IP-Spoofing: Wenn Angreifer ihre IP verschleiern

Datum: 15.04.2019 | Internet, Sicherheit

Die Digitalisierung hat auch Ihre Schattenseiten. Mit der zunehmenden Vernetzung versuchen immer mehr Cyberkriminelle, sich Zugriff auf Ihre sensiblen Daten zu verschaffen oder Ihr System durch einen Angriff zu schädigen. **Dabei nutzen die Hacker verschiedene Methoden, mit denen sie Ihre Identität verbergen**. **Eine davon ist das sogenannte IP-Spoofing**, das eine systembedingte Schwäche des TCP/IP-Protokolls ausnutzt. **In diesem Beitrag erklären wir Ihnen, wie IP-Spoofing genau funktioniert** und wie Sie sich am besten vor derartigen Angriffen schützen können.

- ✔ Mit Hilfe von IP-Spoofing können Hacker komplette Rechnernetze lahmlegen oder IP-basierte Authentifizierungen einfach umgehen.
- ✔ IP-Spoofing in seiner ursprünglichen Form war bereits in den Achtzigern ein Thema in Expertenkreisen.
- ✔ Durch die verbesserten Sicherheitseigenschaften von IPv6 werden Spoofing-Angriffe deutlich erschwert.

Inhalt [Ausblenden]

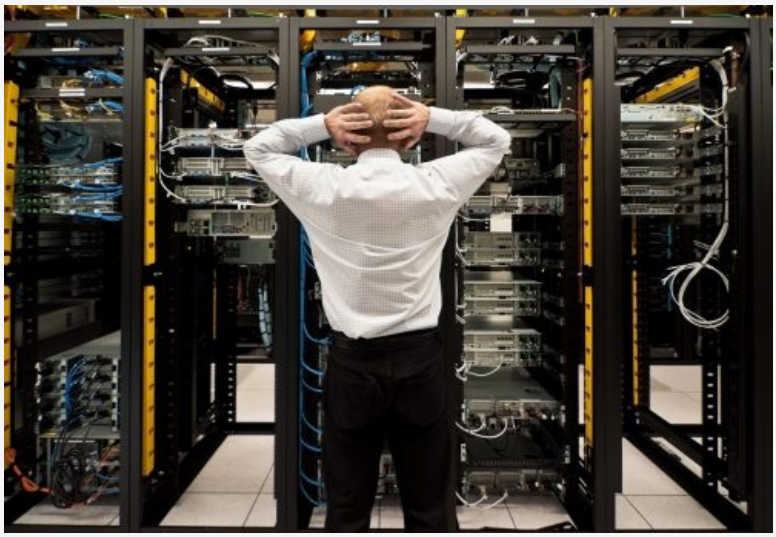
1. Was ist IP-Spoofing und wo wird es eingesetzt?

Beim IP-Spoofing (engl. für „Verschleierung“) nutzen Hacker **systembedingte Schwächen der TCP/IP-Protokollfamilie** aus, um die eigene IP zu verschleiern und Datenpakete von einer gefälschten Adresse zu versenden oder sichin fremde Computersysteme einzuschleusen. **Dazu gaukeln sie dem Empfänger vor, dass die Daten von einer vertrauenswürdigen Quelle stammen.**

Grundsätzlich wird zwischen zwei Arten von IP-Spoofing unterschieden:

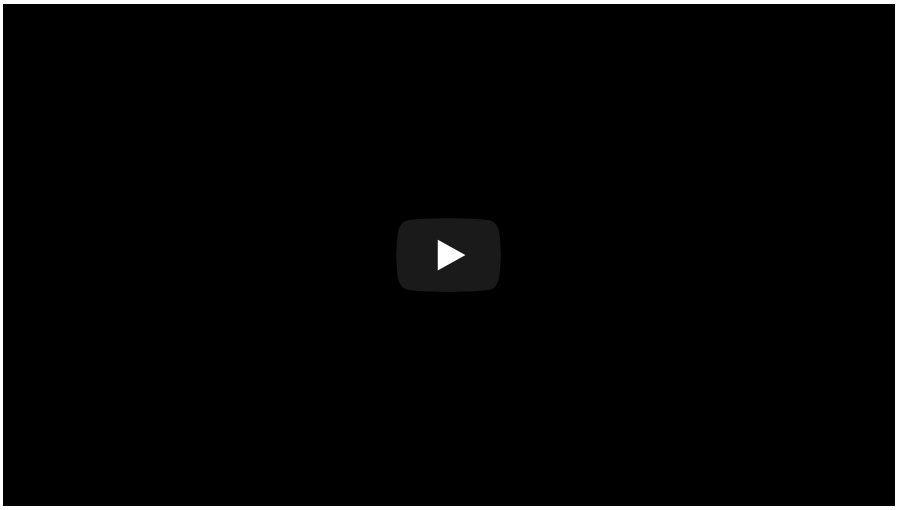
- **Beim Non-Blind-Spoofing befindet sich der Angreifer im selben Subnetz wie das Opfer** und nutzt die entwendete IP-Adresse, um den Datenverkehr zwischen zwei oder mehreren Rechner abzufangen oder zu manipulieren („Man-in-the-Middle“-Angriffe).
- Im Gegensatz dazu befindet sich der **Angreifer beim „Blind-Spoofing“ außerhalb des Subnetzes**. Von dort schickt er Datenpakete an das Opfer, um anschließend aus den Empfangsbestätigungen Rückschlüsse auf die Sequenznummern ziehen zu können.

Im Rahmen von Dos- und DDoS-Attacken kommt zudem **immer häufiger auch das sogenannte SYN-Flooding zum Einsatz**. Dabei werden mit Hilfe von „unterschlagenen“ ACK-Nachrichten absichtlich Dienstblockaden ausgelöst**,** die dann in Folge zu einer **Überlastung von einzelnen Komponenten einer IT-Infrastruktur** führen**.**

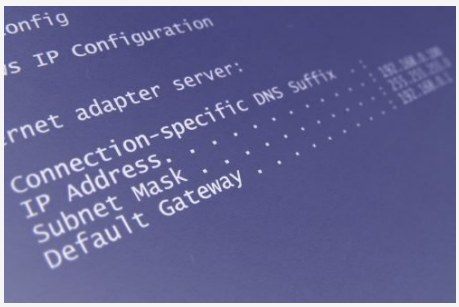


Die durch IP-Spoofing ausgelösten Dienstblockaden führen zur Überlastung einzelner Infrastruktur-Komponenten und können im schlimmsten Fall sogar das komplette Rechenzentrum lahmlegen.

Gut zu wissen: Die IP-Adresse lässt sich zwar auch über einen Proxy-Server maskieren, dieser leitet die Pakete aber lediglich weiter. Dadurch können Hacker auch bei verschleierten Adressen immer noch anhand der Log-Dateien des Proxy-Servers identifiziert werden.



2. Wie wird das Fälschen der IP-Adresse technisch umgesetzt?



Der Spoofer verändert zwar den Adresseintrag des IP-Paketes, die eigentliche IP-Adresse bleibt jedoch erhalten.

Jedes IP-Paket enthält in seinem Header eine Quell- und eine Zieladresse, für die es heutzutage noch keinen ausreichenden Schutz vor Manipulationen gibt. Das bedeutet, dass sie **weder verschlüsselt noch auf Ihre Korrektheit hin überprüft** werden. Der Empfänger muss also im Prinzip blind darauf vertrauen, dass die Pakete auch wirklich von der angegeben Adresse stammen.

Mit einem einfachen Spoofing-Angriff erhält ein Hacker per se noch keinen Zugriff auf den Datenverkehr. Er kann damit nur den Adresseintrag des jeweiligen Paketes ändern, wohingegen die eigentliche IP-Adresse bestehen bleibt. Die Antwort auf die ausgesendeten Daten gelangt daher auch nicht direkt zum Angreifer, sondern wird an den Rechner mit der zweckentfremdeten IP-Adresse übermittelt.

Die TCP-Pakete ihrerseits sind allesamt mit einer eindeutigen Sequenznummer gekennzeichnet, die verwendet wird, um eine

vollständige und duplikatfreie Übertragung zu garantieren. Hat sich der Hacker allerdings erst einmal unter falscher Identität in den Kommunikationsweg eingeklinkt („Session Hijacking“), kann er **relativ einfach die kommenden Sequenznummern voraussagen** und damit im Hintergrund agieren, wie es ihm beliebt.

Hinzu kommt, dass sich die Teilnehmer nur bei Beginn der Kommunikation gegenseitig authentifizieren. Nach dem Aufbau der Verbindung wird automatisch davon ausgegangen, dass die Parameter der Gegenseite sich nicht mehr ändern.

> **Gut zu wissen:** Die Computer, deren IP-Adresse übernommen wird, können selbst das Ziel einer Attacke sein oder aber im Verbund als Instrument für einen Angriff benutzt werden. Der Hacker selbst bleibt in beiden Fällen unbekannt.

3. Wie kann ich mich gegen IP-Spoofing schützen?

Das Verschleiern der IP funktioniert von jedem beliebigen Ort aus, der angegriffenen Rechner muss dafür lediglich über eine Verbindung zum Internet verfügen. Aus diesem Grund **zielen die meisten Gegenmaßnahmen vor allen auf Sicherheitskonfigurationen, Berechtigungen und Zugriffskontrollen ab**.

Dos- oder DDos-Attacken mittels IP-Spoofing sind erschreckend einfach, darum beschäftigen sich Sicherheitsexperten und IT-Spezialisten schon seit Jahrzehnten damit.

Das Problem beschäftigt Computer-Spezialisten und Sicherheitsbeauftragte schon seit einigen Jahrzehnten. Schon alleine die Tatsache, dass sich DoS- und DDoS-Angriffe mit einer derartigen Leichtigkeit durchführen lassen, macht **IP-Spoofing zu einer der beliebtesten kriminellen Methoden überhaupt** im Internet. In der Vergangenheit gab es deshalb schon häufiger Forderungen in Richtung der Internet-Provider, den Datenverkehr gezielt zu filtern und die entsprechenden Pakete samt Quelladressen außerhalb des Netzwerkes zu erfassen und anschließend zu verwerfen.

Was sich so einfach anhört, ist neben einem erheblichen Aufwand auch eine Kostenfrage. Aus diesen Gründen wollte sich auch bislang niemand wirklich mit der Realisierung befassen.

3.1. IPv6 macht Spoofern den Garaus

Aktivieren Sie die Paket-Filterung auf Ihrem Netzwerk-Router, um Adressen von außerhalb den Zugriff zu verweigern.

Das überarbeitete IPv6-Protokoll bietet verbesserte Sicherheitseigenschaften im Vergleich zum Vorgänger IPv4. Dazu gehören beispielsweise neue (optionale) Verschlüsselungstechniken und Authentifizierungsverfahren, durch die **IP-Spoofing in naher Zukunft gänzlich aussterben** wird. Zum aktuellen Zeitpunkt unterstützen allerdings noch nicht alle gängigen Netzwerkgeräte das neue Protokoll. **Außerdem wird der Umstieg wohl noch einige Zeit in Anspruch nehmen**.

Das bedeutet natürlich nicht, dass Sie den Verschleierungs-Angriffen einfach hilflos ausgeliefert sind. Um IP-Spoofing-Angriffe abzuwehren, können Sie auch selbst tätig werden und **entsprechende Schutzmaßnahmen einrichten**:

- Eine mögliche Gegenmaßnahme gegen IP-Spoofing sind **Paketfilter auf Ihrem Router oder dem Gateway**. Dadurch werden die eingehenden Pakete analysiert und all diejenigen verworfen, die die Quelladresse eines Rechners von innerhalb des Netzwerks besitzen.

Auf diese Weise können Hacker die Adresse eines internen Computers nicht von außen fälschen. Aus dem selben Grund sollten Sie **auch die Adressen der ausgehenden Pakete filtern** und all diejenigen verwerfen, deren Quelladresse nicht innerhalb des Netzwerkes liegt.

- **Verzichten Sie grundsätzlich auf hostbasierte Authentifizierungsverfahren und führen Sie alle Log-In-Methoden über verschlüsselte Verbindungen durch**. Dadurch verhindern Sie nicht nur Angriffe durch Spoofing, sondern erhöhen zugleich auch die Sicherheitsstandards innerhalb des Netzwerkes.
- **Tauschen Sie möglichst alle alten Betriebssysteme, Programme und Netzwerkgeräte aus**, denn diese entsprechen meist nicht mehr den aktuellen Sicherheitsstandards. Zudem besitzen sie neben Ihrer Anfälligkeit für IP-Spoofing **häufig auch noch zahlreiche andere Sicherheitslücken**, die sich Cyberkriminelle zu nutzen machen könnten.

Entsorgen alte Hardware und tauschen Sie Betriebssystem und Programme gegen neuere Versionen aus, um die Anfälligkeit Ihres Netzwerkes gegen IP-Spoofing zu reduzieren.

Gut zu wissen: Die meisten aktuellen Firewalls besitzen bereits ein integriertes Anti-Spoofing-Tool, das die TCP-Sequenznummern zufallsgeneriert. Auf diese Weise wird die Voraussage der kommenden Nummern deutlich erschwert.

Ähnliche Artikel:

- Mail-Spoofing: Betrügerische Mails erkennen und abwehren
- Inkognito surfen – Wie anonym sind Sie tatsächlich?
- Avast Test 2019: Wie schlägt sich die Internet…
- PGP-Verschlüsselung: Funktionsweise und Sicherheit
- Sicherheit im Heimnetzwerk – so schützen Sie Ihren…
- Gefahr durch Cryptojacking: So können Sie sich vor…