EMPFEHLUNG: IT IM UNTERNEHMEN / INTERNET-DIENSTLEISTER

Maßnahmen gegen Reflection Angriffe

Das BSI beobachtet in den letzten Monaten eine deutliche Zunahme an Distributed-Denial-of-Service (DDoS) Angriffen, die sogenannte Reflection-Techniken einsetzen.

Bereits 2012 hat das BSI über eine Zunahme von DNS-Reflection Angriffen berichtet [CSE-042]. Inzwischen werden auch andere Internetdienste für diese Art von Angriffen verwendet. Dazu zählen neben DNS insbesondere NTP, SNMP und CHARGEN.

Reflection Angriff

Bei einem Reflection Angriff wird das Opfersystem nicht direkt angegriffen. Stattdessen spielt der Angreifer „über Bande“ (**reflection**). Dazu sendet er eine Anfrage mit gefälschter Absenderadresse an ein Zielsystem (Bande). Als Absenderadresse wählt er dabei die Adresse des Systems, das er angreifen möchte (Opfersystem). Die Antwort auf die Anfrage des Angreifers erhält dann aufgrund der gefälschten Adresse nicht der Angreifer, sondern das Opfersystem (siehe Abbildung 1).

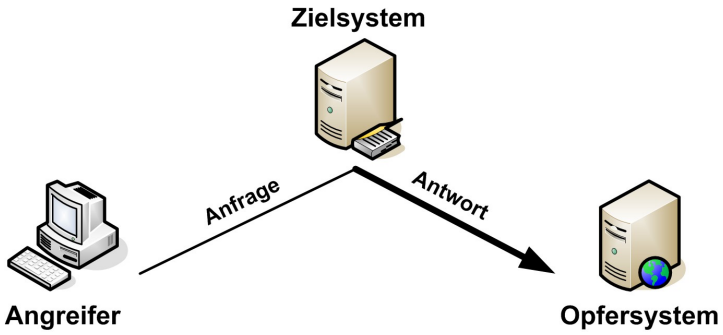

Abbildung 1: Prinzip eines Reflection Angriffs

Die Antwortpakete sind häufig sehr viel größer als die Anfragen. Dadurch ist es dem Angreifer möglich, mit dem Einsatz einer geringen eigenen Bandbreite viel Angriffsbandbreite zu erzeugen. Man spricht in diesem Fall von einer Verstärkung der eingesetzten Bandbreite (**amplification**).

Voraussetzung für diese Art des Angriffs ist die Möglichkeit die Absenderadresse zu fälschen (**IP-Spoofing**). Daher wird für die meisten dieser Angriffe das verbindungslose Transportprotokoll UDP verwendet.

Schlussfolgerung

Eine ganze Reihe an Internetdiensten kann für Angriffe ausgenutzt und als Verstärker missbraucht werden. Die Betreiber solcher Dienste können so unabsichtlich zum Mittäter bei einem Distributed-Denial-of-Service (DDoS) Angriff werden.

Maßnahmen

BCP-38

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

Network Time Protocol (NTP)

NTP dient zur Synchronisation der Systemzeiten (Uhren) zwischen Computersystemen. Unabhängig von der Version sollte der Zugriff auf den NTP-Server eingeschränkt werden (erlaubte Kommandos sowie zulässige IP-Adressbereiche und ggf. Rate-Limiting). Aus dem Internet sollten weder Mode 7 noch Mode 6 Anfragen an den NTP-Server gestellt werden können [RFC 4330].

Insbesondere das NTP Mode 7 Kommando *monlist* wird oft in NTP-basierten Reflection-Angriffen verwendet. Dieses Kommando liefert bei älteren Versionen von NTP-Servern eine Liste von bis zu 600 Systemen zurück, die den NTP-Server zuletzt kontaktiert haben. Durch die damit verbundene Größe der Antwort im Vergleich zur Anfrage lässt sich im Rahmen von DDoS-Angriffen ein enormer Verstärkungsfaktor erzielen. Prinzipiell lassen sich auch NTP Mode 6 Anfragen (bspw. *readvar*) für DDoS-Angriffe ausnutzen. Der Verstärkungsfaktor ist hierbei allerdings geringer.

Die meisten Server basieren auf der Referenz-Implementierung der Network Time Foundation (www.ntp.org). Wenn möglich, sollten Sie Ihren NTP-Server auf Version 4.2.7p26 oder höher aktualisieren, in der das *monlist* Kommando nicht mehr vorhanden ist. Einige Betriebssystem-Distributionen haben den betreffenden Bug [NTP 1532] auch in älteren Versionen des NTP-Servers gefixed.

Hinweise für die Konfiguration auf verschiedenen Plattformen bietet [TeamCymru]. Informationen zum Test der eigenen Gefährdung für derartige Angriffe sind bei [ONTPP] verfügbar.

Simple Network Management Protocol (SNMP)

SNMP ist ein Protokoll zum Verwalten von Geräten in Netzen (Router, Switches, Drucker, etc.).

Die Verwendung von SNMPv3 bietet eine Authentifizierung, mit der sich Reflection Angriffe vermeiden lassen. In den Vorgängerversionen war eine Authentifizierung nur bedingt über community strings möglich. Auch bei SNMP sollte der Zugriff auf die nötigen IPs und Funktionen eingeschränkt werden.

Character Generator Protocol (CHARGEN)

CHARGEN wird typischerweise zum Testen und Optimieren von Netzwerkverbindungen genutzt. Sobald das Protokoll nicht mehr benötigt wird, sollte der entsprechende Dienst deaktiviert werden.

Alternativ lässt sich CHARGEN auch über TCP nutzen. Sofern eine Verwendung von UDP notwendig ist, sollte der Zugriff mittels Paketfilterregeln eingeschränkt werden (UDP Port 19).

Domain Name System (DNS)

Für Hinweise zur sicheren Konfiguration von DNS-Servern siehe [CSE-042] und [CSE-055].

Literatur

[CSE-002] Abwehr von DDoS-Angriffen v1.0, BSI, 03.02.2012,
www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/sofortmassnahmen/BSI-CS_002.pdf

[CSE-042] Zunahme von DDoS-Angriffen durch DNS-Reflection v1.0, BSI, 15.10.2012
www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/angriffsmethoden/statistiken/BSI-CS_042.pdf

[CSE-055] Sichere Bereitstellung von DNS-Diensten v1.0, BSI, 02.04.2013
www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-055.pdf

[NTP 1532] http://bugs.ntp.org/show_bug.cgi?id=1532

[ONTPP] http://openntpproject.org/

[RFC 4330] http://tools.ietf.org/html/rfc4330#page-10

[TeamCymru] Secure NTP Template, TeamCymru,
www.team-cymru.org/ReadingRoom/Templates/secure-ntp-template.html

Diese BSI-Empfehlung ist unter Mitwirkung der als Partner der Allianz für Cyber-Sicherheit registrierten Internet-Service-Provider 1&1 Internet AG, Deutsche Telekom, Vodafone und Strato AG entstanden.