytovatele činí 21 (slovy: dvacet jedna) dnů od doručení faktury objednateli doporučenou listovní zásilkou nebo osobně do podatelny na adresu sídla ČSÚ anebo do datové schránky objednatele.

11. Objednatel je oprávněn před uplynutím lhůty splatnosti vrátit poskytovateli fakturu, která neobsahuje požadované náležitosti, která obsahuje cenu vyúčtovanou v rozporu s touto smlouvou nebo chybně vyúčtovanou DPH. Lhůta splatnosti začíná v takovém případě znovu běžet ode dne doručení opravené faktury objednateli způsobem uvedeným v předchozím odstavci.

12. Ceny služeb se pokládají za uhrazené okamžikem odepsání příslušné částky z účtu objednatele ve prospěch účtu poskytovatele.

Článek VI.
Akceptace služeb

1. Služby poskytovatele se považují za řádně poskytnuté a akceptované objednatelem bez výhrad podpisem akceptačního protokolu, v němž bude potvrzeno, že poskytovatel služby poskytl objednateli ve sjednaném rozsahu a kvalitě.

2. Nedílnou součástí akceptačního protokolu v případě datových služeb podle článku III. odst. 1. písm. a): služeb přenosu dat a ochrany před DDoS útoky bude přehled o dodržení SLA/dostupnosti služeb přenosu dat a ochrany před DDoS útoky za příslušný měsíc poskytování těchto datových služeb.

3. Objednatel je povinen do 5 (slovy: pěti) pracovních dnů od doručení akceptačního protokolu poskytnutí služeb ve sjednaném rozsahu a kvalitě potvrdit, nebo do akceptačního protokolu uvést své výhrady k rozsahu a kvalitě poskytnutých služeb s uvedením závazného termínu pro odstranění nedostatků objednatelem anebo s uvedením výše uplatněného nároku na slevu z ceny služeb. V případě zmeškání lhůty uvedené v předchozí větě objednatelem se má za to, že objednatel služby akceptuje bez výhrad.

4. Akceptace služeb objednatelem bez výhrad anebo s výhradami, za předpokladu, že poskytovatel uzná výhrady objednatele k nedodržení SLA/dostupnosti služeb přenosu dat a ochrany před

DDoS útoky, je podmínkou oprávněnosti fakturace cen služeb v plné výši či případně snížené o příslušnou započtenou částku ve výši smluvní pokuty.

Článek VII.
Povinnosti poskytovatele a objednatele

1. Poskytovatel se zavazuje zahájit poskytování datových služeb objednateli od prvého dne třetího měsíce následujícího po nabytí účinnosti této smlouvy. Poskytovatel je zároveň povinen zajistit, v součinnosti s objednatelem a jeho stávajícím poskytovatelem datových služeb, kontinuitu poskytovaných datových služeb tak, aby v souvislosti s ukončením smluvního vztahu objednatele a stávajícího poskytovatele a uzavřením této smlouvy nedošlo k žádnému přerušení nebo výluce v poskytovaných službách.

2. Poskytovatel se zavazuje provést případnou změnu kapacity anebo zrušení datových linek podle určení a požadavků objednatele nejpozději do jednoho týdne od doručení takového požadavku objednatele. Poskytovatel bere na vědomí, že objednatel není povinen v průběhu trvání této smlouvy požádat o změnu kapacity nebo o zrušení datových linek.

3. Poskytovatel se zavazuje poskytovat objednateli služby podle této smlouvy řádně, v profesionální kvalitě a s veškerou odbornou péčí.

4. Poskytovatel se zavazuje oznámit objednateli alespoň 6 (slovy: šest) pracovních dnů předem plánované výpadky poskytovaných služeb. Tyto plánované a předem oznámené výpadky služeb nesmí překročit 5 (slovy: pět) hodin v jednom kalendářním měsíci a musí být předem odsouhlaseny objednatelem. Nevyjádří-li se objednatel k oznámení poskytovatele o plánovaných výpadcích služeb do 3 (slovy: tří) pracovních dnů od doručení oznámení, má se za to, že s oznámenými výpadky služeb souhlasí. V případě odložení výpadku musí být dodržena znovu oznamovací lhůta a odsouhlasení ze strany objednatele.

5. Poskytovatel se zavazuje po celou dobu trvání této smlouvy zachovat kvalifikaci, profesionální složení a počet členů svého SOC týmu tak, jak bylo uvedeno v nabídce k veřejné zakázce a bezodkladně písemnou formou informovat objednatele o změnách v personálním složení SOC týmu.

6. Poskytovatel se zavazuje vždy k datu vystavení faktury s vyúčtováním ceny datových služeb poskytnout objednateli elektronickou formou přehled celkových měsíčních nákladů na jednotlivé datové služby přenosu dat a ochrany před DDoS útoky s tím, že každý měsíční přehled umístí na dobu nejméně 6 (slovy: šesti) měsíců na vlastní server a oprávněným osobám objednatele umožní k přehledu on-line zabezpečený přístup prostřednictvím veřejné internetové sítě.

7. Poskytovatel je povinen podle parametrů definovaných objednatelem po podpisu této smlouvy bezodkladně vytvořit, dodržovat a průběžně aktualizovat plán ochrany po celou dobu trvání této smlouvy.

8. Poskytovatel je povinen i bez pokynů objednatele provést neodkladné úkony související s předmětem plnění podle této smlouvy, které jsou nezbytné pro zamezení vzniku škody. V případě takových úkonů bude smluvními stranami podle jejich povahy projednána a provedena případná náhrada ve smyslu ust. § 2908 občanského zákoníku.

9. Poskytovatel se zavazuje řídit se při poskytování služeb pokyny objednatele a jeho interními předpisy souvisejícími s předmětem smlouvy anebo pokyny objednatelem pověřených osob. Dále je poskytovatel povinen provádět svoje činnosti tak, aby nebyl v nadbytečném rozsahu omezen provoz v místech plnění.

10. Poskytovatel se zavazuje zajistit, aby všechny osoby, které se na jeho straně podílí na plnění předmětu smlouvy a které budou přítomny v prostorách objednatele, dodržovaly všechny bezpečnostní a provozní předpisy, především „Bezpečnostní pokyny pro obchodní partnery v oblasti požární ochrany, bezpečnosti práce a ochrany majetku", které tvoří přílohu č. 4 této smlouvy, jakož i další obdobné dokumenty, s nimiž jej objednatel seznámí.

11. Poskytovatel se zavazuje před ukončením této smlouvy poskytnout veškerou potřebnou součinnost novému poskytovateli služeb, jejichž poskytování je předmětem této smlouvy.

12. Poskytovatel souhlasí s tím, aby subjekty oprávněné podle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, provedly finanční kontrolu závazkového vztahu vyplývajícího ze smlouvy s tím, že se poskytovatel podrobí této kontrole a bude působit jako osoba povinná ve smyslu ust. § 2 písm. e) uvedeného zákona.

13. Poskytovatel se zavazuje, že bude mít po celou dobu trvání této smlouvy sjednánu platnou pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou poskytovatelem třetí osobě, s limitem pojistného plnění na jednu škodní událost minimálně 5.000.000 Kč (slovy: pět miliónů korun českých). Na vyžádání je poskytovatel povinen tuto pojistnou smlouvu doložit objednateli kdykoli v průběhu trvání této smlouvy.

14. Objednatel se zavazuje poskytovat po celou dobu trvání smlouvy poskytovateli součinnost nezbytnou k řádnému poskytování služeb.

15. Objednatel prohlašuje, že jeho zaměstnanci nebo jiné osoby, jím označené jako spolupracující a kontaktní osoby, splňují všechny kvalifikační požadavky potřebné pro zajištění součinnosti k plnění předmětu smlouvy a jsou k takové činnosti jménem objednatele kompetentní.

Článek VIII.
Subdodavatelé

1. Poskytovatel je oprávněn zajistit provádění instalačních a migračních prací při poskytování služeb uvedených v článku III. odst. 1. písm. a) a b) této smlouvy prostřednictvím subdodavatelů, jejichž specifikace, včetně specifikace dílčích částí plnění, které budou těmito subdodavateli poskytovány, je obsažena v příloze č. 3 této smlouvy.

2. Poskytovatel není oprávněn zajistit prostřednictvím subdodavatelů poskytování datových služeb uvedených v článku III. odst. 1. písm. a) této smlouvy, s výjimkou provádění instalačních a migračních prací.

3. Poskytovatel se zavazuje zajistit, že subdodavatelé budou jimi prováděné části služeb provádět v souladu se všemi podmínkami této smlouvy. Tím není dotčena výlučná odpovědnost poskytovatele za poskytování řádného plnění podle této smlouvy; poskytovatel tedy odpovídá objednateli za řádné poskytování služeb, které svěřil subdodavatelům, ve stejném rozsahu, jako by je poskytoval sám.

4. Poskytovatel je oprávněn změnit subdodavatele pouze z vážných objektivních důvodů a s předchozím písemným souhlasem objednatele; objednatel se zavazuje souhlas se změnou subdodavatele poskytovateli bezdůvodně neodpírat.

5. Poskytovatel je povinen předložit objednateli seznam subdodavatelů, kterým za plnění subdodávky uhradil více než 10% z celkové ceny veřejné zakázky uhrazené objednatelem jako

veřejným zadavatelem v jednom kalendářním roce, a to nejpozději do 28. 2. následujícího kalendářního roku.

6. Má-li subdodavatel právní formu akciové společnosti, je poskytovatel povinen společně se seznamem subdodavatelů podle předchozího odstavce předložit objednateli seznam vlastníků akcií, jejichž jmenovitá hodnota přesahuje 10% základního kapitálu. Seznam vlastníků akcií musí být vyhotoven nejpozději 90 (slovy: devadesát) dnů před dnem předložení seznamu subdodavatelů.

Článek IX.
Ochrana důvěrných informací

1. Poskytovatel se zavazuje zachovávat mlčenlivost ohledně skutečností, které se v souvislosti s plněním smlouvy dozvěděl nebo které objednatel označil za důvěrné, jakož i údajů dle zákona č. 89/1995 Sb., o státní statistické službě, v platném znění (dále jen „důvěrné informace"). Důvěrné informace budou poskytovatelem použity výhradně k činnostem, kterými bude zajištěno dosažení účelu smlouvy. Poskytovatel nesdělí či nezpřístupní žádnou z důvěrných informací třetím osobám, nevyužije ji k vlastnímu prospěchu nebo jinak nezneužije. Povinnost mlčenlivosti a zachování důvěrnosti informací se nevztahuje na informace, které se staly obecně známými za předpokladu, že se tak nestalo porušením některé z povinností vyplývajících ze smlouvy, nebo o kterých tak stanoví zákon, zpřístupnění je však možné vždy jen v nezbytném rozsahu.

2. Za důvěrné se nepovažují fakturační údaje poskytovatele a dále takové informace, které je objednatel, jako organizační složka státu, povinen zveřejňovat. Sdělení informací nezbytných pro dosažení účelu smlouvy subdodavatelům poskytovatele není porušením povinnosti mlčenlivosti podle odstavce 1. tohoto článku smlouvy.

3. Poskytovatel se rovněž zavazuje pro případ, že se v průběhu plnění předmětu smlouvy dostane do kontaktu s osobními údaji, že je bude ochraňovat a nakládat s nimi v plně v souladu s příslušnými právními předpisy, zejména se zákonem č. 101/2000 Sb., o ochraně osobních údajů, v platném znění (dále jen „zákon o ochraně osobních údajů"). Smluvní strany se v případě kontaktu s osobními údaji, který bude spadat pod zákon o ochraně osobních údajů, zavazují uzavřít dodatek ke smlouvě, jehož obsahem bude dohoda o zpracování osobních údajů.

Článek X.
Sankce

1. V případě prodlení poskytovatele se zahájením poskytování datových služeb v termínu podle článku VII. odst. 1 této smlouvy je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 50.000 Kč (slovy: padesát tisíc korun českých) za každý započatý den prodlení.

2. V případě nesplnění kteréhokoli parametru služeb uvedených u datových linek v příloze č. 1 této smlouvy je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 100.000 Kč (slovy: jedno sto tisíc korun českých) za každý jednotlivý případ takového porušení smluvní povinnosti.

3. V případě nesplnění kteréhokoli parametru služeb uvedeného v příloze č. 1 v technickém popisu ochrany proti DDoS útokům je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 250.000 Kč (slovy: dvě stě padesát tisíc korun českých) za každý jednotlivý případ takového porušení smluvní povinnosti.

4. V případě, že dojde během jednoho kalendářního měsíce k více než jednomu neplánovanému, poskytovatelem neoznámenému anebo objednatelem neschválenému výpadku služeb, je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši:

- 2.000 Kč (slovy: dva tisíce korun českých) za každou započatou hodinu nedodržení SLA u datových linek pro Internet;
- 1.000 Kč (slovy: jeden tisíc korun českých) za každou započatou hodinu nedodržení SLA u datových linek pro MPLS s kapacitou nad 50 Mbps;
- 500 Kč (slovy: pět set korun českých) za každou započatou hodinu nedodržení SLA u datových linek pro MPLS s kapacitou do 50 Mbps včetně.

5. V případě porušení povinností poskytovatele podle článku VII. odst. 5, 13 a článku VIII. odst. 2 této smlouvy je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 100.000 Kč (slovy: jedno sto tisíc korun českých) za každý jednotlivý případ porušení smluvní povinnosti.

6. V případě porušení povinností poskytovatele podle článku IX. této smlouvy je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 500.000 Kč (slovy: pět set tisíc korun českých) za každý jednotlivý případ porušení smluvní povinnosti.

7. V případě porušení kterékoli jiné smluvní povinnosti poskytovatele je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 5.000 Kč (slovy: pět tisíc korun českých) za každý den prodlení a každý jednotlivý případ porušení smluvní povinnosti.

8. Splatnost smluvních pokut nastává dnem porušení smluvní povinnosti. Poskytovatel se zavazuje zaplatit smluvní pokutu ve lhůtě uvedené ve výzvě objednatele k zaplacení smluvní pokuty. Objednatel je oprávněn jednostranně započíst svou pohledávku za poskytovatelem z titulu smluvní pokuty vůči jakékoli splatné pohledávce poskytovatele za objednatelem.

9. Ujednáním o smluvních pokutách není dotčen nárok objednatele na náhradu škody vzniklé v důsledku porušení smluvní povinnosti, kterou je objednatel oprávněn požadovat vedle smluvní pokuty v plné výši. Tím není dotčeno ustanovení § 64 odst. 12 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů.

10. V případě prodlení objednatele s uhrazením ceny služeb je poskytovatel oprávněn požadovat zaplacení úroku z prodlení ve výši podle platných právních předpisů k prvnímu dni prodlení.

Článek XI.
Platnost a účinnost smlouvy, ukončení smlouvy

1. Tato smlouva nabývá platnosti a účinnosti dnem jejího podpisu oprávněnými zástupci obou smluvních stran.

2. Tato smlouva se uzavírá na dobu určitou 48 (slovy: čtyřiceti osmi) měsíců od data zahájení poskytování datových služeb podle článku VII. odst. 1. této smlouvy.

3. Před uplynutím sjednané doby trvání lze tuto smlouvu ukončit na základě písemné dohody smluvních stran, jednostranným odstoupením od smlouvy nebo výpovědí objednatele.

4. Smluvní strany jsou oprávněny od této smlouvy jednostranně odstoupit s účinky do budoucna v případě jejího podstatného porušení druhou smluvní stranou s tím, že za podstatné porušení smlouvy se pro účely tohoto ujednání považuje zejména:
   - prodlení poskytovatele se zahájením poskytování datových služeb v termínu podle článku VII. odst. 1 této smlouvy delší než 10 (slovy: deset) dnů;
   - dojde-li během jednoho kalendářního měsíce k více než jednomu neplánovanému výpadku služeb nad rámec SLA v délce min. 8 hodin;

- porušení kterékoli z povinností poskytovatele uvedených v článku VII. odst. 4, článku VIII. odst. 2 a článku IX. této smlouvy;
- nesplnění, byť i jediného z parametrů služeb uvedených v příloze č. 1 této smlouvy, včetně parametrů služeb uvedených v technickém popisu ochrany proti DDoS útokům, a to i u jediné datové linky;
- ocitne-li se poskytovatel v úpadku ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení;
- prodlení objednatele s uhrazením ceny služeb po dobu delší než 30 (slovy: třicet) dnů.

5. Objednatel je oprávněn od této smlouvy jednostranně odstoupit s účinky do budoucna v případě neschválení finančních prostředků ze státního rozpočtu na plnění poskytované na základě této smlouvy pro příslušné období. Případné neschválení finančních prostředků ze státního rozpočtu na příslušné období je objednatel povinen bezodkladně písemnou formou oznámit poskytovateli.

6. Účinky odstoupení od smlouvy nastávají dnem doručení písemného oznámení odstupující smluvní strany, kdy přednost má datum doručení do datové schránky, druhé smluvní straně, nebo k datu pozdějšímu, které bude uvedeno v oznámení o odstoupení.

7. Odstoupení od smlouvy se nedotýká práva na zaplacení smluvních pokut, úroku z prodlení, práva na náhradu škody vzniklé z porušení smluvní povinnosti ani ujednání, které má vzhledem ke své povaze zavazovat smluvní strany i po odstoupení od smlouvy.

8. Objednatel je oprávněn tuto smlouvu bez udání důvodu vypovědět, a to jako celek, nebo zčásti, tj. ohledně jednotlivých služeb, datových linek, resp. míst plnění. Výpověďní lhůta je tříměsíční a počne běžet prvého dne kalendářního měsíce následujícího po doručení písemné výpovědi poskytovateli.

Článek XII.
Závěrečná ustanovení

1. Tuto smlouvu lze měnit a doplňovat pouze vzestupně číslovanými písemnými dodatky podepsanými oprávněnými zástupci obou smluvních stran.

2. Práva a povinnosti vzniklé na základě této smlouvy nebo v souvislosti s ní se řídí českým právním řádem, zejména občanským zákoníkem.

3. Neplatnost nebo neúčinnost některého ustanovení této smlouvy nezpůsobuje neplatnost nebo neúčinnost celé smlouvy. V případě, že některé ustanovení této smlouvy bude neplatné nebo neúčinné, zavazují se smluvní strany nahradit takové neplatné nebo neúčinné ustanovení platným a účinným ustanovením, které bude co do obsahu a významu neplatnému nebo neúčinnému ustanovení co nejblíže.

4. Veškerá oznámení podle této smlouvy musí být učiněna písemně a zaslána všem oprávněným osobám ve věcech technických druhé smluvní strany, do datové schránky, doporučenou poštou, prostřednictvím elektronické pošty nebo osobně do podatelny.

5. Smluvním jazykem je jazyk český, v českém jazyce bude probíhat veškerá komunikace a musí být zpracovány veškeré dokumenty související s plněním předmětu smlouvy.

6. Poskytovatel bere na vědomí skutečnost, že tato smlouva podléhá povinnosti zveřejnění plného znění v souladu s ustanovením § 147a zákona o veřejných zakázkách a uděluje s tímto zveřejněním anebo zveřejněním podle zákona č. 106/1999 Sb., o svobodném přístupu

k informacím, ve znění pozdějších předpisů nebo podle jiných právních předpisů bezvýhradní souhlas.

7. Smluvní strany se dohodly, že veškeré sporné záležitosti, které se vyskytnou a budou se týkat závazků vyplývajících z této smlouvy, budou prioritně řešit dohodou a případnému soudnímu sporu bude vždy předcházet snaha smluvních stran o řešení sporu smírem. Smluvní strany se dohodly, že v případě řešení sporů soudní cestou bude místně příslušným soudem Obvodní soud pro Prahu 10, popřípadě Městský soud v Praze.

8. Nedílnou součástí této smlouvy jsou tyto přílohy:
   - příloha č. 1: Rozsah a technická specifikace služeb
   - příloha č. 2: Ceny služeb
   - příloha č. 3: Specifikace subdodavatelů
   - příloha č. 4: Bezpečnostní pokyny pro obchodní partnery v oblasti požární ochrany, bezpečnosti práce a ochrany majetku

9. Oprávněnými osobami smluvních stran ve věcech technických jsou:

Za objednatele:	Ing. Iva Auingerová e-mail: tel.:	Ing. Jiří Lejnar e-mail: tel.:
Za poskytovatele:	Dohledové centrum T-Mobile e-mail: tel.:	Roman Pieklak e-mail: tel.

10. Tato smlouva byla sepsána ve čtyřech vyhotoveních, z nichž po dvou obdrží každá ze smluvních stran.

11. Smluvní strany prohlašují, že tato smlouva byla sepsána podle jejich pravé a svobodné vůle, vážně, určitě a srozumitelně, že si ji přečetly a s jejím obsahem souhlasí.

V Praze dne 13. 10. 2016

.....

Česká republika – Český statistický úřad
Mgr. Radoslav Bulíř, ředitel
sekce ekonomické a správní

V Praze dne .....

.....

T-Mobile Czech Republic a.s.
Ing. Libor Komárek na základě pověření
Senior manažer prodeje státní správě

.....

T-Mobile Czech Republic a.s.
Ing. Miroslav Klásek na základě pověření
Senior manažer presalesu

Příloha č. 1
Smlouvy o poskytování služeb

ROZSAH A TECHNICKÁ SPECIFIKACE SLUŽEB

Příloha č. 2
Smlouvy o poskytování služeb

CENY SLUŽEB

Příloha č. 1

Technická specifikace soutěžených služeb

1. Parametry služeb:

- Trvalé připojení do IP VPN prostřednictvím MPLS sítě včetně potřebných koncových zařízení, placené paušálně za použití technologií:
  - Leased Line – Wired (LL,-SHDSL);
  - Leased Line – Wireless (licencované pásmo);
  - Ethernet – metalický;
  - Ethernet – optický;

- Symetrické (upstream = downstream) linky s kapacitou plně duplexní, nesmí být využito žádné asymetrické xDSL technologie

- Koncová zařízení pro linky pro připojení do Internetu musí podporovat IPv6;

- Ochrana před podvržením zdrojových IP adres bezstavovým paketovým filtrem (anti spoofing filter) – jiné bezpečnostní služby (např. antivirové, antispamové) nejsou požadovány;

- Fyzická přípojka není sdílena - poskytována 1 VPN vyvedená na na 1 ethernetovém portu;

- Rozhraní:
  - metalické rozhraní (konektor RJ-45), přičemž typ rozhraní závisí na poptané kapacitě přípojky;
  - optické rozhraní, přičemž typ rozhraní závisí na poptané kapacitě přípojky;

- Možnost zvýšení rychlosti bez změny technologie do 1 týdne od podání požadavku:
  - Připojka internet 200 Mbit/s – do 0,5 Gbit/s;
  - Připojka internet 32 Mbit/s – do 50 Mbit/s;
  - *Přípojka MPLS 184 Mbit/s – do 0,5 Gbit/s;*
  - Přípojka MPLS 32 Mbit/s – do 50 Mbit/s;
  - Přípojka MPLS 16 Mbit/s – do 32 Mbit/s;
  - Přípojka MPLS 8 Mbit/s – do 16 Mbit/s;

- Redundance (MPLS i Internet):
  - Centrála a záložní lokalita (lokalita Praha) – plná redundance 2 nezávislými směry včetně koncových zařízení;
  - Krajská pracoviště – záložní připojení v šířce pásma min. 25% primárního připojení. Záložní připojení musí být vybaveno samostatným koncovým zařízením.
- Přepínání provozu (Internet):
  - Řešení musí na vyžádání umožnit přepnutí provozu mezi centrálou a záložní lokalitou.Přepnutí provozu musí být realizováno na vrstvě L3 v rámci routování BGP, případně OSPF protokolem bezodkladně

Poptávané služby včetně SLA (MPLS):

Místo			Dostupnost (SLA) [%/měsíc]	Max. latence při 75% vytížení linky [ms]	Šířka pásma
Praha 10	Na padesátém	81	99,99%	100	184 Mbit/s
Praha 3	Vinohradská	190	99,99%	100	32 Mbit/s

Brno	Jezuitská	2	99,99%	100	16 Mbit/s
České Budějovice	Žižkova	1	99,99%	100	16 Mbit/s
Pardubice	V Ráji	872	99,99%	100	16 Mbit/s
Hradec Králové	Myslivečkova	914	99,99%	100	16 Mbit/s
Jihlava	Ke Skalce	30	99,99%	100	8 Mbit/s
Karlovy Vary	Sportovní	28	99,99%	100	8 Mbit/s
Liberec	nám. Dr. E.Beneše	585/26	99,99%	100	8 Mbit/s
Olomouc	Jeremenkova	1142/42	99,99%	100	8 Mbit/s
Plzeň	Slovanská alej	36	99,99%	100	16 Mbit/s
Ostrava	Repinova	2661/17	99,99%	100	16 Mbit/s
Ústí nad Labem	Špálova	2684/1	99,99%	100	16 Mbit/s
Zlín	Třída Tomáše Bati	1565	99,99%	100	8 Mbit/s

Poptávané služby včetně SLA (Internet):

Místo			Dostupnost (SLA) [%/měsíc]	Max. latence při 75% vytížení linky [ms]	Šířka pásma
Praha 10	Na padesátém	81	99,99%	100	200 Mbit/s
Praha 3	Vinohradská	190	99,99%	100	32 Mbit/s

- *Zadavatel požaduje pro každou lokalitu přiložit detailní technický popis řešení poptávané linky* minimálně v rozsahu[i]:
  - Použitá technologie včetně parametrů detailně specifikujících vrstvu L1
  - *Typ a technický popis nasazených koncových zařízení na straně uchazeče*
  - Přesná lokalizace přípojných bodů na straně uchazeče na úroveň konkrétního umístění zařízení
  - Vhodně strukturovaný technický popis[ii], dokládající nezávislé vedení tras*)

*) nezávisle vedenou trasou se pro účely této zadávací dokumentace rozumí trasa v celé své délce dostatečně prostorově vzdálená od alternativní trasy tak, že případné znefukčnění alternativní trasy například technickým zásahem třetí strany v rámci stavebních nebo údržbových prací funkcionalitu nezávisle vedené trasy nijak neovlivní

2. Služba ochrany před DDoS útoky

Zadavatel požaduje na právě provoz přenášející lince pro připojení do internetu (Praha 10, Na padesátém 81 – linka 200 Mbit/s nebo Praha 3, Vinohradská 190 – linka 32 Mbit/s) aktivně a nepřetržitě nasazenou službu zabezpečující tuto linku proti DDoS útokům a to za splnění následujících podmínek:

Parametr	Požadavek	Nabízené plnění
Ochrana proti DDoS útokům implementována na všech vstupních bodech vlastní sítě (národní peeringová centra, mezinárodní konektivity)	Ano	Ano
Předem dohodou v písemné formě mezi provozovatelem a zákazníkem stanovený plán ochrany, který obsahuje minimálně:		
Zákazníkem definované odchylky v režimu detekce vůči standardnímu chování služby	Ano	Ano
Zákazníkem definované odchylky v režimu ochrany	Ano	Ano

vůči standardnímu chování služby		
Zákazníkem definované jiné než standardní ochranné postupy (blokování IP adres i celých sítí, filtrování nebo zákaz provozu některých protokolů…)	Ano	Ano
V režimu monitoringu sleduje příchozí provoz minimálně na vrstvách L3 a L4 v režimu 24/7 přičemž alespoň:		
Analyzuje na vzorcích provoz na výskyt protokolových anomálií	Ano	Ano
Analyzuje vzorkované pakety/rámce na výskyt chyb a anomálií v hlavičkách	Ano	Ano
Detekuje známé útoky dle signatur, získávaných pravidelně a opakovaně v kratších než denních intervalech z renomované databáze specializované pro tento účel s celosíťovým dosahem (atlas.arbor.net nebo obdoba)	Ano	Ano
V režimu ochrany, spouštěném automaticky na základě plánu ochrany a vyhodnocení z monitoringu minimálně:		
Po neomezenou dobu zákazníkův provoz analyzuje v celém objemu datového toku a odstraňuje z něj nelegitimní části („mitigace") tak, aby zákazníkovi byl *doručována již pouze jeho požadovaná legitimní* části	Ano	Ano
Informuje zákazníka bezodkladně o každém jednotlivém zahájení režimu ochrany i o jeho ukončení (SMS a e-mail, volitelně telefon)	Ano	Ano
V operátorském režimu v součinnosti se zákazníkem aktivuje další ochranné postupy	Ano	Ano

Zadavatel požaduje, aby uchazeč provozoval zákaznický portál s minimálně následujícími funkcionalitami:

Parametr	Požadavek	Nabízené plnění
Sledování zatížení (bit/s, pkt/s)chráněné linky on-line	Ano	Ano
Sledování detailů probíhajících mitigací on-line	Ano	Ano
Prohlížení minimálně tříměsíční historie průběhu ukončených režimů ochrany včetně mitigací on-line	Ano	Ano
Detailní report o průběhu každé ukončené mitigace včetně chronologického seznamu užitých *ochranných opatření a vyhodnocení jejich účinnosti*	Ano	Ano

- Zadavatel požaduje:
  - Zajištění referenční návštěvy pro sledování řešení ochrany proti DDoS v reálném provozu
  - Přiložení technického popisu a funkčního schématu řešení ochrany proti DDoS[iii].
  - Přiložení návrhu plánu ochrany datových linek před útoky a navazující konfigurace prvků[iv]
  - Přiložení detailního popisu činnosti členů SOC týmu v době aktivovaného režimu ochrany[v].

Poptávané služby včetně SLA (ochrana před DDos):

Místo			Dostupnost monitoringu [%/měsíc]	Dostupnost režimu ochrany [%/měsíc]	Maximální doba pro oznámení/plná aktivace režimu ochrany
Praha 10	Na padesátém	81	99%	99,99%	15/10
Praha 3	Vinohradská	190	99%	99,99%	15/10

3. Další požadavky – všechny služby:

Parametr	Požadavek	Nabízené plnění
Monitoring všech přípojek v režimu 24x7x365 a jejich proaktivní správa a odstraňování poruch bez nutnosti Zadavatele poruchu nahlásit	Ano	Ano
Poskytování služeb HelpDesku v rozsahu 24x7x365	Ano	Ano
Komunikace v českém nebo slovenském jazyce	Ano	Ano
Migrace stávajících služeb a linek včetně implementace, ladění, testování a komunikace se stávajícím operátorem (cena musí být součástí paušálního poplatku)	Ano	Ano
Uchazeč zajistí součinnost při sestavení a průběžné aktualizaci plánu ochrany	Ano	Ano
Sledování detailů probíhajících mitigací on-line	Ano	Ano
Plná odpovědnost za funkčnost linek a koncových zařízení	Ano	Ano
On-line dostupný report o dodržování SLA za celou doby trvání smlouvy	Ano	Ano

- Poskytnutí kontaktních osob (zastupitelných) v režimu 12x5 (s výjimkou bezpečnostního zástupce):
  - Technická řešení (technický zástupce);
  - Administrativní a ekonomické záležitosti (obchodní zástupce);
  - Bezpečnostní řešení (bezpečnostní zástupce) – režim 24x7;

Příloha č. – 2.1 Detailní technický popis řešení poptávané linky pro každou lokalitu
Příloha č. - 2.2 Strukturovaný technický popis, dokládající nezávislé vedení tras

NEZVEŘEJŇUJÍ SE PŘÍLOHY Č. 2.1 a 2.2.
Přílohy obsahují konkrétní detailní technický popis nabízeného řešení, včetně potenciálně citlivých informací o nastavení infrastruktury. Jako takové mohou potenciálním útočníkům prozradit informace, které jim umožní lépe zacílit jejich snahu o narušení aktiv ČSÚ, proniknutí do sítě ČSÚ nebo realizaci útoků s cílem znepřístupnit služby ČSÚ jejich oprávněným uživatelům.

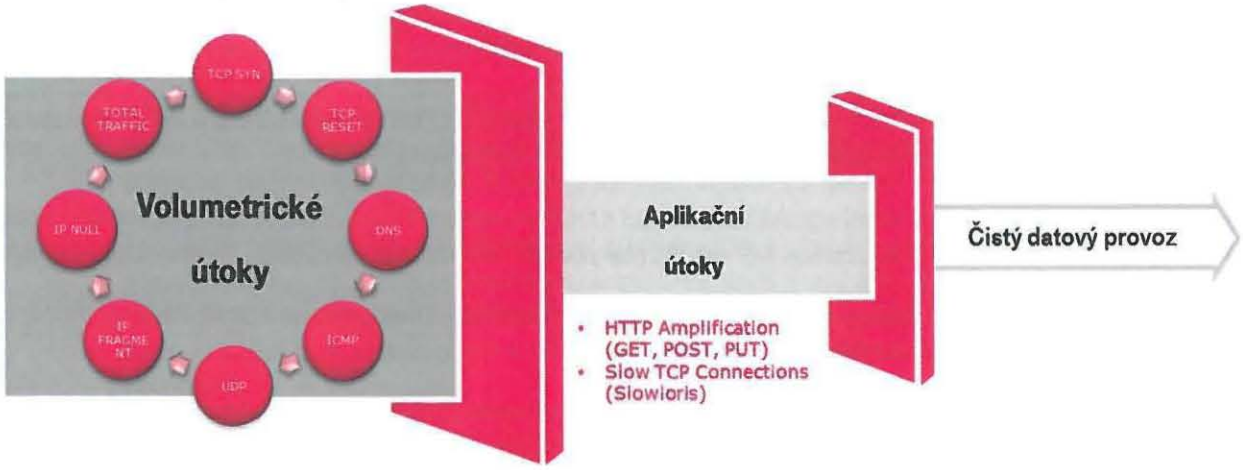
Příloha č. – 2.3 Technický popis a funkční schéma řešení ochrany proti DDoS

Popis 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.



Služba DDoS ochrana od společnosti T-Mobile Czech Republic je aktuálně schopna ochránit síť zákazníka proti volumetrickým útokům o kapacitě až **60 Gbps**.

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

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.

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

Popis služby DDoS ochrana - operátorská vrstva

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.

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.

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	-	-	+

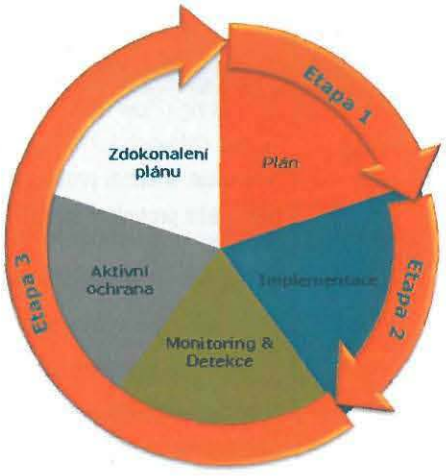
Varianta **Bronze** je vhodná pro organizace, které potřebují zajistit detekci DDoS útoků a proaktivní informování v případě útoku. Tato varianta nezahrnuje aktivní ochranu. Tuto je možno si doplatit. Doplatek za aktivní ochranu se je kalkulován za každý započatý den čištění provozu.

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.

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.

Principy 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.

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

Je vhodné zdůraznit **garantované reakční doby**, které zajistí real-time ochranu proti DDoS útokům.

Nejedná se tedy pouze o vlastní dostupnost či výkonnostní parametry technologie samotné, ale rovněž o její **provázanost na související procesy a lidskou obsluhu**.

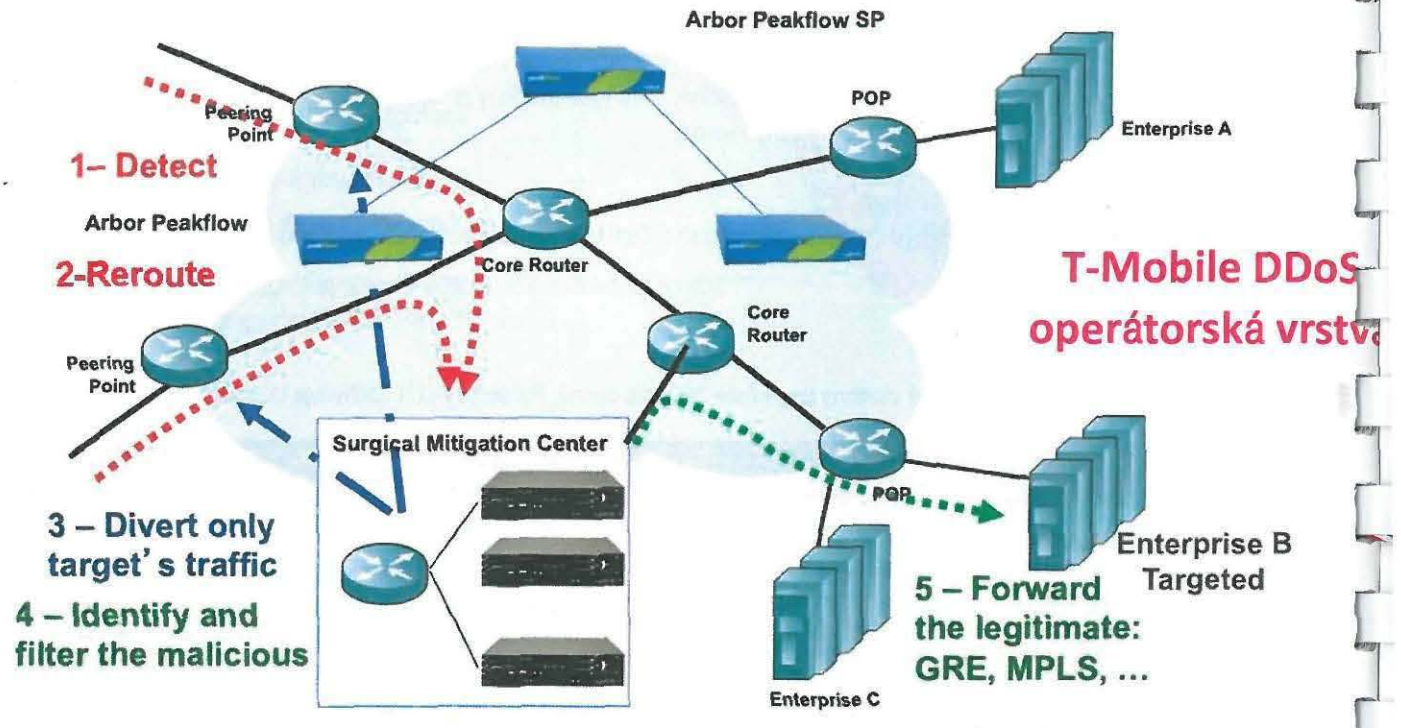
Cílem je vytvořit garantovanou účinnou ochranu proti DDoS útokům, které často mění svůj charakter i sílu a vzájemně se kombinují.

Toto se bez **špičkové technologie** a dobře **fungujícího SOC týmu** nedá zajistit.

Architektura nabízeného řešení

Nabízené řešení se je založeno na využití ochranného DDoS štítu, vybudovaného T-Mobile na technologii ARBOR. Jedná se o špičkovou technologii, kterou celosvětově využívá více než 80% poskytovatelů.

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).

Celková **lokální** mitigační kapacita je **60 Gbps**.

Celková mitigační kapacita se zapojením nadřazeného DTAG DDoS ochranného štítu je **v řádech stovek Gbps**.

Automitigace

Analytický modul na základě vstupních informací z core routerů, které získává pomocí Flow, **SNMP** a **BGP**, **automaticky** vyhodnotí typ útoku a připraví úvodní sadu protiopatření tak, aby všechny známé útoky mohly být okamžitě **automaticky mitigovány**.

Po aktivaci mitigačního modulu, se úvodní sada protiopatření doplní o další, která jsou vytvořena na základě podrobné analýzy datového toku (inspekce obsahu paketů).

Ať už se jedná o volumetrický flood útok na kapacitu datového připojení nebo útok cílený na konkrétní webový server oběti, **již za 4 sekundy** dokáže Arbor platforma **útok izolovat a odstranit**, aniž by to ovlivnilo ostatní uživatele.

Vše, co Arbor dokáže detekovat, dokáže i mitigovat.

Arbor řešení se neustále učí a adaptuje v reálném čase, upozorňuje operátory jak na DDoS útoky, tak na neobvyklé změny úrovní požadavků a provozu.

Metody potlačení DDoS útoku zahrnují identifikaci škodlivých hostitelů a jejich zaneseni na "černou listinu", mitigaci založenou na umístění IP adres útočníků, filtraci založenou na detekci protokolových anomálií, odstranění zdeformovaných paketů a omezení rychlosti (pro elegantní zvládnutí špiček legitimního provozu).

Mitigace může být automatická nebo iniciována operátorem a protiopatření je možné kombinovat, aby bylo možné adresovat kombinované útoky.

Podporované detekční metody a schopnosti mitigace řešení Arbor jsou uvedeny níže.

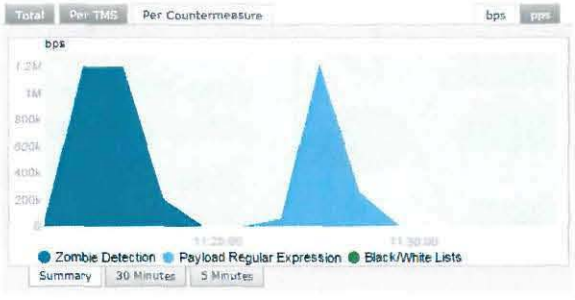
Arbor - detekční metody
ATLAS Intelligence Feed (AIF)
Blacklist Fingerprints
DNS Authentication
DNS Malformed
DNS Rate Limiting
DNS Regular Expression
DNS Scoping
HTTP Authentication
HTTP Malformed
HTTP Rate Limiting
HTTP Scoping
HTTP/URL Regular Expression
Inline Filter
Invalid Packets
IP Location Filter Lists
IP Location Policing
IPv4/IPV6 Address Filter Lists
IPv4/IPV6 Black/White Filter Lists
Packet Header Filtering
Payload Regular Expression Filter
Per Connection Flood Protection
Protocol Baselines
Shaping
SIP Malformed
SIP Request Limiting

SSL Negotiation
TCP Connection Limiting
TCP Connection Reset
TCP Syn Authentication
Zombie Detection

Uživatelské rozhraní

Řešení Arbor umožňuje zákazníkovi prostřednictvím webového rozhraní **sledovat** probíhající mitigaci **v reálném čase**.

Každá čistící procedura poskytuje v průběhu čištění **podrobnou číselnou statistiku** o potlačeném a propuštěném provozu a to v detailu **dle jednotlivých protiopatření**. (viz. obrázek níže jako příklad zobrazení účinnosti dvou vybraných protiopatření během testovacího útoku)



Celé řešení Arbor je postaveno jako vysoce dostupné (**HA architektura**) a to i včetně portálů uživatelského rozhraní.

Webové rozhraní je pro **zvýšení bezpečnosti** přístupné pouze z evidovaných adres zákazníka a interní sítě TMCZ.

Webové stránky se dají zobrazit i **na prohlížeči v mobilním zařízení** (speciální mobilní aplikace není k dispozici)

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 odmitnutí 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.

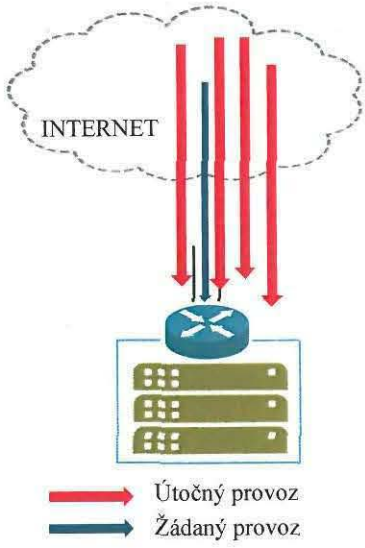
Během útoku je čistý, legitimní provoz potlačen obrovským počtem požadavků, který generují útočící stroje. Proto hlavním smyslem obrany je ochránit legitimní provoz a zajistit jeho doručení k cíli, ale přitom odstranit datový tok útočníků, kteří přetěžují linky a cílové počítače – servery.

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 (10x - 100x)

Příloha č. – 2.5 Detailní popis činnosti členů SOC týmu v době aktivovaného režimu ochrany

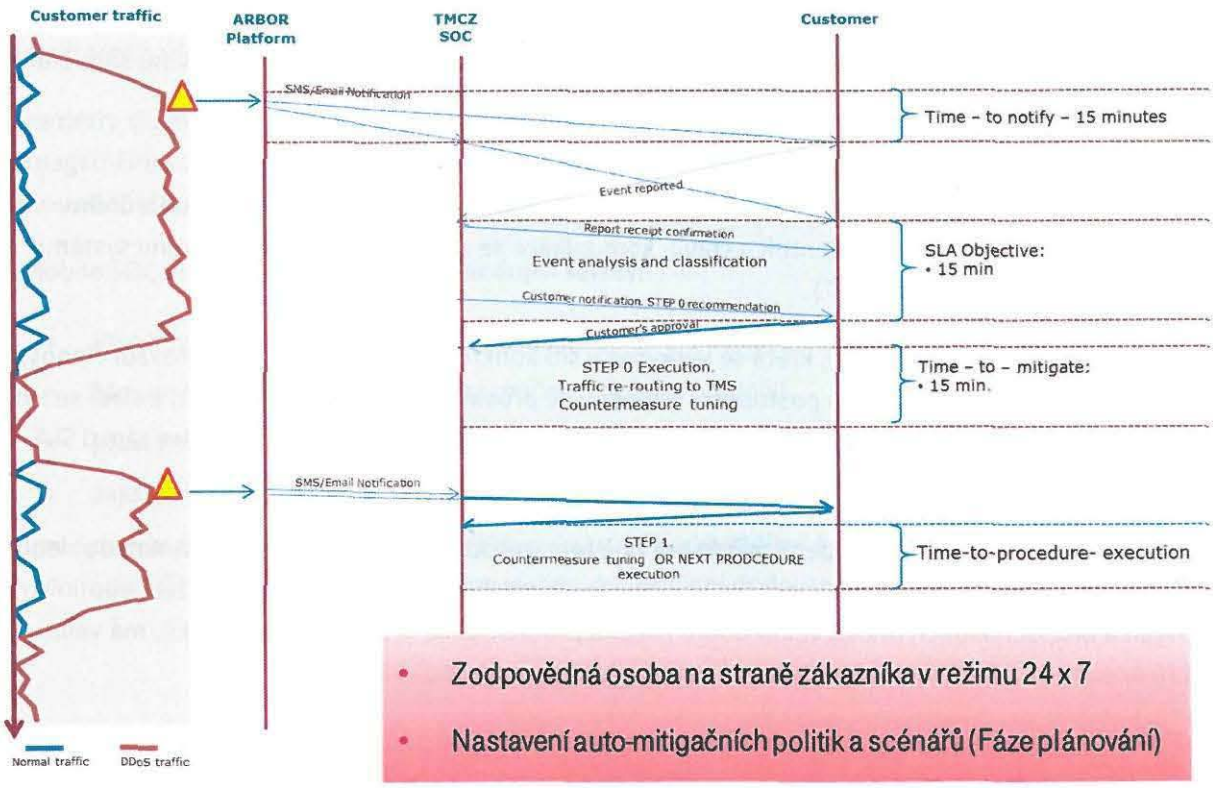
V případě záplavového (volumetrického) útoku na zákazníkem definované chráněné cíle v síti T-Mobile, vyšle monitorovací část operátorské vrstvy DDoS ochrany alarm na SOC T-Mobile.

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.

Potlačení DDoS útoku – časový harmonogram

Diagram níže popisuje v chronologickém sledu jednotlivé procesní kroky probíhající při potlačení DDoS útoku.



Služby SOC

Princip fungování T-Mobile SOC, **kompetence** jednotlivých skupin SOC a **kvalifikaci** SOC je popsán níže:

Oblast bezpečnosti je výrazně rostoucím tématem, které díky zvyšující se mobilitě a elektronizaci veškerých dat a informací, nabývá klíčového významu. V souvislosti s tímto trendem dochází v celé řadě společností ke změně pohledu a přístupu k řízení informační bezpečnosti.

T-Mobile, jako klíčový ISP poskytovatel a komunikační společnost poskytující komplexní ICT služby, v návaznosti na tento trend vytvořil koncept nazvaný Bezpečná firma (Secure company), jehož cílem je rozvíjet schopnosti T-Mobile v oblasti služeb informační bezpečnosti a to především v oblastech konzultace, zabezpečení síťové a aplikační vrstvy a prostředí koncových stanic.

Nedílnou součástí konceptu Bezpečná firma je oblast bezpečnostního dohledu, který se v důsledku rostoucí hrozby kybernetické kriminality a jejích dopadů, stává nutností pro celou řadu firem.

Vybudování vlastního centra bezpečnostního dohledu, často nazývaného jako SOC – Security Operation Center, je pro většinu středních a větších firem neefektivní cíl a to především s ohledem na vysoký provozní náklad, související s nutností zajištění vyškolených bezpečnostních specialistů s potřebnou zkušeností a jejich kontinuálního rozvoje.

Jako řešení se nabízí služba sdíleného SOC na úrovni ISP a ICT poskytovatele služeb. Zákazník přitom platí za určité služby SOC, které si vybere z katalogu služeb a to v rozsahu, který je poplatný jeho aktuální potřebě.

Vzhledem k výraznému vývoji bezpečnostních hrozeb a s ní související rostoucí poptávce po službách z oblasti informační bezpečnosti, se T-Mobile rozhodnul vytvořit svůj vlastní specializovaný SOC tým, který se věnuje výhradně dohledu bezpečnostních služeb, a jeho schopnosti nabízet jako součást svých služeb. Nepopiratelnou výhodou tohoto řešení je skutečnost, že se členové SOC týmu věnují svou pozornost jen a pouze problematice informační bezpečnosti, což jim umožňuje získat v této oblasti potřebnou odbornost a zkušenosti a tyto neustále rozvíjet.

Vytvoření dedikovaného SOC týmu poskytuje T-Mobile významnou výhodu proti konkurenci, která má funkci bezpečnostního dohledu ve většině případů koncipovánu jako sdílenou v rámci týmu síťového dohledu.

Základní popis služby SOC:

Hlavní činností SOC týmu je proaktivní dohled nad chráněnými objekty z pohledu nestandardního provozu, samostatné řešení incidentních stavů, komunikace se zákazníky a dalšími složkami systému kybernetické ochrany (např. CERT).

Na základě bezpečnostní události, která se vyskytne v síti konkrétního zákazníka, SOC provádí činnosti v souladu s předem domluveným postupem, případně se proaktivně spojí se zákazníkem a sladí se s ním na dalším postupu řešení. SOC zajišťuje služby v reakčních časech, které jsou definovány v rámci SLA služby.

Základem SOC týmu je skupina operátorů, která zajišťuje službu L1 supportu bezpečnostního dohledu v režimu 24x7x365. Tato skupina je proškolena na problematiku síťového provozu a služeb, administraci síťových a bezpečnostních prvků, velmi dobře rozumí problematice kybernetických útoků, má velmi dobré analytické a kombinační schopnosti a proaktivní zákaznickou orientaci.

V případě, že si L1 support s danou bezpečnostní situací nedokáže poradit sám (za pomocí aktivace předem domluvených scénářů), eskaluje problém na L2 support z týmu technologické bezpečnosti. V případě nutnosti existuje pro L2 support tým smluvní možnost kontaktovat přímo dodavatele dotčených bezpečnostních technologií pro řešení HW problémů nebo L3 podporu výrobce.

SOC tým jako celek disponuje certifikacemi CCNP, CCNA a celou řadou certifikací, týkající se konkrétních bezpečnostních produktů (Arbor Networks, Fortinet, Cisco, CheckPoint, F5, HP ArcSight, IBM Q Radar, FlowMon...).

SOC je v režimu 24x7x365 dostupný na vyhrazeném telefonu či mailu pro případ, že zákazník zaznamená nějakou bezpečnostní událost sám a potřebuje jí ve spolupráci se SOC týmem řešit.

Témata, kterými se SOC tým často zabývá, jsou především problematika bezpečnosti sítí, internetové útoky typu DDoS (pomalé aplikační útoky, volumetrické útoky), útoky na web a SQL, problematika BOT sítí a CCC.

SOC rozesílá zákazníkům upozornění na výskyt botnet stanic a na „podezřelou komunikaci". Každý měsíc řeší desítky DDoS alarmů jak pro zákaznické tak i pro interní cíle T-Mobile.

Služba SOC je v tuto chvíli komerčně poskytována především zákazníkům využívajícím službu „DDoS ochrana", kdy je služba SOC poskytována jako nedílná součást služby DDoS ochrana. SOC tým rovněž pomáhá řešit dohled prvků ochrany perimetru sítí, který T-Mobile nabízí jako volitelnou nadstavbu služby Managed Firewall. SOC tým je rovněž nedílnou součástí služby „Bezpečnostní monitoring", jejíž technologickým základem je SIEM platforma rozšířena o prvky behaviorální analýzy, a která zajišťuje sběr a vyhodnocení bezpečnostních událostí. Úkolem SOC týmu je reagovat na zachycené události dle předem dohodnutého postupu, průběžně sledovat statistiku zachycených událostí a na základě zkušeností navrhovat případnou úpravu korelačních pravidel s cílem minimalizovat false-positive alarmy.

Rozsah služby:
Rozsah služby SOC je vyhodnocován na základě počtu reálně zpracovaných incidentů, nikoliv v závislosti na velikosti společnosti.

Zákazník platí měsíční platbu, která pokrývá určitý počet konzultačních hodin. Nad rámec základu jsou konzultační hodiny zpoplatněny dle ceníkové hodinové sazby.

Parametry služby SOC jsou buď standardně definovány v rámci nadřazené služby (DDoS ochrana, Managed Firewall, Bezpečnostní monitoring), nebo jsou dojednávány individuálně dle potřeb zákazníka (komunikační schéma, použité metody a postupy...)

T-Mobile SOC je schopen nabídnout následující služby:

- Proaktivní monitoring a dohled nad celým životním cyklem událostí a incidentů
- Monitoring incidentů nad logy bezpečnostních technologií
- pravidelný reporting, odborná analýza a doporučení
- zajištění řízení příchozí komunikace k Zadavateli v kontextu ZKB a Vyhlášky
- doporučení a příprava odchozí komunikace od Zadavatele v kontextu ZKB a Vyhlášky (připravuje i dohlíží dodavatel a odesílá Zadavatel na doporučení dodavatele).

---

[i] Uchazeč vyplní přílohu č. 2.1 technické specifikace soutěžených služeb
[ii] Uchazeč vyplní přílohu č. 2.2 technické specifikace soutěžených služeb
[iii] Uchazeč vyplní přílohu č. 2.3 technické specifikace soutěžených služeb
[iv] Uchazeč vyplní přílohu č. 2.4 technické specifikace soutěžených služeb
[v] Uchazeč vyplní přílohu č. 2.5 technické specifikace soutěžených služeb

Příloha č. 2
Smlouvy o poskytování služeb

CENY SLUŽEB

Příloha č. 2

Místo	Kapacita [Mbps]	Maximální kapacita [Mbps]	Paušál platba bez DPH [Kč/měs]	Paušál platba s DPH [Kč/měs]	Cena za přeložení bez DPH [Kč]	Cena za přeložení s DPH [Kč]	Paušální platba za maximální kapacitu bez DPH [Kč]	Paušální platba za maximální kapacitu s DPH [Kč]
Praha 10 - MPLS	184	500	11 000,00	13 310,00	5 000,00	6 050,00	12 750,00	15 427,50
Praha 10 - Internet	200	500	49 000,00	59 290,00	5 000,00	6 050,00	67 750,00	81 977,50
Praha 3 - MPLS	32	50	2 300,00	2 783,00	5 000,00	6 050,00	3 000,00	3 630,00
Praha 3 - Internet	32	50	2 300,00	2 783,00	5 000,00	6 050,00	3 000,00	3 630,00
Brno	16	32	3 900,00	4 719,00	5 000,00	6 050,00	4 500,00	5 445,00
České Budějovice	16	32	3 800,00	4 598,00	5 000,00	6 050,00	4 500,00	5 445,00
Pardubice	16	32	3 800,00	4 598,00	5 000,00	6 050,00	4 500,00	5 445,00
Hradec Králové	16	32	3 800,00	4 598,00	5 000,00	6 050,00	4 500,00	5 445,00
Plzeň	16	32	3 800,00	4 598,00	5 000,00	6 050,00	4 500,00	5 445,00
Ostrava	16	32	3 800,00	4 598,00	5 000,00	6 050,00	4 500,00	5 445,00
Ústí nad Labem	16	32	3 800,00	4 598,00	5 000,00	6 050,00	4 500,00	5 445,00
Jihlava	8	16	2 700,00	3 267,00	5 000,00	6 050,00	3 000,00	3 630,00
Karlovy Vary	8	16	2 700,00	3 267,00	5 000,00	6 050,00	3 000,00	3 630,00
Liberec	8	16	2 700,00	3 267,00	5 000,00	6 050,00	3 000,00	3 630,00
Olomouc	8	16	2 700,00	3 267,00	5 000,00	6 050,00	3 000,00	3 630,00
Zlín	8	16	2 700,00	3 267,00	5 000,00	6 050,00	3 000,00	3 630,00

			Celková cena za paušální platby bez DPH [Kč]	Celková cena za paušální platby s DPH [Kč]	Cena za přeložení bez DPH [Kč]	Cena za přeložení s DPH [Kč]		
Celkem za měsíc			104 800,00	126 808,00			133 000,00	160 930,00
Celkem za 12 měsíců			1 257 600,00	1 521 696,00			1 596 000,00	1 931 160,00
Průměrná cena přeložek					5 000,00	6 050,00		
Cena za 5 přeložek					25 000,00	30 250,00		
							bez DPH [Kč]	**s DPH [Kč]**
Celková cena za období 48 měsíců							5 393 800,00	6 526 498,00

	Hodnoceno
	Dopočítáno automaticky
	Vyplní uchazeč

Příloha č. 3
Smlouvy o poskytování služeb

SPECIFIKACE SUBDODAVATELŮ

Při plnění smlouvy nebudou využiti subdodavatelé.

Příloha č. 4
Smlouvy o poskytování služeb

BEZPEČNOSTNÍ POKYNY PRO OBCHODNÍ PARTNERY V OBLASTI POŽÁRNÍ OCHRANY, BEZPEČNOSTI PRÁCE A OCHRANY MAJETKU

Článek I.
Úvod

Tento dokument:

1) je písemnou informací o rizicích a dokladem o dohodnuté koordinaci mezi stranami při zajišťování bezpečnosti a ochrany zdraví při práci, ve smyslu ustanovení platného znění zákoníku práce, tak, aby ohrožení bezpečnosti a zdraví bylo minimalizováno,

2) se současně stává dokladem o způsobu zabezpečování povinností na úseku požární ochrany ve smyslu § 30, odst. 2, písm. h), vyhlášky č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci),

3) zavazuje obchodního partnera, jeho zaměstnance a osoby jím vyslané k dodržování pravidel stanovených Českým statistickým úřadem k ochraně majetku.

Obchodním partnerem se v tomto dokumentu rozumí firma, která provádí práce nebo služby v budově ČSÚ na základě požadavku ČSÚ.

Zaměstnancem se v tomto dokumentu rozumí obchodní partner, pokud je fyzickou osobou, zaměstnanci obchodního partnera a osoby vyslané obchodním partnerem k provedení práce nebo služeb.

Tento dokument může být operativně doplňován písemnou i ústní formou.

Článek II.
Požární ochrana a Bezpečnost a ochrana zdraví při práci

1. Požární ochrana

1.1. Podle ustanovení § 4 odst. 2 písm. g) zákona č. 133/85 Sb., o požární bezpečnosti, ve znění pozdějších předpisů, se objekt Českého statistického úřadu, Na padesátém 81, 100 82 Praha 10, zařazuje do kategorie činností se zvýšeným požárním nebezpečím. Toto začlenění bylo provedeno na základě § 28 vyhlášky č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci).

1.2. V celé budově ČSÚ je vyhlášen přísný zákaz kouření (vyhrazené místa pro kuřáky je zřetelně označeno) a používání otevřeného plamene nebo jiného zdroje zapálení kromě činností, na které je zpracován technologický postup nebo je vypracován příkaz ke svařování podle vyhlášky č.87/2000 Sb., kterou se stanoví podmínky požární bezpečnosti při svařování a nahřívání živic v tavných nádobách. Pro vykonávání svářečských prací je obchodní partner povinen stanovit organizační a technická opatření k zajištění požární ochrany a odpovídá za zajištění požární bezpečnosti po celou dobu výkonu svářecích prací. Následný požární dohled po skončení svařování může po dohodě zajistit ČSÚ. Tato skutečnost musí být potvrzena v písemném příkazu ke svařování.

1.3. Zaměstnanci jsou povinni si počínat tak, aby nedošlo ke vzniku požáru.

1.4. Zaměstnanci, kteří provádějí práce, které nejsou časově omezeny, musí absolvovat školení o požární ochraně. K tomuto školení obchodní partner určí vedoucího zaměstnance, jehož proškolení provede technik požární ochrany (dále jen „PO") ČSÚ. Vedoucí zaměstnanec pak školí své podřízené zaměstnance podle tematického plánu a časového rozvrhu školení o PO objednatele.

1.5. Vždy nejpozději do dvou dnů po každém opakovaně provedeném školení předloží vedoucí skupiny kopii záznamu o školení požárnímu technikovi PO ČSÚ.

1.6. **Zaměstnanci jsou povinni se seznámit s Požárním řádem, Požárními poplachovými směrnicemi a Evakuačním plánem Českého statistického úřadu.** Požární řád, Požární poplachové směrnice a Evakuační plán jsou vyvěšeny na chodbách v prostoru u výtahů, event. na dalších vybraných volně přístupných místech.

1.7. Ohlašovnou požáru je recepce v 1. nadzemním podlaží.

1.8. Hlásiče požáru jsou zřetelně označeny, v určených prostorách jsou rozmístěny hasicí přístroje.

1.9. **Každý poplach** (nejen požární, ale i poplach vyhlášený při mimořádných událostech) **je vyhlašován vnitřním rozhlasem.** Po jeho vyhlášení se automaticky odblokují turnikety a elektromagnetické zámky. **Při opuštění budovy se zaměstnanci řídí Evakuačním plánem.**

Je zakázáno zejména:

1) používat únikové východy v jiných než mimořádných situacích,

2) blokovat dveře na únikových cestách, zastavět tyto cesty nebo snižovat jejich průchodnost (např. zastavěním těchto cest inventářem, materiálem apod.),

3) znemožnění přístupu k rozvodům vody a el. energie, k požárním hydrantům a přenosným hasicím přístrojům.

2. Bezpečnost a ochrana zdraví při práci

2.1. *Činnost ČSÚ je převážně administrativního charakteru s odpovídajícími pracovními riziky.*

2.2. K minimalizování ohrožení bezpečnosti a zdraví jsou zaměstnanci povinni dodržovat tato pravidla:

- přísný zákaz kouření v celé budově ČSÚ (výjimkou je kuřárna),
- nemanipulovat se žádným zařízením, pokud není určeno k výkonu prací obchodního partnera.

2.3. Pro výkon své činnosti musí mít obchodní partner zpracován svůj seznam pracovních rizik pro výkon prací a je povinen v rámci svého bezpečnostního školení s těmito riziky své zaměstnance seznámit.

2.4. Zaměstnanci musí mít k výkonu dané práce potřebnou odbornou a zdravotní způsobilost a příslušné instrukce k činnostem, které mají provádět.

2.5. K činnosti, kterou mají zaměstnanci vykonávat, musí být vybaveni osobními ochrannými pracovními prostředky odpovídajícími ohrožení, jež vyplývá z prováděných prací, popř. rizika pracoviště, dále vhodnými pracovními pomůckami a prostředky (nářadí).

Článek III.
Ochrana majetku

Ohlašování prací

Práce prováděné obchodními partnery v pracovní i mimopracovní době hlásí ředitel příslušného odboru předem písemně Odboru bezpečnosti a krizového řízení s uvedením názvu obchodního partnera, účelu prací, doby jejich trvání, kontaktních osob obchodního partnera i ČSÚ, jména a příjmení osob vykonávajících práce a čísla jejich občanského průkazu. Zaměstnanci se hlásí v recepci, kde se evidují jako návštěva. O jejich příchodu vyrozumí strážný kontaktní osobu ČSÚ.

Přidělování přístupových karet a klíčů

Přístupové karty a klíče od určených prostor mohou být na základě písemné žádosti ředitele odboru vydány zaměstnancům, kteří se dlouhodobě nachází na jeho pracovišti, pokud to charakter práce vyžaduje (např. úklidové práce apod.). Ztrátu či zcizení přístupové karty nebo klíče, jejich zneužití nebo poškození, které brání funkčnosti, ohlásí zaměstnanci řediteli příslušného odboru, který neprodleně informuje Odbor bezpečnosti a krizového řízení, a to písemně nebo telefonicky

s následným písemným potvrzením. Obchodní partner je povinen uhradit veškeré náklady spojené s pořízením nové karty, klíče nebo změnami klíčového režimu.

Vjezd a parkování

Ve výjimečných případech je možné krátkodobé parkování vozidel zaměstnanců, a to pouze v 1. podzemním podlaží, pokud není z provozních důvodů možné použít technický vjezd. Potřebu takového parkování sdělí písemně ředitel příslušného odboru strážní službě s uvedením firmy a účelu požadovaného parkování.

Zaměstnanec je povinen respektovat zejména tato nařízení:

1) V garážích je nutné dodržovat platné dopravní předpisy.
2) Není povolen vjezd automobilů na pohon LPG.
3) Je zakázáno zdržovat se s vozidlem v prostoru vjezdu do garáží a výjezdu z nich.
4) Vozidlo musí být zaparkováno tak, aby umožnilo volný průchod k výtahům, schodišti a do technického zázemí. Zároveň musí být umožněn volný přístup k požárním hydrantům, přenosným hasicím přístrojům a požárním hlásičům.
5) Průchod osob příjezdovým tunelem nebo příjezdovými vraty je možný pouze v mimořádných případech za dodržení zvýšené opatrnosti a zajištění dozoru strážného.

Dodržování pravidel

Zaměstnanec zejména:

1) Nesmí na pracovišti požívat alkohol nebo jiné návykové látky a nesmí pod jejich vlivem nastoupit do práce.
2) Nesmí poškozovat, zapůjčovat si nebo zcizit majetek ČSÚ.
3) Nesmí používat prostředky a předměty ČSÚ, pokud to není dohodnuto nebo nezbytně nutné pro výkon sjednané práce.
4) Nesmí otevírat uzamčené i neuzamčené části zařízení kanceláře nebo jiných prostor.
5) Je zavázán mlčenlivostí o skutečnostech, které se dozví během své činnosti, a to i po ukončení prací nebo pracovního poměru.
6) Má zakázáno nahlížet do materiálů umístěných nebo uložených v místnosti, ani je nebo jejich části jakýmkoliv způsobem kopírovat, upravovat, pořizovat z nich výpisy, seznamovat s obsahem nebo jeho částí další osoby a rovněž si je nesmí zapůjčovat nebo je zcizit, ani k těmto činnostem napomáhat.
7) Má povinnost chovat se tak, aby nedošlo ke zneužití materiálů, jejich poškození nebo zničení.
8) Nesmí nikomu poskytovat svěřený klíč ani vyrábět jeho kopie.
9) Nesmí klíč nijak označovat ani upravovat.
10) Vždy po ukončení prací uzamkne kancelář nebo jiný prostor, ve kterém prováděl práce.
11) Používá a ukládá klíč tak, aby nedošlo k jeho ohnutí nebo jinému poškození, které by způsobilo jeho nefunkčnost, nebo by vedlo k jeho ztrátě či zcizení.
12) Používá a ukládá přístupovou kartu tak, aby nedošlo k jejímu ohnutí, prasknutí, poškrábání, jinému poškození nebo její ztrátě či zcizení.
13) Nesmí přístupovou kartu polepovat, popisovat, proděravět nebo jinak upravovat.

<u>Je zakázáno zejména:</u>

1) Umožnit vstup do budovy nepovolané osobě.
2) Poskytovat osobní průkazy, vstupní kartu, svěřené klíče nebo jiné pomůcky sloužící k ochraně majetku neoprávněným osobám.
3) Jakkoliv manipulovat s prvky bezpečnostních technologií a poškozovat je.

4) Nechávat otevřená okna během pracovní i mimopracovní doby, pokud by mohlo dojít k ohrožení nebo poškození majetku ČSÚ.

5) Blokovat dveře ovládané čtecím zařízením.

6) Používat výtah jinak, než v souladu s provozními pokyny, dveře výtahu nesmí být v žádném případě blokovány.

7) Vstupovat na střechy /výjimkou je kuřárna/ a slunolamy (pokud to nevyžaduje charakter práce), odkládat nebo vhazovat na ně předměty nebo je jinak znečisťovat.

Článek IV.
Organizační opatření

1) Chce-li obchodní partner provést výměnu vedoucího zaměstnance, musí informovat ČSÚ s předstihem nejméně 14 dnů, aby ČSÚ mohl včas zajistit školení o požární ochraně nového vedoucího zaměstnance dodavatele.

2) Pracovní úrazy zaměstnanců vyšetřuje, ohlašuje a záznamy o úrazu zasílá v souladu s nařízením vlády č. 201/2010 Sb., o způsobu evidence úrazů, hlášení a zasílání záznamu o úrazu, kterým se stanoví vzor záznamu o úrazu a okruh orgánů a institucí, kterým se ohlašuje pracovní úraz a zasílá záznam o úrazu, obchodní partner.

3) Obchodní partner se zavazuje zajistit dodržení výše uvedených bezpečnostních pokynů a potvrzuje, že pracoviště, na kterém se mají práce vykonávat, bylo řádně předáno.