*Authored by Lenny Zeltser in English. Translated to German by Carsten Probst. Original at https://zeltser.com/ddos-incident-cheat-sheet. Distributed according to the Creative Commons v3 “Attribution” License.*

**Grundsätzliche Vorgehensweise bei DDoS Angriffen:**

1. Vorbereitungen: Kontakte knüpfen und Verfahren definieren sowie Tools festlegen um während eines Angriffs wertvolle Zeit zu sparen
2. Analyse: den Vorfall erkennen, den Umfang der Attacke bestimmen und die relevanten Personen hinzuziehen
3. Mitigation: Abmilderung des Angriffs auf die Zielumgebung
4. Wrap-up: die Details des Vorfalls dokumentieren, Lessons learned besprechen und Pläne zur Abwehr/Verteidigung anpassen

**Allgemeine und grundlegende Aspekte:**

* DDoS-Attacken treten meist in der Form auf, dass das Netzwerk mit unerwünschten Datenverkehr überflutet wird; manche

Angriffe konzentrieren sich auch auf Ressourcen nur eines bestimmten Systems

* Es ist sehr schwer, wenn nicht sogar unmöglich, sich gegen einen Angriff zu verteidigen ohne spezielle Ausrüstung oder die Hilfe von Experten oder dem Internet Service Provider
* Es empfiehlt sich ein kleines kompetentes Team zu bilden und mit diesem Team den Angriff zu bewältigen
* DDoS Angriffe können sich über viele Tage erstrecken. Vorab Überlegungen machen wie das Team während eines längeren Angriff aufgestellt werden muss - Menschen werden irgendwann mal müde
* Die Fähigkeiten des vorhandenen Equipments vorab verstehen lernen um eine DDoS-Attacke abzufangen - Know your Tools!

**Vorbereitungen für einen Angriff:**

* ohne gute Vorbereitung verliert man im Falle eines Angriffs sehr wertvolle Zeit
* Kontakt zum eigenen ISP aufnehmen um zu verstehen welche Anti-DDoS Verfahren der ISP anbietet und welchen Prozess er dafür vorsieht
* Erstellen einer White-List der Source-IPs und Protokolle die unbedingt zugelassen werden müssen wenn während eines Angriffs bestimmter Datenverkehr priorisiert/durchgelassen werden muss/soll. Wichtige Kunden und Lieferanten beachten!
* DNS TTL Einstellungen für potentiell gefährdete Systeme absenken um bei Bedarf einen DNS Schwenk zu erleichtern wenn die ursprünglichen IP-Adressen angegriffen werden
* Kontakte/Schnittstellen zu folgenden Funktionen festlegen: ISP, Firewall-, System- und Netzwerkteams und  ggf. Strafverfolgungsbehörden
* detaillierte Dokumentation der IT-Infrastruktur (inkl. IP-Adressen, Netzwerk-Topologie und einer Übersicht vorhandener Systeme
* Auswirkungen von eventuellen DDoS Angriffen feststellen (Umsatzverlust, Imageschaden)
* bei hohem Risiko eines DDoS Angriffs sollte die Anschaffung spezialisierter Anti-DDoS Systeme erwogen werden
* grundsätzlich sollten alle Komponenten der Umgebung (Netzwerk, OS und Applikationen) die durch eine DDoS Attacke gezielt angegriffen werden können, gehärtet werden

**Analyse eines (laufenden) Angriffs:**

* den Ablauf der DDoS-Attacke verstehen lernen und besonders betroffene Komponenten identifizieren
* laufende Überprüfung der Systemlast und Logdateien von Servern, Routern, Firewalls, Applikationen und anderer betroffener Infrastruktur (Logdaten zentral erfassen!)
* Identifikation der besonderen Merkmale des schädlichen DDoS Datenverkehrs sowie Feststellung was den DDoS Traffic von legitimen Traffic unterscheidet (zum Beispiel spezifische Quelle IPs, Ziel Ports, URLs, TCP-Flags, etc.).
* nach Möglichkeit ein Netzwerkanalysetool (z.B. tcpdump, ntop, MRTG oder SFlow-Tool) verwenden um den Traffic auf obige Merkmale zu überprüfen
* den Internet Service Provider sowie alle relevanten internen Teams kontaktieren um die jeweilige Sicht auf das Problem zu besprechen
* bei Kontakt mit dem ISP möglichst ganz genaue Angaben zum schädlichen Traffic machen der gefiltert werden soll (welche Netze blockieren? Rate-Limit welcher Quell-IPs?)
* ggf. prüfen ob das Unternehmen im Vorfeld des DDoS Angriffs erpresst wurde
* Falls möglich eine NDIS Signatur erstellen um sich auf schädlichen Traffic konzentrieren zu können, und zwischen gutartigen und bösartigen Traffic unterscheiden zu können
* Info an die Geschäftsleitung ggf. wird dort eine Strafverfolgung beabsichtigt

**Auswirkung des Angriffs abmildern:**

* Während eines laufenden Angriffs ist es sehr schwierig die gesamte DDoS-Attacke zu blockieren, meist ist aber eine Abmilderung der Auswirkungen möglich
* DDoS Traffic sollte so nah wie möglich am Perimeter des eigenen Netzwerks abgewehrt werden um die Auswirkung des schädlichen Datenverkehrs zu minimieren
* unerwünschte Verbindungen oder nicht benötigte Prozesse auf eigenen Systemen deaktivieren
* nach Möglichkeit auf eine alternative Webseite oder andere Netzwerkblöcke mittels DNS oder anderer Verfahren umswitchen  und den ursprünglichen Traffic nullrouten/blackholen
* Sollte ein besonderes Merkmal der angegriffenen Applikation einen Bottleneck darstellen, sollte eine zeitweise Abschaltung dieser Komponente geprüft werden
* evtl. kann zusätzliche Netzwerk-Bandbreite hinzugeschaltet werden um der Last des DDoS Traffics Herr zu werden (Katz&Maus Spiel!)
* wenn möglich (z.B. bei Verwendung von providerunabhängigen IPs) den Traffic durch BGP Announcement über ein Scrubbing Center eines Anti-DDoS Anbieters leiten (ggf. Wechsel auf PI Space zur künftigen Vorbereitung auf DDoS)
* Wenn Verteidigungsmassnahmen getroffen werden, dann lautet eine wichtige Regel immer nur eine Einstellung zu verändern und deren Auswirkung zu beobachten bevor eine weitere Änderung durchgeführt wird
* Konfigurieren eines Egress Filters um Traffic zu unterdrücken den die eigenen Systeme aufgrund des DDoS Traffics erzeugen - dies verhindert unnötigen Traffic im eigenen Netzwerk

**Review des Angriffs und Nachjustieren der eigenen Reaktionen**

* welche Massnahmen/Schritte hätten getroffen werden können, um auf den Vorfall schneller und effizienter reagieren zu können
* Annahmen die vor einem laufenden Angriff gemacht wurden, nochmal mit dem Wissen nach einem DDoS Angriff anpassen und nachjustieren
* Effektivität und Effizienz der getroffenen Massnahmen sowie der Kommunikation bewerten
* überlegen welche Ressourcen  innerhalb und außerhalb der eigenen Organisation könnten bei einem künftigen Angriff helfen