Denial-of-Service-Angriff

Als Denial-of-Service-Angriff (kurz „DoS-Attacke“) wird in der Informationstechnik ein Hackerangriff bezeichnet, bei dem ein Server so lange mit Anfragen bombardiert wird, bis er aufgrund von Überlastung nicht mehr reagiert.

Definition

„Denial of Service“ bedeutet übersetzt „Dienstverweigerung“. DoS-Angriffe führen demnach dazu, dass der attackierte und überlastete Server seine Dienste verweigert. Sie werden absichtlich herbeigeführt und haben in der Regel das Ziel, einen ganz bestimmten Dienst einzuschränken oder komplett zu blockieren. Dazu werden die zur Verfügung stehenden Programme oder Netzwerk-Ressourcen außerordentlich frequentiert, manchmal auch kollektiv von tausenden Nutzern. Der Server ist daraufhin entweder nicht mehr erreichbar oder kann zusammenbrechen.

Varianten

DoS-Attacken können auf verschiedene Wege vorbereitet und durchgeführt werden. Zu den häufigsten Formen zählen u. a.

IP-Spoofing (Vortäuschen einer falschen oder das Fälschen einer IP-Adresse): Der Angreifende verwendet die Netzwerkadresse eines autorisierten Benutzers und erhält den Zugriff auf bestimmte Ressourcen eines Netzwerks oder eines Systems.

Mailbombing: Der Mail-Empfänger wird mit bis zu tausend E-Mails bombardiert. Das Herunterladen nimmt so viel Zeit in Anspruch, dass der Mail-Empfänger überlastet ist und korrekte Mails nicht mehr öffnen kann.

SYN-Flooding: Gezielter Angriff auf einen Server, um diesen zu überlasten und zum Absturz zu bringen. Der Verbindungsmechanismus vom TCP-Protokoll wird geflutet, um den Server mit falsch beschrifteten TCP-Datenpaketen zu überfordern.

Ping-Flooding / Smurf-Attacke: Gezielter Angriff durch den die Systemperformance von Servern stark beeinträchtigt wird oder der Server abstürzen kann. Wie im Ping-Pong-Verfahren wird der Server mit unzähligen ICMP-Echo-Requests bombardiert. Durch die hohe „Pingzahl“ sinkt das Antwortverhalten des Servers und die Netzverbindung wird stark belastet.

Broadcaststurm: Entsteht dann, wenn in einer Netzkonfiguration viele Stationen gleichzeitig eine Antwort übertragen. Jede Antwort erzeugt wiederum mehr Antworten, was sich wie ein Schneeballeffekt auswirkt.

Distributed Denial-of-Service (DDos-Angriff)

Eine besonders böswillige Form von DoS-Angriffen sind sogenannte DDos-Attacken. Im Gegensatz zur DoS-Attacke erfolgt der Angriff hier von vielen verteilten Rechnern (sogenannten Botnetzen) aus und ist dadurch nur schwer zu orten und noch schwieriger zu unterbinden. DDos-Attacken können nicht nur einzelne Programme oder Server, sondern ganze Netzwerke lahmlegen.

Siehe auch:
Man-in-the-middle-Angriff

Zurück