Podmienky služby UPC Anti-DDoS

1. Definícia

Ak nie je uvedené inak, výrazy s veľkými začiatočnými písmenami majú význam definovaný v tomto článku 1.

1.1 „Výstražné upozornenie“ znamená dáta, ktoré by mohli naznačovať potenciálny DDoS útok na základe internetovej prevádzky Účastníka, ktorý sa odchyľuje od profilu Účastníka, pričom taká odchýlka presahuje dopredu stanovenú minimálnu hodnotu.

1.2 Účastník, na ktorého sa vzťahuje obmedzenie, znamená účastníka, ktorého obchodná činnosť spadá do niektorej z kategórií uvedených v článku 12. V definícii „zakázaných činností“.

1.3 „Protokol BGP“ (Border Gateway Protocol) znamená smerovací protokol, ktorý môže požiť Účastník na ohlásenie svojich prefixov alebo UPC na presmerovanie prevádzky na Stránky ochrany pred útokmi DDoS.

1.4 „Dôverné informácie“ znamená materiály, dáta, systémy a ďalšie informácie týkajúc sa prevádzky, obchodnej činnosti, prognóz, tržných cieľov, finančných záležitostí, produktov, služieb, účastníkov a práv k duševnému vlastníctvu druhej zmluvnej strany, ktoré nemusia byť prístupné alebo známe širokej verejnosti. Dôverné informácie zahŕňajúce najmä (avšak nie výlučne) podmienky a ustanovenia Špecifikácie objednanej služby UPC Anti-DDoS (ďalej len „Špecifikácie Anti-DDoS“), ako aj všetky informácie týkajúce sa jednotlivých podmienok prevádzky akýchkoľvek Služieb UPC poskytovaných na základe tejto zmluvy.

1.5 „Účastník“ znamená zákazník UPC BROADBAND SLOVAKIA, s.r.o.

1.6 „Portál účastníka“ znamená webový portál, kde môže Účastník sledovať svoju Internetovú prevádzku, správy, Výstražné upozornenia a informácie o účtoch. Zriadenie Portálu účastníka nie je automatickou súčasťou služby UPC Anti-DDoS. Zriaďuje sa na požiadanie Účastníka a je spoplatnené podľa Cenníka. Ustanovenia v tejto špecifikácii vzťahujúcej sa k Portálu účastníka sa uplatnia iba v prípade, že Účastník požiadal o zriadenie tejto doplnkovej služby.

1.7 „Prípad DDoS“ (distributed denial of service) znamená pokus z externých zdrojov spôsobiť nedostupnosť internetových služieb Účastníka pre jeho zamýšľaných používateľov. Existenciu takých pokusov meria a určuje UPC.

1.8 „Naliehavá údržba“ znamená odstávku mimo termínu pravidelnej plánovanej údržby z dôvodu inštalácie naliehavo vyžadovaných patchov alebo vykonávania opráv či inej urgentne vyžadovanej údržby.

1.9 „Filtrovaný prípad DDoS“ nastáva, keď dôjde k presmerovaniu Internetovej prevádzky Účastníka na Stránku ochrany pred útokmi DDoS prevádzkovanej spoločnosťou UPC a toto presmerovanie trvá až do niektorej z nasledujúcich udalostí, ktorá nastane skôr: (a) okamih navrátenia Účastníka už nie je presmerovaný na Stránku ochrany pred útokmi DDoS prevádzkovanú spoločnosťou UPC) ; alebo (b) uplynutie štyridsiatich ôsmich (48) hodín bez ohľadu na to, koľko Prípadov DDoS u Účastníka nestane v medziobdobí. Ak bude Filtrovaný prípad DDoS trvať aj po uplynutí štyridsiatich ôsmich (48) hodín, bude považovaný za nový Filtrovaný prípad DDoS.

1.10 „Hackerská činnosť“ znamená (a) nelegálny alebo neoprávnený prístup k počítačom, účtom, informáciám alebo komunikačným zariadeniam či zdrojom alebo sieťam tretej strany (vrátane UPC); (b) obídenie či narušenie alebo pokus o obídenie či narušenie bezpečnostných opatrení tretej strany; alebo (c) vykonávanie akejkoľvek činnosti, ktorá by mohla predchádzať pokusu o preniknutie do systému.

1.11 „Obmedzenie infraštruktúry“ znamená, že určitý Prípad DDoS u Účastníka (a) nemožno zmierniť pomocou Služby ochrany pred útokmi DDoS poskytovanej spoločnosťou UPC; alebo (b) môže mať dopad na prevádzkovú stabilitu siete UPC alebo iných účastníkov UPC.

1.12 „Práva k duševnému vlastníctvu“ znamená všetky v súčasnej dobe známe alebo v budúcnosti existujúce práva súvisiace s autorskými právami (najmä, avšak nie výlučne, vrátane práva na používanie, reprodukcie, úpravy, distribúciu, verejné vystavovanie a verejné predvádzanie autorských diel), práva k databázam, ochranné známky (najmä, avšak nie výlučne, charakteristické vizuálne prvky, obchodné názvy, značky, firemné označenia a logá), vynálezy, patenty (najmä, avšak nie výlučne, práva na výrobu, používanie, ponúkanie na predaj a predaj), žiadosti o patenty, softvér, firmware, know-how, obchodné tajomstvo, morálne práva a všetky ďalšie práva alebo formy ochrany chránených práv akejkoľvek povahy alebo obdobného charakteru alebo s podobným účinkom na čokoľvek z vyššie uvedeného, ktoré môžu existovať kdekoľvek na svete a môžu byť označené akokoľvek, bez ohľadu na to, či sú ktorékoľvek z nich registrované, a vrátane prípadných žiadostí o registráciu čohokoľvek z vyššie uvedeného.

1.13 „Internetová prevádzka“ znamená najmä, avšak nie výlučne, všetky internetové prenosy, VPN, elektronickú poštu, prenosy súborov a ďalšie dáta prechádzajúce niektorou verejnou sieťou s prepojovaním paketov.

1.14 „Právne predpisy“ znamená všetku miestnu a európsku legislatívu, zákony, vyhlásenia, smernice, právne úpravy, nariadenia, predpisy, zásady alebo iné záväzné obmedzenia.

1.15 „Routery na zmierňovanie dopadov útokov“ znamená určitý počet routerov, pomocou ktorých UPC presmerováva Internetovú prevádzku Účastníka, ako je popísané v článku 2.3.

1.16 „Normálne podmienky“ znamená situácie, kedy u Účastníka neprebieha žiadny Prípad DDoS.

1.17 „Pravidelná plánovaná údržba“ znamená akúkoľvek údržbu vykonávanú v rámci vyčleneného okna na údržbu, pričom takáto údržba musí rešpektovať požiadavku na 99,99 % dostupnosť služby.

1.18 „Dátum komerčnej aktivácie Služby“ znamená dátum, kedy UPC zašle Účastníkovi e-mail v súlade s článkom špecifikujúcim kontaktné údaje v dokumente o sprevádzkovaní služieb pre Účastníka oznamujúci sprevádzkovanie IP objektov v súlade s pokynmi UPC. Dátumom technickej aktivácie služby sa rozumie dátum, kedy bude Účastník pridaný do príslušného nástroja na detekciu/zmierňovanie následkov útokov DDoS.

1.19 „Dane“ znamená dane, clá, poplatky a ďalšie štátom uložené čiastky akejkoľvek povahy (vrátane daní z obchodnej činnosti, predaja, služieb, používania a pridanej hodnoty a všetky príslušné sankcie, úroky

a ďalšie príplatky, avšak s výnimkou daní z čistého príjmu UPC), ktoré sú uložené akoukoľvek vládou alebo akoukoľvek jej politickou súčasťou alebo z ich poverenia z poplatkov účtovaných za akékoľvek zo Služieb ochrany pred útokmi DDoS poskytovaných spoločnosťou UPC alebo súvisiace dokumentácie predané Účastníkovi na základe tejto zmluvy.

1.20 „Stránky ochrny UPC proti útokom DDoS" znamená stránky určené na zmierňovanie škôd, kde UPC zmierňuje škody vzniknuté v dôsledku Udalostí filtrovaných útokov DDoS.

1.21 „Systém Arbor" je komplexné riešenie zaisťujúce detekciu a filtrovanie škodlivej prevádzky.

2. Popis služieb

V súlade s podmienkami a ustanoveniami tejto Zmluvy o ochrane bude UPC poskytovať Účastníkovi nasledujúce služby prostredníctvom zdieľanej platformy označovanej ako Služba ochrany pred útokmi DDoS poskytovaná spoločnosťou UPC (ďalej len ako „UPC Anti-DDoS"):

2.1 Nastavenie Účastníka. UPC začne proces nastavovania Účastníka po odsúhlasení Špecifikácie Anti-DDoS a tejto Prílohy. Účastník súhlasí a berie na vedomie, že UPC môže podľa vlastného uváženia z akéhokoľvek dôvodu odmietnuť alebo zamietnuť vykonanie akéhokoľvek zriadenia služieb predložené UPC, pričom v takom prípade UPC nebude povinná Účastníkovi poskytovať UPC Anti-DDoS.

(a) Portál Účastníka. Na základe žiadosti zriadi UPC Účastníkovi účet na Portáli služby Anti-DDoS a poskytne Účastníkovi používateľské meno a heslo na prístup k Portálu. UPC poskytne Účastníkovi jedno (1) základné školenie na Portáli Účastníka.

(b) Informácie nutné na sprevádzkovanie služieb. UPC môže podľa vlastného uváženia požadovať od Účastníka poskytnutie informácií na sprevádzkovanie služieb v podobe určenej spoločnosťou UPC. Po odovzdaní požadovaných informácií na sprevádzkovanie služieb UPC vykoná kontrolu týchto informácií. Poskytnuté dáta sú využité na nastavenie profilu pre príslušnú šablónu Účastníka.

2.2 Účastník týmto berie na vedomie a súhlasí, že sám zodpovedá za všetky monitorovania svojej internej siete a svojho vybavenia a že UPC nebude Účastníkovi poskytovať žiadne monitorovacie služby vo vzťahu k jeho internej sieti a k jeho vybaveniu. Účastník ďalej berie na vedomie a súhlasí, že je povinný informovať UPC, ak u neho nastane nejaký Prípad DDoS alebo ak sa bude Účastník domnievať, že u neho nastal Prípad DDoS.

2.3 Zmierňovanie škôd

Počas útoku sa k Účastníkovi (t. j. k jeho serveru, IP adresám atď.) snaží dostať škodlivá prevádzka a súčasne aj normálna/legálna prevádzka. Prevádzka sa meria podľa sieťových uzlov a odosiela sa do centrálnej zbernice. Prítomnosť škodlivej prevádzky sa zisťuje na základe stanovených minimálnych/maximálnych hodnôt a vzorcov. Automatické zmierňovanie škôd sa spúšťa dosiahnutím určitej konfigurovateľnej maximálnej hodnoty v určitom časovom intervale spôsobenej útokom. Po skončení útoku sa tento systém opäť vypne. Routery v sieti sú naprogramované tak, aby presmerovávali prevádzku spojenú s útokom DDoS cielenú na účastníka na čistiaci server TMS. Škodlivá prevádzka sa odfiltrováva a bežná prevádzka sa odosiela späť k účastníkovi.

Služba ochrany proti útokom DDoS ponúkaná spoločnosťou UPC chráni najmä pred volumetrickými útokmi, ktoré sú predovšetkým dôsledkom útokov využívajúcich amplifikáciu.

UPC ponúka ochranu pred zdrojmi zo svojej siete (onnet) aj pred zdrojmi mimo siete LGI (offnet).

Na žiadosť UPC bude UPC pracovať na zmernení následkov Prípadu DDoS tak, že poskytne odporúčanie ďalšieho postupu. Ak bude odporúčaným ďalším postupom presmerovanie internetovej prevádzky Účastníka, bude sa postupovať nasledovne:

Nastavenie v systéme Arbor definuje, čo je považované za normu (štandardnú prevádzku) a kedy má byť vydané upozornenie na útok DDoS. Hneď ako systém Arbor zistí útok DDoS, kontrola nainštaluje trasu na čistenie a všetka prevádzka z útoku DDoS bude presmerovaná na základe adresy destinácie do systémov TMS.

Systémy TMS vyradia všetku prevádzku, ktorá bude podľa nastavenia vyhodnotená ako škodlivá.

Odhalenie útoku

Vybavenie používané spoločnosťou UPC, Arbor Networks SP, vykonáva analýzu vzorky získanej z routerov.

Útok môže spustiť štandardné výstražné upozornenie DoS Host alebo upozornenie na útok v podobe rýchlej záplavy Fast Flood DoS Host. Štandardné výstražné upozornenie DoS Host sa spustí, keď prevádzka na monitorovanom routeri smerujúcom k jedinému hostiteľovi presiahne konfigurovanú medznú hodnotu povoleného typu zneužitia za určitý stanovený čas. Výstražné upozornenie na útok v podobe rýchlej záplavy Fast Flood DoS Host sa spustí pri zistení veľkého objemu prevádzky smerujúcej k jedinému hostiteľovi na určitý povolený typ zneužitia.

Zmierňovanie škôd sposobených útokom

Zariadenia TMS umožňujú spoločnosti UPC zmierniť dopady útokov pomocou protiopatrení, správ a výstražných upozornení. Zariadenia TMS tiež umožňujú UPC monitorovať najdôležitejšie aplikácie a sieťové služby za účelom zaistenia dostupnosti služieb a poskytnutia včasného upozornenia v prípade útokov na sieť.

Keď systém Arbor Networks SP odhalí nejakú neobvyklú udalosť, presmeruje prevádzku prostredníctvom zariadenia TMS tak, aby bolo možné vykonať overenie a v prípade potreby zareagovať na útok. Zariadenia TMS a systém Arbor Networks SP si medzi sebou odovzdávajú základné dáta a dáta o prevádzke, aby bolo zaistené presné blokovanie škodlivej prevádzky.

Systém automatického zmierňovania škôd umožňuje systému Arbor Networks SP automatické spustenie procesu zmierňovania dopadov pomocou TMS, hneď ako dôjde k útoku na určitý objekt spravovaný účastníkom.

Útoky DDoS sa odhaľujú na základe získaných dát o prevádzke v sieti z vopred definovaných okrajových routerov spoločnosti UPC (PEs).

UPC bude aplikovať vrstvené filtre na Internetovú prevádzku presmerovanú do systému UPC Anti-DDoS, kde bude progresívnym spôsobom blokovaná prevádzka, cieľom ktorej je narušiť alebo vyradiť

z prevádzky internetové služby Účastníka. Účastník týmto berie na vedomie a súhlasí, že UPC bude filtrovať len také objemy Internetovej prevádzky Účastníka, ktoré sú nevyhnutné na zaistenie dostupnosti internetových služieb Účastníka pre jeho koncových používateľov.

Návrat k bežnému fungovaniu:

Hneď ako systém vyhodnotí, že Prípad DDoS skončil, vráti Účastníka do normálnej prevádzky.

Účastník sa môže rozhodnúť pre ukončenie presmerovania svojej Internetovej prevádzky do systému UPC Anti-DDoS, a to kedykoľvek v priebehu trvania Filtrovaného prípade DDoS v súlade s Plánom eskalácie. V takých prípadoch nevzniká UPC akákoľvek zodpovednosť voči Účastníkovi a Účastník nesie plnú zodpovednosť za zmierňovanie dopadov Filtrovaného prípadu DDoS od okamihu ukončenia procesu filtrácie na žiadosť Účastníka, kedy Internetová prevádzka Účastníka už nie je naďalej filtrovaná; súčasne však Účastník nesie všetky náklady vzniknuté v dobe, kedy bola Internetová prevádzka Účastníka presmerovaná do systému UPC Anti-DDoS a/alebo kedy bol Filtrovaný prípad DDoS spravovaný spoločnosťou UPC.

2.4 Podmienky služby

Na pripojenie k službe UPC Anti-DDoS musí Účastník spĺňať nasledujúce podmienky:

- Využívať dlužby UPC Internet alebo IP konektivita – služba UPC Anti-DDoS nemôže byť ponúkaná ako samostatná služba.
- Byť pripojený do siete UPC pomocou optických vlákien s minimálnou prenosovou rýchlosťou 100 Mbit/s.
- Služba ochrany pred útokmi DDoS bude k dispozícii pre účastníkov využívajúcich služby internetu pre firmy s pripojením pomocou optických vlákien.

Ďalšie pravidlá a popis služby UPC Anti-DDoS:

- Akýkoľvek prístup cez koaxiálny kábel je mimo rámca dohodnutého rozsahu.
- Služba je ponúkaná len v podobe automatického zmierňovania dopadov útokov. Automatické zmierňovanie dopadov útokov vyžaduje monitorovanie internetovej prevádzky smerujúcej k účastníkovi a odoberanie vzoriek z tejto prevádzky. Automatické nápravné opatrenia budú prijímané bez ľudského zásahu.
- Dosiahnutím maximálnej kapacity UPC začne prevádzku namiesto čistenia vyraďovať.
- Služba ochrany proti útokom DDoS môže byť aplikovaná len na internetové služby poskytované spoločnosťou Liberty Global, nie na pripojenie poskytované tretími stranami, ktoré môže účastník využívať od ďalších poskytovateľov.

2.5 Parametre dostupnosti služby

Relevantným aspektom Služby UPC Anti-DDoS je reakčná doba zmierňovania dopadov útokov DDoS, t. j. čas, ktorý uplynie od okamihu začatia procesu zmierňovania dopadov.

Parameter	Hodnota
Reakčná doba v prípade útoku	UPC povolila funkciu detekcie útoku v podobe rýchlej záplavy, ktorá odhalí útok počas menej než 60 sekúnd a začne automatický proces zmierňovania dopadov, hneď ako sa spustí výstražné upozornenie na útok.
Garantovaná ročná dostupnosť služieb (Platforma Arbor)	99,99 %
Dopad na latenciu, jitter a stratu paketov v internetovej službe počas čistenia prevádzky?	Účastník vidí viac skokov, ale nedochádza k strate paketov. Dopad na reakčnú dobu v prípade zmierňovania dopadov útoku: < 50 ms.
Maximálna doba čistenia prevádzky po skončení útoku DDoS	5 minút
Minimálna prenosová rýchlosť pre čistenie	100 Mbit/s

2.6 Zákaznícka podpora. Tím B2B podpory spoločnosti UPC poskytuje (a) telefonickú a e-mailovú podporu Účastníkovi; (b) odpovede na otázky týkajúce sa fakturácie za službu UPC Anti-DDoS; (c) primerané úsilie na bezodkladné informovanie Účastníka (forma e-mailu sa považuje za dostatočnú o prípadnej Naliehavej údržbe. UPC poskytne Účastníkovi otázky/odporúčania na odstránenie problémov týkajúcich sa Služby Anti-DDoS poskytované spoločnosťou UPC.

2.7 Úprava alebo prerušenie Služieb. Účastník týmto berie na vedomie a súhlasí, že UPC môže podľa vlastného uváženia kedykoľvek, avšak len na základe konzistentnej zmeny vykonanej spoločnosťou UPC, upraviť alebo prerušiť službu UPC Anti-DDoS ako celok alebo akúkoľvek jej časť alebo inak upraviť akékoľvek podmienky vzťahujúce sa na službu UPC Anti-DDoS poskytovanú spoločnosťou UPC na základe písomného oznámenia (postačuje e-mailom) zaslaného Účastníkovi tridsať (30) dní vopred alebo s okamžitou účinnosťou na základe písomného oznámenia (postačuje e-mail) zaslaného Účastníkovi, ak je to nutné na dodržanie platných Právnych predpisov (každý z bodov vyššie je ďalej označovaný ako „Dátum účinnosti úpravy Služby“).

3. Overenie správneho fungovania vyčistenej prevádzky

3.1 Ako súčasť nastavenia Účastníka UPC nadefinuje profil statickej prevádzky na základe informácií poskytnutých Účastníkom v prihlasovacom formulári a z toho potom nadefinuje zoznam statických medzných hodnôt, kde budú stanovené hodnoty, pri prekročení ktorých sa automaticky spustia výstražné upozornenia a (v závislosti od závažnosti) opatrenia smerujúce k zmierňovaniu dopadov. Pri poklese pod nastavené hodnoty sa prevádzka vráti do normálneho stavu a proces zmierňovania dopadov a presmerovania prevádzky sa ukončí.

3.2 Ak niektorý Filtrovaný prípad DDoS prekročí Hranicu čistej prevádzky, prevádzka Účastníka bude presmerovaná na stránku (stránky) ochrany pred útokmi DDoS prevádzkovanú spoločnosťou UPC.

Ak nie je v Zmluve o ochrane dohodnuté inak, UPC môže tieto dáta používať iba na poskytovanie služby UPC Anti-DDoS.

4. Podmienky a obmedzenia

4.1 Ak UPC na základe vlastného uváženia s prihliadnutím k obvyklým komerčným štandardom dospeje k záveru, že došlo alebo dochádza k Obmedzeniu infraštruktúry, UPC sa môže bezodkladne rozhodnúť, že (a) nebude naďalej prijímať žiadnu Internetovú prevádzku Účastníka alebo jeho časť; alebo (b) vyradí (zablokuje) všetku Internetovú prevádzku Účastníka alebo jeho časť zo služby UPC Anti-DDoS. Ak UPC využije svoje práva vyplývajúce z Obmedzenia infraštruktúry, UPC môže pozastaviť plnenie svojich záväzkov vyplývajúcich z tejto Prílohy a po dobu takého pozastavenia plnenia nebude služba UPC Anti-DDoS (respektíve akákoľvek jej časť) Účastníkovi k dispozícii. Hneď ako UPC na základe vlastného uváženia dospeje k záveru, že Obmedzenie infraštruktúry pominulo, UPC obnoví plnenie svojich záväzkov vyplývajúcich z tejto Prílohy a služba UPC Anti-DDoS bude Účastníkovi opäť sprístupnená.

4.2 Účastník týmto berie na vedomie a súhlasí, že UPC (a) bude používať Výstražné upozornenia a Informácie na spustenie služieb na účely poskytovania služby UPC Anti-DDoS; (b) môže zverejňovať dáta v agregovanej podobe, pričom však také zverejnenie musí byť vždy úplne anonymné; (c) môže byť povinná poskytovať informácie alebo dáta súvisiace s Prípadmi DDoS vynucovacím orgánom a/alebo národným útvarom pre počítačovú bezpečnosť („CERT“), pričom UPC neponesie zodpovednosť za žiadne také požadované poskytnutie informácií či dát. Ak sa také informácie či dáta o Prípade DDoS týkajú Účastníka, UPC (i) v rozsahu povolenom právnymi predpismi bude Účastníka o takom požadovanom poskytnutí informovať; a (ii) bude s Účastníkom v primeranom rozsahu spolupracovať na získaní ochranného príkazu alebo iného právneho prostriedku ochrany zabraňujúceho takému poskytnutiu informácií či dát.

4.3 Účastník berie na vedomie a udeľuje povolenie spoločnostiam UPC a UPC BV alebo ďalším tretím stranám na vzájomné zdieľanie všetkých relevantných informácií, vrátane (avšak nie výlučne) Dôverných informácií Účastníka, v súvislosti s poskytnutím Služieb podľa tejto Prílohy.

4.4 Účastník týmto berie na vedomie a súhlasí s tým, že služba UPC Anti-DDoS podlieha určitým technickým obmedzeniam a je určená na obranu proti známym formám Prípadov DDoS. Účastník má možnosť o týchto obmedzeniach informovať. V dôsledku toho nemusia služby UPC Anti-DDoS vždy odhaliť všetky Prípady DDoS a zmierniť ich dopady, a napriek tomu, že UPC vynakladá a aj naďalej bude vynakladať všetko z komerčného hľadiska primerané úsilie na to, aby službu Anto-DDoS prevádzkovala tak, aby dokázala odhaliť známe aj neznáme Prípady DDoS a zmierňovať ich dopady, UPC nemôže garantovať, že budú odhalené a zmiernené všetky Prípady DDoS.

5. Platby poplatkov a daní

5.1 Pozastavenie Služieb z dôvodu neuhradenia dlžných čiastok

Účastník týmto berie na vedomie a súhlasí, že (i) Účastník bude hradiť spoločnosti UPC príslušné poplatky za Službu; (ii) UPC môže pozastaviť plnenie a/alebo prístup k službe UPC Anti-DDoS alebo prerušiť poskytovanie služby Anti-DDoS v prípade neuhradenia alebo opakovaného omeškania s úhradou akýchkoľvek platieb, a to na základe písomného oznámenia svojho zámeru tak učiniť (ktoré môže byť zaslané e-mailom) ; (iii) UPC môže vypovedať túto Špecifikáciu Anti-DDoS v prípade neuhradenia alebo opakovaného omeškania s úhradou akýchkoľvek platieb.

5.2 Poplatky. Účastník týmto berie na vedomie a súhlasí, že poplatky za službu UPC Anti-DDoS poskytovanú spoločnosťou UPV sa skladajú z platby za inštaláciu a z pravidelných fixných mesačných poplatkov a že poplatky za prípadné obdobia predĺženia alebo za nové objednávky budú stanovené vo výške aktuálne platných sadzieb v dobe takého predĺženia alebo novej objednávky.

6. Povinnosti Účastníka

Ako podmienku poskytovania Služby UPC Anti-DDoS zo strany UPC Účastník berie na vedomie a súhlasí, že nesie výlučnú zodpovednosť za plnenie nasledujúcich záväzkov:

6.1 Medzné hodnoty Ak nebude Účastník spokojný s východiskovým profilom nastaveným pre neho spoločnosťou UPC, Účastník navrhne minimálne medzné hodnoty Internetovej prevádzky Účastníka, pri prekročení ktorých bude zaslané výstražné upozornenie.

6.2 Účastník je povinný (a) na vyžiadanie vykonať zmeny alebo vydať svojim poskytovateľom hostingových služieb a/alebo poskytovateľom služieb pokyn na vykonanie zmien súčasného sieťového vybavenia a/alebo infraštruktúry tak, aby UPC mohla poskytovať Službu Anti-DDoS; (b) zaobstarať všetky potrebné oprávnenia a povolenia na vykonanie takých zmien (najmä vrátane úhrady všetkých poplatkov účtovaných akýmikoľvek Prostrediami tretích strán za zasielanie Výstražných upozornení spoločnosti UPC; (c) poskytnúť spoločnosti UPC kontaktné body, ktoré UPC pomôžu s Nastavením Účastníka a so zavedením Služby Anti-DDoS a poskytovaním priebežnej podpory; (d) učiniť všetky primerané kroky na zaistenie ochrany pred neoprávneným prístupom, používaním a oznamovaním jeho používateľského mena a hesla poskytnutého mu spoločnosťou UPC za účelom prístupu Účastníka k jeho Portálu Účastníka.

6.3 Účastník vyhlasuje a zaručuje, že (a) získal všetky potrebné súhlasy a povolenia na to, aby mohla UPC oznamovať informácie a údaje Účastníka a/alebo tretích strán (vrátane osobných údajov); (b) bude Službu UPC Anti-DDoS používať na svoje vlastné interné účely a nebude ju predávať ďalším osobám; (c) nezaoberá sa a ani sa nebude zaoberať žiadnou nelegálnou činnosťou a bude dodržiavať všetky platné zásady, predpisy a zákony; a (d) všetky informácie na spustenie služieb poskytnuté Účastníkom (buď prostredníctvom Portálu Účastníka alebo prostredníctvom formulára dodaného spoločnosťou UPC) sú presné, spoľahlivé a úplné a Účastník ich bude podľa potreby vždy včas aktualizovať.

7. Práva na prístup k Portálu

Na Dobu trvania zmluvy udeľuje UPC súhlas Účastníkovi a ten týmto preberá obmedzenú, nevýhradnú, neprevoditeľnú a nepostupiteľnú licenciu na používanie Portálu Účastníka a na prístup k nemu, a to výhradne na účely využívania Služby UPC Anti-DDoS a na prístup k nim a na účely prezerania správy účtu Účastníka a dát na tomto účte obsiahnutých, a to výhradne v súlade so všetkými príslušnými pokynmi alebo dokumentáciou, ktoré môže UPC v tejto súvislosti Účastníkovi poskytnúť.

8. Obmedzenia

Účastník nesmie (a) vykonávať úpravy, demontáž, dekompiláciu, vytvárať odvodené diela alebo sa inak pokúšať odhaliť alebo získať zdrojový kód k akémukoľvek softvéru alebo systému poskytujúcemu Službu ochrany proti útokom DDoS spoločnosti UPC; (b) komunikovať akýkoľvek softvér poskytnutý spoločnosťou UPC v súvislosti so Službou ochrany proti útokom DDoS s akýmkoľvek programom alebo softvérom licencovaným na základe Všeobecnej verejnej licencie alebo akejkoľvek

inej licencie z otvoreného zdroja spôsobom, ktorý by mohol viesť k tomu alebo by mohol byť vykladaný ako vedúci k tomu, že sa na taký softvér (alebo akúkoľvek jeho modifikáciu) začnú vzťahovať podmienky príslušnej Všeobecnej verejnej licencie alebo inej licencie z otvoreného zdroja; alebo (c) využívať služby UPC spôsobom predstavujúcim nadmerné používanie alebo zneužívanie alebo spôsobom, ktorý inak nespĺňa podmienky dohodnuté v tejto Zmluve alebo je s nimi v rozpore. Účastník týmto berie na vedomie a súhlasí, že si UPC ponechá všetky Práva k duševnému vlastníctvu, nároky a práva ku všetkým ďalším informáciám, dátam, obsahu, softvéru, námetom, konceptom, technikám, procesom, konfiguráciám alebo inému duševnému vlastníctvu obsiahnutému v Službách ochrany proti útokom DDoS poskytovanýchspoločnosťou UPC alebo praktikovaných v súvislosti s týmito službami (vrátane Portálu Účastníka). Všetky také práca UPC k duševnému vlastníctvu sa považujú za Dôverné informácie.

9. Doba trvania, ukončenie zmluvy

9.1. Zmluva na poskytovanie služby UPC Anti-DDoS sa uzatvára na dobu neurčitú, pričom ju možno na základe výpovede Účastníka ukončiť najskôr 6 mesiacov od dátumu odovzdania. Službu Anti-DDoS možno potom vypovedať aj bez udania dôvodu, výpovedná doby služby činí 3 mesiace a začína bežať prvý deň nasledujúceho mesiaca po jej doručení. V prípade ukončenia poskytovania dátovej služby je zároveň automaticky ukončená služba Anti-DDoS. Služba Anti-DDoS je tiež ukončená zároveň s ukončením služby internetového pripojenia, pretože bez tejto nie je možné službu Anti-DDoS poskytovať. Účastník týmto berie na vedomie, že UPC môže kedykoľvek a z akéhokoľvek dôvodu alebo bez uvedenia dôvodu Špecifikáciu Anti-DDoS vypovedať bez ohľadu na akékoľvek ustanovenia Špecifikácie Anti-DDoS, v opačnom zmysle je UPC oprávnená túto Špecifikáciu Anti-DDoS vypovedať písomnou výpoveďou s výpovednou dobou s dĺžkou 30 dní.

9.2. Výpoveď zmluvy z dôvodu podstatného prerušenia povinností. Ktorákoľvek zo zmluvných strán môže túto Zmluvu o ochrane vypovedať písomnou výpoveďou druhej zmluvnej strane v prípade podstatného porušenia zmluvných povinností touto druhou stranou a nenapravenia takého porušenia v lehote (30) dní od doručenia písomnej výzvy na nápravu obsahujúcej špecifikáciu predmetného porušenia.

9.3 Insolvencia. V rozsahu povolenom platnými Právnymi predpismi môže ktorákoľvek zo zmluvných strán túto Zmluvu o ochrane vypovedať s okamžitou účinnosťou v prípade (a) začatia akéhokoľvek konania voči zmluvnej strane alebo z jej popudu požadujúceho úľavu, reorganizáciu alebo vysporiadanie v súlade s akýmikoľvek zákonmi či predpismi upravujúcimi insolvenciu, pričom také konanie nebude do tridsiatich (30) dní zamietnuté; (b) postúpenie majetku v prospech veriteľov alebo menovanie núteného správcu, likvidátora alebo konkurzného správcu vo vzťahu k majetku či aktívam druhej zmluvnej strany; alebo (c) likvidácii, zrušení alebo zániku obchodnej činnosti druhej zmluvnej strany.

9.4 Účinky ukončenia zmluvy

9.4.1 Výpoveď zo strany UPC. V prípade výpovede Špecifikácie Anti-DDoS podľa článku 9.2 alebo 9.3 vyššie sa môže UPC podľa vlastného uváženia rozhodnúť s okamžitou účinnosťou Službu ukončiť. Ak UPC ukončí Službu podľa tohto článku 9.4.1, všetky licencie udelené Účastníkovi na základe príslušnej Špecifikácie Anti-DDoS okamžite zanikajú.

9.4.2 Všeobecné ustanovenie. Po uplynutí doby trvania Špecifikácie Anti-DDoS alebo po jej ukončení je Účastník povinný prestať používať Službu UPC Anti-DDoS. Žiadne uplynutie doby trvania alebo ukončenia zmluvy však Účastníka nezbavuje akejkoľvek povinnosti uhradiť finančné záväzky vzniknuté alebo splatné k dátumu ukončenia alebo uplynutia doby trvania zmluvy.

9.4.3 Prechod Účastníka. Akékoľvek ukočenie či výpoveď (z akéhokoľvek dôvodu), uplynutie doby trvania alebo neobnovenie služieb (okrem prípadov uplynutia doby trvania alebo neobnovenia Služby UPC Anti-DDoS) nezbavuje Účastníka jeho povinnosti naďalej hradiť spoločnosti UPC všetky platby za Službu UPC Anti-DDoS, s výnimkou nasledujúcich prípadov a výlučne v rozsahu takých prípadoch: (i) ak Účastník uzavrie s UPC zmluvu týkajúcu sa Služieb UPC Anti-DDoS; a (ii) ak UPC písomne súhlasí s odpustením zostávajúcich platobných záväzkov vo vzťahu k Službe UPC Anti-DDoS.

Bez ohľadu na čokoľvek o obsahu tejto Zmluvy o ochrane v opačnom zmysle a okrem ďalších práv UPC vyplývajúcich zo Zmluvy je UPC oprávnená túto Zmluvu vypovedať s okamžitou účinnosťou písomnou výpoveďou doručenou Účastníkovi v prípade, že UPC na základe vlastného uváženia dospeje k záveru, že sa Účastník dopustil porušenia zásad zákazu zneužívania (článok 12).

10. Neexistencia práva na odškodnenie voči UPC

Účastník týmto berie na vedomie a súhlasí, že nie je oprávnený a nebude požadovať akékoľvek odškodnenie od UPC vo vzťahu k Službe UPC Anti-DDoS.

11. Vyhlásenie a záruky, obmedzenie zodpovednosti

11.1 Vyhlásenie a záruky Účastníka. Účastník týmto (i) vyhlasuje a zaručuje, že nie je ani nebude Účastníkom, na ktorého sa vzťahuje obmedzenie; a (ii) zaručuje, že bude vždy dodržiavať podmienky a ustanovenia tejto Prílohy a riadiť sa nimi.

11.2 Neexistencia záruk. Bez ohľadu na čokoľvek z obsahu tohto popisu v opačnom zmysle platí, že služba UPC Anti-DDoS poskytovaná spoločnosťou UPC je poskytovaná „vo svojej súčasnej podobe“ a „podľa aktuálnej dostupnosti“, bez akýchkoľvek záruk. UPC týmto vylučuje všetky výslovné, implicitné či zo zákona vyplývajúce záruky, najmä (avšak nie výlučne) všetky implicitné záruky predajnosti, vhodnosti na určitý účel, splnenie požiadaviek účastníka, neporušenie akýchkoľvek práv a všetky záruky vyplývajúce z plnenia, predaja a/alebo obchodného použitia. UPC nevyhlasuje, nezaručuje ani negarantuje, že služba ochrany proti útokom DDoS poskytovaná podľa tejto zmluvy bude fungovať bez prerušenia, porúch a chýb. Účastník si je vedomý a súhlasí s tým, že UPC nezodpovedá za akékoľvek konanie či nekonanie účastníka založené na akýchkoľvek informáciách poskytnutých v rámci služieb ochrany pred útokmi DDoS poskytovaných spoločnosťou UPC. UPC nevyhlasuje, nezaručuje ani negarantuje, že (a) dôjde k odhaleniu bezpečnostných hrozieb, škodlivých programov a/alebo zraniteľných miest; (b) služba UPC Anti-DDoS poskytovaná spoločnosťou UPC zaistí bezpečnosť sietí a systémov účastníka pred škodlivými programami, vniknutím alebo inými formami porušenia zabezpečenia; (c) bude odhalené každé zraniteľné miesto na každom testovanom systéme či aplikácii; alebo (d) sa nevyskytnú žiadne falošné potvrdenia útokov.

11.3 Bez ohľadu na čokoľvek v opačnom zmysle platí, že v súvislosti so službou ochrany pred útokmi DDoS poskytovanou spoločnosťou UPC, nenesie UPC akúkoľvek zodpovednosť vo vzťahu k zásadám prijateľného používania (najmä, avšak nie výlučne, vo vzťahu k akémukoľvek konaniu či nekonaniu spolooločnosti UPC).

12. Zásady prijateľného používania

12.1 Zakázané činnosti. Účastník nesmie vykonávať ani sa pokúšať vykonávať žiadne z nasledujúcich zakázaných činností: (a) hackerská činnosť, testovanie dostupnosti (pingping), zahlcovanie, rozosielanie hromadnej pošty alebo útoky v podobe DoS (odopretie služby) alebo akékoľvek iné činnosti, ktoré narušujú používanie alebo možnosť ostatných efektívne používať akúkoľvek sieť, službu alebo vybavenie; (b) podieľanie sa alebo šírenie návodných informácií ohľadom podvodnej alebo nelegálnej činnosti (vrátane online hazardu vo všetkých podobách, bez ohľadu na to, či je alebo nie je v rozpore s platnými právnymi predpismi), porušovanie alebo odcudzovanie Práv k duševnému vlastníctvu tretích strán (vrátane softvérového pirátstva), narušovanie práv na súkromie, publicitu a ďalších osobnostných práv ďalších osôb, zhromažďovanie, inzerovanie, odovzdávanie, uchovávanie, zverejňovanie, zobrazovanie, nahrávanie alebo iné sprístupňovanie detskej pornografie alebo iných obscénnych verbálnych prejavov alebo materiálov alebo používanie siete UPC alebo jej predajcov (podľa konkrétnej situácie) na takéto činnosti; (c) podieľanie sa na akejkoľvek zákonnej či nezákonnej činnosti, o ktorej sa UPC domnieva, že by mohla poškodiť jej prevádzku, povesť, dobré meno alebo vzťahy s účastníkmi; (d) rozosielanie nevyžiadanej hromadnej pošty a/alebo komerčných elektronických oznámení, vírusov, červov alebo trójskych koní; (e) falšovanie, vymazávanie alebo skresľovanie nadpisov správ, spiatočných adries alebo adries internetových protokolov alebo iná manipulácia aj identifikačnými znakmi ako celkom alebo sčasti, za účelom skrytia pôvodcu príslušnej správy; (f) podpora alebo podnecovanie na fyzickú ujmu alebo násilie na určitej skupine osôb ale jednotlivcov; (g) reklama, prenos, poskytovanie alebo iné sprístupňovanie akéhokoľvek softvéru, programov, produktov, služieb, možností alebo informácií určených na uľahčenie porušovania týchto Zásad prijateľného používania. Účastník je povinný učiniť všetky primerané kroky na zaistenie toho, aby žiadna tretia strana, ktorej Účastník povolí využívať svoje služby, neprevádzkovala ani sa nepokúšala prevádzkovať žiadnu zo zákazaných činností špecifikovaných nižšie.

12.2 Potvrdenie zo strany Účastníka. Účastník týmto berie na vedomie a súhlasí, že (a) informácie, ktoré sa dostanú do zariadenia UPC alebo jej predajcov, môžu mať pôvod u niektorého z účastníkov Účastníka alebo inej tretej strany, a že teda UPC prípadne jej predajca môžu Účastníka požiadať o vykonanie zodpovedajúcich krokov smerujúcich priamo voči jeho účastníkom za účelom prevencie porušenia Zásad prijateľného používania; a (b) ak to vyžaduje zákon, UPC môže informovať príslušné donucovacie orgány, ak sa dozvie o akejkoľvek nelegálnej činnosti prevádzkovanej v sieti UPC alebo prenášanej jej prostredníctvom.

12.3 Práva UPC. Ak UPC dospeje k záveru, že Účastník nesplnil niektoré ustanovenie tohto článku 12 alebo urobil prípadne sa pokúsil urobiť niečo z tu popísaných zakázaných činnosti, Účastník súhlasí s tým, že UPC je oprávnená bezodkladne prijať nápravné opatrenia, ktoré zahŕňajú najmä, nie však výlučne, pozastavenie Služby UPC Anti-DDoS a/alebo ukončenie tejto Služby na základe oznámenia (ktoré môže byť tiež zaslané e-mailom) doručeného (48) hodín vopred. Takéto nápravné opatrenie existuje okrem prípadných ďalších práv UPC vyplývajúcich z tejto Špecifikácie alebo zo zákona. UPC môže Účastníkovi predložiť oznámenie o svojom zámere prijať opatrenia podľa tohto článku, avšak nie je povinná tak urobiť.

UPC môže podľa vlastného uváženia kedykoľvek vykonať zmeny alebo aktualizácie týchto Zásad podľa ustanovenia článku 2.4. Všeobecných podmienok. Účastník je povinný spolupracovať s UPC a/alebo s jej predajcami pri vykonávaní akýchkoľvek nápravných alebo preventívnych opatrení, ktoré môžu UPC alebo jej predajcovia považovať za nevyhnutné.

13. Dodržiavanie Právnych predpisov

Každá zo zmluvných strán súhlasí, že bude v súvislosti s plnením tejto Zmluvy dodržiavať všetky platné miestne zákony, predpisy a nariadenia. UPC je oprávnená pozastaviť plnenie akýchkoľvek svojich záväzkov vyplývajúcich z tejto Zmluvy o ochrane, a to aj bez predchádzajúceho oznámenia a bez vzniku akejkoľvek zodpovednosti, ak Účastník nedodrží ustanovenia tohto článku 13.

14. Rôzne

14.1 Rozhodné právo. Táto Zmluva o ochrane sa vo všetkých ohľadoch riadi právnym poriadkom krajiny založenia UPC a bude vykladaná a vymáhaná v súlade s tým právnym poriadkom.

14.2 Vyššia moc. S výnimkou platobných záväzkov Účastníka nebude žiadna zo zmluvných strán v omeškaní podľa tejto Zmluvy ani nebude voči druhej zmluvnej strane zodpovedná za akékoľvek pozastavenie, prerušenie alebo zdržanie s plnením svojich záväzkov vyplývajúcich z tejto Zmluvy (okrem platobných záväzkov), ak bude taký stav spôsobený zemetrasením, povodňou, požiarom, búrkou, prírodnou katastrofou, pôsobením vyššej moci, vojnou, terorizmom, ozbrojeným konfliktom, štrajkom, odstávkou, bojkotom alebo inými skutočnosťami mimo rozumnej kontroly príslušnej zmluvnej strany, avšak s tým, že strana dovolávajúca sa tohto ustanovenia (a) bude bezdokladne písomne informovať druhú stranu o tejto skutočnosti; a (b) urobí všetky kroky, ktoré sú v primeranom rozsahu nevyhnutné na zmiernenie dopadov takejto vyššej moci, a ďalej za predpokladu, že ak bude pôsobenie vyššej moci trvať v súhrne dlhšie než šesťdesiat (60) dní, je každá zo zmluvných strán oprávnená vypovedať túto Zmluvu o ochrane s okamžitou účinnosťou alebo na základe písomnej výpovede doručenej druhej zmluvnej strane.

14.3 Poradie prednosti pri výklade. V prípade rozporov medzi ustanoveniami tejto Prílohy majú v rozsahu takéhoto rozporu prednosť ustanovenia Špecifikácie služieb, avšak iba vo vzťahu ku konkrétnej Službe UPC Anti-DDoS na základe príslušnej Špecifikácie. Ak bude sieť UPC vyžadovať kapacitu zo služby UPC Anti-DDoS v rozsahu znemožňujúcom zaistenie úplnej ochrany internetovej prevádzky Účastníka, majú interné a vlastné potreby ochrany UPC prednosť pred potrebami Účastníka.