DDOS PROTECTION SERVICE

Gli attacchi DDoS: un grande rischio per le aziende.

Gli attacchi Distributed Denial of Service (DDoS) hanno l'obiettivo di ridurre la disponibilità di siti web, computer o interi segmenti di rete, fino a bloccarli completamente.

In generale, si distinguono due tipi di attacchi DDoS. Gli attacchi Sophisticated DDoS si concentrano su un punto debole a livello di applicazioni. L'attacco richiede una larghezza di banda ridotta e può essere identificato e bloccato da parte dei clienti utilizzando appositi meccanismi di protezione. Un attacco DDoS Brute Force si colloca principalmente a livello di rete e viene eseguito contemporaneamente da diversi computer (botnet). Spesso genera grandi volumi di dati, che rallentano o bloccano la connessione Internet e le infrastrutture IT del cliente. In questo modo, la vittima rischia danni economici diretti. Per questo tipo di attacchi, UPC Business offre la sua protezione DDoS Protection.

Attacchi DDoS (Brute Force)

Rispetto ad un classico attacco da parte di hacker, che penetrano all'interno del sistema d'arrivo, un attacco DDoS è notevolmente più semplice da portare a termine per gli aggressori. Rispetto ai danni che provocano, gli attacchi DDoS non sono costosi da ot-tenere su Internet come servizio. Ed è proprio per le aziende i cui modelli commerciali e processi dipendono da Internet (ad es. e-commerce, istituti finanziari, media digitali e aziende IT basate su cloud), un attacco di questo tipo può rivelarsi una questione molto spinosa dal punto di vista economico. Più a lungo un servizio rimane indisponibile, maggiori sono i costi e i danni sul fatturato. Per questo gli attacchi DDoS vengono spesso utilizzati per danneggiare aziende concorrenti o per ricattarle.

Secondo uno studio statunitense, i danni economici ammontano in media a 40 000 CHF per ogni ora. Nella maggior parte dei casi, gli attacchi DDoS durano diverse ore e possono protrarsi fino ad una settimana intera. Le aziende colpite da un attacco di questo tipo soffrono direttamente, ma anche indirettamente per danni alla reputazione e alla fiducia.

Protezione efficace contro gli attacchi DDoS

Allo scopo di proteggersi dagli attacchi e di assicurare la disponibilità continua dei servizi del cliente, UPC Business offre l'efficace protezione DDoS Protection.

Quando questa è attivata, il sistema analizza continuamente il flusso dati allo scopo di rilevare anomalie. Se si riscontra un attacco, questo viene deviato su un Threat Management System (TMS). Questi TMS risiedono spesso nei cosiddetti «scrubbing center» all'interno della rete di Liberty Global. Negli «scrubbing center», il flusso dati degli attacchi viene separato dal traffico dati «sano». Dopo questa separazione, il flusso pulito viene trasmesso a destinazione, consentendo al cliente di continuare la sua attività.

Aumento effettivo dei clienti per i collegamenti Business Internet e IP Transit

DDoS Protection Service è un'opzione di assistenza per clienti Business Internet e IP Transit. Con DDoS Protection Service, il cliente è protetto in maniera ottimale contro i tipi più disparati di attacchi di tipo flooding.

Con l'attivazione di DDoS Protection Service, i tempi di latenza del traffico Internet vengono aumentati con la deviazione su TMS. L'aumento dei tempi di latenza dipende dalla connessione Internet del cliente e dal TMS impiegato.

Come prerequisito per l'attivazione, DDoS Protection Service richiede che il servizio Internet disponga di assistenza 7 × 24.

upc business

Caratteristiche standard

Servizio	DDoS Protection Service richiede come prerequisito una connessione Business Internet o IP Transit di UPC Business con assistenza 7 × 24	
Servizio e supporto	**Segnalazione guasti**	7 × 24: 365 giorni l'anno
	Orario di supporto	7 × 24: 365 giorni l'anno
	Service level	A seconda del servizio Business Internet o IP Transit disponibile

Data di pubblicazione: Luglio 2019