# DDOS PROTECTION SERVICE

## DDoS attacks – a high risk for companies.

The aim of Distributed-Denial-of-Service (DDoS) attacks is to limit the availability of websites, computers or entire network segments and even to bring them to a complete standstill.

In general, two types of DDoS attack can be identified. Sophisticated DDoS attacks target a weak point in the application layer. The attack requires little bandwidth and can be identified and prevented by the customer using appropriate protective mechanisms. A DDoS brute-force attack is generally based on the network layer and is carried out by several dispersed computers (botnets). Often, high data volumes are created which slow or block the customer's Internet access and IT infrastructures. This results in direct economic damage for the victim. For this type of attack, UPC Business provides a DDoS protection service.

### DDoS attacks (brute force)

Compared to a traditional hacker attack whereby the target system is invaded, a DDoS attack is much easier for attackers to carry out. In relation to the damage they cause, DDoS attacks are a reasonably-priced online service. For companies with business models and process which are Internet-dependent (such as e-commerce, financial institutes, e-media and cloud-based IT companies), a DDoS attack can prove to be a very delicate matter. The longer the service is unavailable, the higher the costs incurred and the greater the loss in sales. DDoS attacks are therefore often used to damage rivals or to blackmail companies.

According to a study conducted in the US, average economic damage totals CHF 40,000 per hour. In most cases, DDoS attacks last for several hours and can continue for up to an entire week. Companies subject to a DDoS attack suffer directly and indirectly from a damaged reputation and a loss of trust.

### Effective protection against DDoS attacks

To repel attacks and ensure that services remain available to the customer, UPC Business offers an effective DDoS protection service.

If the protection is activated, the system constantly analyses the data stream for anomalies. If an attack is detected, the data stream is diverted by the threat management system (TMS). The TMS are found in the so-called "scrubbing centres" within the Liberty Global network. In the scrubbing centres, the data stream of the attack is separated from the desired data traffic. After this separation process, the clean data stream is transferred to its target so that the customer can continue to do business.

### Effective extension for Business Internet and IP Transit customers

The DDoS Protection Service is a service option for Business Internet and IP Transit customers. With the DDoS Protection Service, customers enjoy optimum protection against a wide range of flooding attacks.

Activating the DDoS Protection Service increases the Internet traffic latency period due to the diversion of the traffic via the TMS. The increase in the latency period depends on the Internet source (user) and the TMS used.

A prerequisite for activation of the DDoS Protection Service is 24/7 support for the underlying Internet service.

upc business

## Standard features

| | | |
|---|---|---|
| Service | Prerequisite for the DDoS Protection Service is a Business Internet or IP Transit connection from UPC Business with 24/7 support | |
| Service and support | **Fault acceptance** | 7 × 24 : 365 days |
| | **Support time** | 7 × 24 : 365 days |
| | **Service level** | In accordance with the underlying Business Internet or IP Transit service |

The details in this document do not constitute a binding offer. Subject to modification without notice.
Date of publication: July 2019