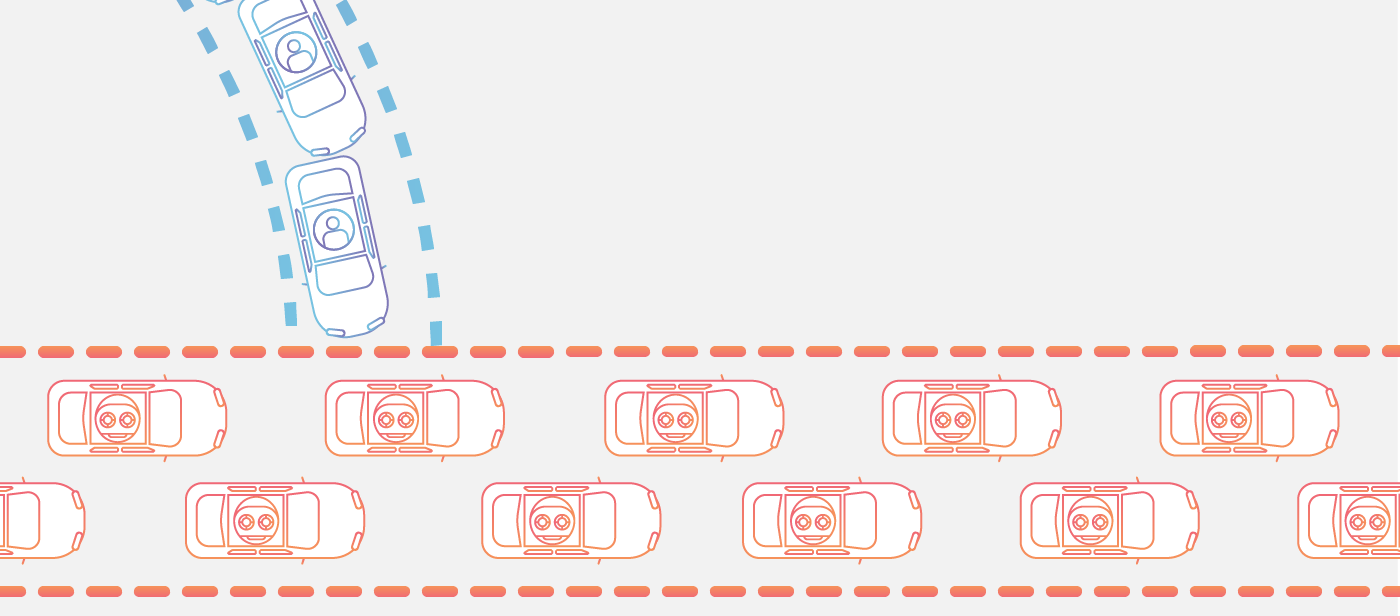
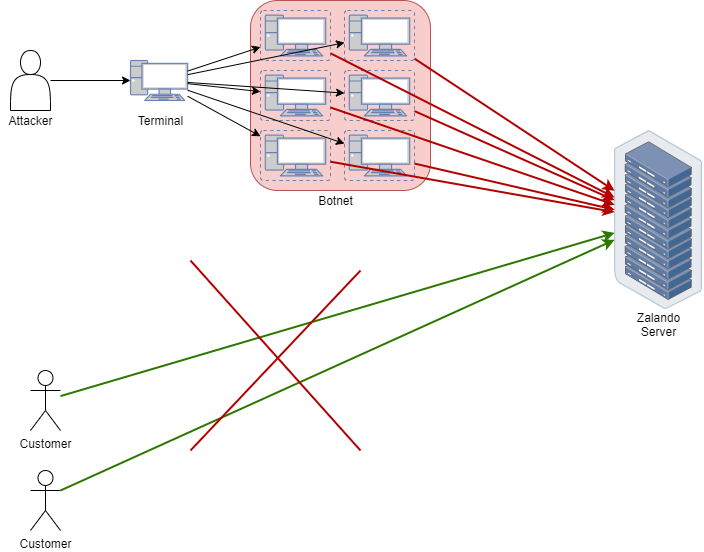
DDOS

Distributed Denial Of Service

# DDOS Attacke erklärt

DDOS ist eine Abkürzung für «distributed denial of service», was auf Deutsch so viel heisst wie: «verteilte Ablehnung vom Service». Eine solche Attacke bezweckt das Lahmlegen oder Verlangsamen eines Service, damit der Zugriff für den Endbenutzer eingeschränkt wird. Bei einem Online Händler wie Digitec oder Zalando kann dies einen hohen finanziellen Verlust anrichten.

In der Regel wird bei einem solchen Angriff mehrere Datenpakete mit möglichst hohem Volumen beim Opfer angefragt. Dieser Versucht die Anfragen zu beantworten, da es jedoch viele Anfragen gibt, wird dadurch der Service verlangsamt oder stürzt ab. Wenn man von einer DDOS Attacke redet werden die Anfragen von mehreren verschiedenen Quellen gesendet (man redet von einem Bot Netz), bei einer DOS Attacke kommen die Anfragen immer von derselben Quelle.

Im folgenden Bild sollten die Roten Autos die anfragen vom Angreifer darstellen. Die Blauen Autos stellen die Anfragen von den Endbenutzern dar. Wie man sieht kommen keine legitimen Anfragen durch, da der Angreifer die Leitung quasi blockiert mit den eigenen Anfragen.

# Szenario

Ein Hacker möchte Zalando schaden und diese mit einer DDOS Attacke blockieren. In der Grafik auf der rechten Seite ist zu erkennen wie das ganze ablaufen sollte. Der Hacker erstellt ein Botnetz aus verschiedenen Physischen oder Virtuellen Geräten. Mit einem Zentralem Kontrollsystem gibt der Hacker dem Botnetz einen Befehl. Anschliessend wird jedes Gerät aus dem Botnetz mehrere tausend Anfragen an den Server senden. Der Server kann die Anfragen nicht alle abwickeln und der Zugang für potenzielle Kunden wird blockiert.

# Schutzmassnahmen

## Angriffsfläche verringen

Wenn die Angriffsfläche verringert wird, werden die Optionen für Angreifer eingeschränkt und die Schutzmassnahmen müssen nur an einem Ort eingerichtet werden. Die Anwendung sollte vor Kontakt mit irrelevanten Ports oder Protokolle geschützt sein, somit wird die Angriffsfläche minimiert. Da dies nicht in der Applikation selbst umgesetzt werden kann, werde ich dies nicht genauer erklären.

## Service gegen DDOS

Es gibt mehrere verschiedene Services im Internet welche die Applikation vor DDOS Attacken schützen kann. Diese Service analysieren den Datenverkehr von Verschiedenen Webseiten und kann so mit Hilfe von Künstlicher Intelligenz DDOS Attacken erkennen und blockieren. Auch auf Firewalls können Funktionen aktiviert werden, welche gegen DDOS schützen sollten. Wie diese genau funktionieren ist sehr komplex. Jedoch gibt es keinen kompletten Schutz gegen DDOS Attacken, da die Anfragen von normalen Anfragen schlecht bis zu gar nicht unterschieden werden können.

## Schlussfolgerung

Schlussendlich kann man sich gegen DDOS Attacken nicht 100%ig schützen. Man kann lediglich die Angriffsmöglichkeiten einschränken und einfache DDOS Attacken mithilfe eines Service unterbinden.