Prilog 6.3.4. Specifični uslovi usluge Zaštita od DdoS napada

1. Predmet Specifičnih uslova

Član 1.

(1) Ovim Specifičnim uslovima utvrđuju se specifičnosti pružanja i korištenja dodatne usluge Zaštita od DDoS napada (u daljem tekstu: Usluga).
(2) Usluga je namijenjena poslovnim korisnicima koji imaju potrebu za zaštitom svog internet poslovanja od DDoS napada.
(3) Za sve što nije regulisano ovim Specifičnim uslovima na odgovarajući će se način primijenit odredbe Opštih uslova za pružanje telekomunikacionih usluga BH Telecoma (u daljem tekstu: Opšti uslovi), Cjenovnika usluga u unutrašnjem i međunarodnom saobraćaju BH Telecoma (u daljem tekstu: Cjenovnik) i drugih specifičnih uslova usluga BH Telecoma koje Pretplatnik/Korisnik koristi.

2. Karakteristike usluge

Član 2.

(1) Usluga je omogućena korisnicima Dedicated servera, Business PRO paketa i paketa Eduka (u daljem tekstu: Pretplatnik).
(2) Za aktiviranje Usluge potrebno je da korisnik prethodno ima aktiviranu jednu od usluga navedenih u prethodnom stavu.

Član 3.

(1) Usluga obuhvaća detekciju, mitigaciju (sprječavanje) i izvještavanje o DDoS napadu.

Član 4.

(1) Sistem reaguje na DDoS napade automatski, a počinje 60 sekundi nakon detekcije napada, te u tom periodu korisnik neće biti zaštićen od napada što može uticati na performanse sistema koji je napadnut.
(2) Usluga ne garantuje 100% zaštitu korisnika, zbog kompleksnosti napada, te može doći do manjih gubitaka u validnom saobraćaju.

Član 5.

(1) Zaštita se vrši od slijedećih DDoS napada:
Invalid Packets (Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment , Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number), Zombie Detection, IPv4 Address Filter Lists, TCP Connection Reset, Payload Regular Expression, DNS Scoping, DNS Malformed Filtering, DNS Query Rate Limiting, DNS NXDomain Rate Limiting, DNS Regular Expressions, Malformed HTTP Filtering, HTTP Scoping, HTTP Rate Limiting, (HTTP Object Limiting, HTTP Request Limiting), HTTP/URL Regular Expression, Malformed SIP Filtering, SIP Request Limiting.

(2) BH Telecom putem ATLAS servisa vrši konstantno ažuriranje ARBOR sistema, čime se omogućava zaštita od najnovijih malicioznih napada.
(3) BH Telecom odgovara da će se pravovremeno izvršiti zaštita korisnika od raznih vrsta malicioznih napada koji su utvrđeni specifikacijom proizvođača opreme tj. ARBORA, a ne odgovara za eventualne posljedice koje mogu nastati na opremi korisnika u vremenu do realizacije usluge tj. do detekcije napada.
(4) BH Telecom ne garantuje da će u 100% slučajeva napada, validan saobraćaj odvojiti od malicioznog saobraćaja, tj. može doći do određenih gubitaka validnog saobraćaj, ali i slučajeva da sistem nije u stanju detektovati i odvojiti maliciozan saobraćaj. Sistem zaštite od DDOS napada detektuje i otklanja maliciozni saobraćaj u slučajevima da je izvor/generator DDoS napada izvan autonomnog sistema BH Telecoma. Također, pošto vrijeme detekcije traje 60 sekundi u tom intervalu korisnik neće biti zaštićen od napada što može uticati na performanse njegovog uređaja npr. servera i nakon uspostavljanje zaštite.

Član 6.

BH Telecom ne odgovara za eventualne posljedice na strani korisnika, a koje mogu nastati u vremenu do realizacije Usluge tj., do detekcije napada.

3. Završne odredbe

Član 7.

(1) Specifični uslovi dostupni su na prodajnim mjestima BH Telecoma i na službenoj web stranici BH Telecoma www.bhtelecom.ba.
(2) Ovi Specifični uslovi stupaju na snagu danom donošenja i primjenjivat će se po proteku 30 dana od dana objavljivanja.
(3) BH Telecom zadržava pravo izmijene ovih Specifičnih uslova u skladu sa primjenjivim propisima.
(4) BH Telecom će ove specifične uslove i njihove kasnije izmjene i dopune objaviti i učiniti dostupnim na način utvrđen pravilima Regulatorne agencije za komunikacije Bosne i Hercegovine.