**Merkblatt «DoS / DDoS-Angriff»**

**Worum geht es?**

Diese Angriffe zielen darauf ab, einen Dienst für deren Benutzer unerreichbar zu machen. Die gängigste Methode besteht darin, Computer oder Netzwerke gezielt mit einer grösseren Anzahl Anfragen zu bedienen, als diese verarbeiten können. Dies wiederum führt dazu, dass das System überlastet wird und reguläre Anfragen nicht oder nur sehr langsam beantwortet werden können.

Diese Angriffe werden auf verschiedenste Arten ausgeführt. Beispielsweise indem an ein Computersystem inkorrekt gestellte Anfragen gesandt werden, wenn die maximale Zahl der Anwender überschritten wird oder indem der Server von weit mehr E-Mails überflutet wird, als er empfangen und verarbeiten kann. In den meisten Fällen führt ein solcher Angriff zum Totalabsturz des Systems.

Die Motivation hinter solchen DDoS-Attacken sind meistens politischer Aktivismus, Erpressung oder Schädigung eines Konkurrenten.

**Tipps**

- Überwachen Sie die Verfügbarkeit Ihrer Kundenanwendungen auch aus der Sicht Ihrer Kunden, das heisst vom Internet her.
- Ihre Systeme sind gehärtet (keine unnötigen Dienste, strikte Rechtevergabe, starke Authentisierung, usw.) und auf aktuellem Patch-Level.
- Prüfen Sie die Möglichkeiten eines GeoIP Blockings. Wenn Ihre Kunden vorwiegend aus der Schweiz und dem nahen Ausland stammen, können Sie ein Profil vordefinieren, welches IP Adressen aus diesem Raum entweder Priorität einräumt oder andere IP Adressen blockiert. Im Angriffsfall können Sie dieses Profil aktivieren und gewinnen so sehr schnell an Handlungsoptionen und zusätzlichem Schutz.
- Systeme, die potenziell Opfer eines DDoS-Angriffs werden könnten (z.B. Webauftritte), sollten an einem anderen Internet-Uplink hängen als die übrigen Systeme der Organisation.
- Eine Web-Application Firewall minimiert die Angriffsfläche auf webbasierte Dienste.

Rechtliche Grundlagen:
Art. 144bis StGB, 156 StGB