DDoS-Angriff – was tun?
Checkliste für Technikbeauftragte angegriffener Unternehmen

Allgemeine flankierende Prozesse

Als geschädigtes Unternehmen sollten Sie bei all den nachstehend beschriebenen technisch-taktischen Massnahmen im Auge behalten, dass gegebenenfalls unter anderem Geschäfts- und Kundenverantwortliche so informiert werden müssen, dass sie ihrerseits kommunizieren können. Zur eigenen Entlastung empfiehlt es sich, die Unternehmenskommunikation einzubeziehen – sie kann auch umgebende Stakeholder identifizieren und eine Priorisierung vorschlagen.

1. Ergreifen Sie Gegenmassnahmen

> Kontaktieren Sie Ihren Internetprovider, um den Angriff zu stoppen.
> Unter Umständen können Sie selbst Gegenmassnahmen ergreifen, indem Sie die IP-Adressen auf der Firewall blockieren (GEO-Blocking) oder das Routing entsprechend anpassen.

2. Informieren Sie Ihr kantonales Polizeikorps sowie MELANI und definieren Sie zusammen das weitere Vorgehen

> Benennen Sie Ihren Internetprovider sowie die Quell- und Zieladressen des Angriffs. Damit können die Strafverfolgungsbehörden erste Ermittlungen aufnehmen.

3. Sichern Sie die relevanten Daten

> Sichern Sie die relevanten Logs nach Beendigung des Angriffs, insbesondere jene der Firewall, und übermitteln Sie diese an die Strafverfolgungsbehörden per E-Mail-Anhang.
> Falls die Täterschaft ein Erpressungsschreiben per E-Mail versandte, kann dieses E-Mail in eine ZIP-Datei verpackt und den Strafverfolgungsbehörden als E-Mail-Anhang übermittelt werden.

4. Überprüfen Sie Ihr Netzwerk auf Anomalien

DDoS-Angriffe werden häufig benutzt, um andere Angriffe wie das Einschleusen von Malware oder den Diebstahl von Daten zu verschleiern. Deshalb sollten Sie Ihr Netzwerk nach einem DDoS-Angriff auf Anomalien überprüfen.

In Zusammenarbeit mit MELANI und Swiss Cyber Experts