Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN / INTERNET-DIENSTLEISTER

Zunahme von DDoS-Angriffen durch DNS-Reflection

Das BSI beobachtet in den letzten Monaten eine deutliche Zunahme von Distributed-Denial-of-Service (DDoS)-Angriffen, die DNS-Reflection Techniken einsetzen. Hierbei wurden bereits Bandbreiten in einer Größenordnung von mehr als 1,7 Terabit pro Sekunde gesehen.

Das Domain-Name-System (DNS) ist analog eines Telefonbuches für die Übersetzung von Namen in IP-Adressen zuständig und wurde erstmals im Jahr 1983 spezifiziert. Aufgrund mangelhafter Sicherheitsmechanismen ist es anfällig für Manipulationen und kann z. B. als Werkzeug für DDoS-Angriffe verwendet werden. Zwei wesentliche Techniken werden nachfolgend beschrieben.

1 DNS-Reflection Angriff

Die Kommunikation zwischen DNS-Servern erfolgt standardmäßig über das UDP-Protokoll. Bei UDP handelt es sich im Gegensatz zu TCP um ein verbindungsloses Protokoll. Da innerhalb des DNS-Protokolls auch sonst keine Prüfmechanismen existieren, besteht für den Empfänger des DNS-Pakets keine Möglichkeit, die Authentizität der Quelle zu überprüfen.

DNS-Server beantworten Anfragen daher „blind“ an den Server, dessen IP-Adresse im Anfrage-Paket enthalten ist.

Sofern es einem Angreifer gelingt, in einer DNS-Anfrage als Quelladresse die IP-Adresse eines Opfers zu platzieren („IP-Spoofing“) wird der beantwortende Server die Antwort statt an den Angreifer an das Opfer senden (**reflektieren**). Die Identität des Angreifers wird so zum einen verschleiert und zum anderen häufig gleichzeitig die Wucht des Angriffs durch die im Folgenden beschriebene DNS-Eigenschaft erhöht.

2 DNS-Amplification

UDP-Pakete mit DNS-Abfragen sind typischerweise relativ klein (< 100 Byte). Antwort-Pakete sind abhängig vom abgefragten Eintrag deutlich größer (< 500 Byte). Unterstützt der befragte DNS-Server DNSSEC, können die Antwortpakete noch größer werden (> 1000 Byte). Dies hat zu Folge, dass ein Angreifer bei geschickter Wahl der DNS-Anfrage mit vergleichsweise kleiner Bandbreite eine deutliche Erhöhung der Angriffslast auf der Opferseite erzielen kann, der Angriff wird somit verstärkt (**Amplification**).

3 Schlussfolgerung

Das DNS-System kann für Angriffe ausgenutzt werden und als Verstärker missbraucht werden. Die Betreiber von DNS-Servern können so unabsichtlich zum Mittäter bei einem Distributed-Denial-of-Service (DDoS) Angriff werden.

4 Maßnahmen

Im Folgenden werden wichtige mögliche Maßnahmen beschrieben, die DNS-Betreiber umsetzen können.

4.1 BCP-38

Internet-Service-Provider sollten an ihren Netzübergängen die in BCP-38 (Network Ingress Filtering, http://tools.ietf.org/html/bcp38) beschrieben Maßnahmen umsetzen, um die Manipulation der Absender-Adresse in UDP-Paketen (IP-Spoofing) zu verhindern.

4.2 Keine Open-Resolver

Als DNS-Caching-Resolver betriebene Server sollten nur Anfragen aus den eigenen Netzen entgegen nehmen und nicht als „Open Resolver“ aus dem gesamten Internet angesprochen werden können.

4.3 Überwachung von DNS-Servern

DNS-Server sollten verstärkt überwacht werden, um bei Veränderungen zeitnah reagieren und Gegenmaßnahmen ergreifen zu können. Häufig angewendete Gegenmaßnahmen sind:

- **Rate-Limiting**

  Die Anzahl zulässiger Anfragen pro Quelladresse in einem Zeitfenster wird begrenzt. Weitere Anfragen werden entweder abgelehnt, oder nur noch per TCP zugelassen.
- **Black-Listing**

  Auffällige Quelladressen werden für Anfragen gesperrt.
- **Einschränkung von Anfragen**

  Es werden nur noch Anfragen zu bestimmten DNS-Einträgen (Ressource-Records) zugelassen. Anfragen zu weiteren Einträgen (beispielsweise ANY-Anfragen) werden temporär gesperrt.

Eine BSI-Empfehlung zur Reaktion auf DDoS-Angriffe finden Sie unter:
https://www.allianz-fuer-cybersicherheit.de/dok/6643790

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.