# DDoS Attack – What to Do?
## Checklist for Technicians of Attacked Companies

### General Supporting Processes

As a damaged party, when considering the following technical-tactical measures your company should bear in mind that if necessary, business and relationship managers, among others, must be informed in such a way they are able to communicate for their part. To relieve your own workload, it is recommended that you get corporate communications involved; they can also identify further stakeholders and suggest a prioritisation.

### 1. Take Countermeasures

> Contact your internet provider in order to stop the attack.
> You may take countermeasures yourself by blocking the IP addresses on the firewall (geo-- blocking) or making the according adaptations to routing.

### 2. Inform Your Cantonal Police Corps and MELANI, and Define the Further Procedure Together

> Name your internet provider and the source and target addresses of the attack. This allows law enforcement to initiate investigations.

### 3. Secure the Relevant Data

> After the attack is over, secure the relevant logs, especially those of the firewall, and send them to law enforcement as e-mail attachments.
> If the perpetrator/s sent a ransom letter by e-mail, you can compress this e-mail into a ZIP file, and send it to law enforcement as an e-mail attachment.

### 4. Check Your Network for Anomalies

DDoS attacks are often used to mask other attacks, such as infiltration with malware, or data theft. This is why you should check your network for anomalies after a DDoS attack.

NEDIK in cooperation with MELANI and Swiss Cyber Experts