

# Attacco DDoS – che fare?

## Lista checking per tecnici di imprese aggredite

### Procedure generali fiancheggianti

Come dipendente di un'impresa danneggiata Lei è ben consigliato a tenere presente, prendendo le misure di carattere tecnico-tattico sotto descritte, che vanno informati eventualmente anche i responsabili delle relazioni affari e clienti, di modo che possano riuscire a loro volta a comunicare. A Sua propria discarica si raccomanda di coinvolgere l'ufficio comunicazioni aziendale – esso può pure identificare gli stakeholder interessati e proporre una definizione delle priorità.

#### 1. Prenda contromisure

- > Contatti il Suo provider internet per sventare l'attacco.
- > Eventualmente riesce a prendere Lei stesso delle contromisure bloccando l'indirizzo IP sul firewall (blocco GEO) oppure adattando il routing in modo adeguato.

#### 2. Informi il corpo di polizia del Suo cantone come anche MELANI e definisca assieme a loro la procedura di seguito

- > Nomini il Suo provider internet e l'indirizzo sia della fonte sia dell'obiettivo dell'attacco. L'autorità inquirente riuscirà così a iniziare le indagini.

#### 3. Metta al sicuro i dati rilevanti

- > Dopo la fine dell'attacco, salvi i log rilevanti, particolarmente quelli del firewall, e li trasmetta all'autorità inquirente come allegati e-mail.
- > Qualora i colpevoli abbiano spedito una lettera di ricatto via e-mail, si può impacchettare la rispettiva e-mail in un file ZIP e trasmetterlo all'autorità inquirente come allegato e-mail.

#### 4. Controlli la Sua rete per verificare la presenza di anomalie

Attacchi DDoS vengono spesso usati per mascherare altri attacchi quali per esempio l'innesto di malware o il furto di dati. Per questo motivo dovrebbe controllare la Sua rete alla ricerca di anomalie dopo ogni attacco DDoS sventato.