17.07.2023

Che cos'è un attacco Denial of Service?

Nelle ultime settimane si è letto più volte di attacchi sferrati contro aziende o istituzioni pubbliche per impedirne il normale funzionamento. Alla base di tutto c'è spesso un cosiddetto attacco DDoS.

Non smettono mai i casi di criminali informatici che riescono a paralizzare intere aziende o amministrazioni. In genere sfruttano il ransomware, cioè un cavallo di Troia ricattatore o crittografante. Un altro metodo usato con maggiore frequenza negli ultimi tempi è l'attacco Distributed Denial of Service.

Un attacco DDoS consiste in un attacco al sito Internet o al server di un'azienda sferrato da più fonti contemporaneamente. Un alto numero di dispositivi (solitamente parte di una botnet) bombarda il bersaglio con una serie innumerevole di richieste. Come risultato, il sito Internet o il server non riescono a resistere al sovraccarico e non sono più accessibili, oppure solo limitatamente. Dietro gli attacchi DDoS alle aziende si cela spesso un tentativo di ricatto. Se non viene pagato quanto richiesto, i criminali minacciano di ripetere gli attacchi.

Purtroppo non esiste una protezione valida al 100% contro gli attacchi Denial of Service. Le aziende possono mettere in campo servizi di verifica per riconoscere e bloccare tempestivamente gli attacchi DDoS, ma comunque con un'efficacia limitata, dato che l'attacco proviene da tante fonti diverse. Ridurre i punti deboli aiuta comunque a contenere gli effetti di un attacco – maggiori informazioni sono disponibili nella nostra sezione «Suggerimenti per le PMI (https://www.ebas.ch/pmi) ».