Wie funktioniert der Türsteher?

Filesharing ist für alle Netzwerkadministratoren wegen seiner Tendenz zur Bandbreitenvernichtung und der ausgelösten juristischen Auseinandersetzungen schon immer eine Plage gewesen.
Dennoch ist die Identifikation von filesharing-Verbindungen und Nutzern von filesharing bis heute eines der schwierigsten Themen in der Netzwerkadministration, zumal die Entwickler von filesharing-Software - häufig aus redlichen und nachvollziehbaren, oft politischen Gründen – auf jeden Ansatzpunkt ihrer Gegner mit neuen anspruchsvolleren Techniken, die in der Regel Kompetenz und technische Möglichkeiten der anderen Seite überfordern, reagieren.
Filesharing-Verbindungen können inzwischen ohne Fachwissen der Nutzer anonymisiert, verschlüsselt und als andere Aktivität – wie Internettelefonie oder normales „Surfen“ - getarnt werden.
Andererseits ist aber jeder, der seinen Internetanschluss anderen zur Verfügung stellt, gezwungen, solche Aktivitäten zu kontrollieren, um nicht selbst wegen Urheberrechtsverletzung oder schlimmer, Verbreitung verbotener Inhalte, haftbar gemacht zu werden.

Techniken zur Identifikation von filesharing
(es ist schon auffällig, wie wenige es gibt)

1) **Portsperren**
   Traditionell benutzten filesharing-Programme bestimmte Ports. Diese wurden deshalb in der Firewall gesperrt. Ein solches Vorgehen ist aber inzwischen kontraproduktiv, da alle aktuellen Programme auf jedem Port kommunizieren können und häufig sogar Sperren entdecken und selbsttätig umgehen.
2) **DPI (Deep-Packed-Inspection) und IPP2P (IPTables-Regeln für Peer-to-Peer)/OpenDPI**
   Hierbei handelt es sich um die kommerzielle und die „freie“ Version der gleichen Technik, entwickelt von der Leipziger Firma Ipoque (www.ipoque.com).
   Der **Inhalt von Datenpaketen** wird nach charakteristischen Strings – überwiegend Befehlssequenzen des P2P-Netzes durchsucht, was hohe Rechenleistung erfordert. Schwierigkeiten bis zum völligen Versagen bestehen lt. Tests bei verschlüsselten und getarnten Übertragungen. Ipoque kombiniert diese Technik in seinen überwiegend für DSL-Provider konzipierten Geräten deshalb offenbar mit einer DDTA ähnlichen Analyse. Die Erkennungsquote liegt laut Firmenangabe bei >90%.
   Da der **Inhalt** von Datenpaketen analysiert wird, ist diese Technik politisch und rechtlich umstritten.
3) **Layer 7- Analyse**
   Filesharing verwendet überwiegend proprietäre Protokolle. Die Methode des L7-Filter-Projekts (http://l7-filter.sourceforge.net) analysiert die Header (also den technisch für die Übermittlung notwendigen Teil) der ersten Pakete einer Verbindung auf dem Application-Layer (nach dem OSI-Schichtenmodell) und erkennt zuverlässig die wichtigsten Protokolle. Sie ist weniger rechenintensiv als DPI, scheitert aber manchen UDP-V erbindungen und kann gerade wegen der richtigen Erkennung des Protokolls getarntes Firlesharing nicht identifizieren.

4) **DDTA (Dynamische Daten-Transfer-Analyse)**
DDTA entstand bei uns als „Abfallprodukt“ der QOS-Entwicklung. QOS, Quality-of-Service ist eine Technik, um bei begrenzter Bandbreite des Außenanschlusses, eine optimale Nutzung und Befriedigung aller gestellten Anforderungen zu ermöglichen. Jeder Dienst (z.B. Surfen oder Internettelefonie) hat sein ganz eigenes Anforderungs-Profil für eine einwandfreie Funktion. Die Voraussetzung um einen Dienst zu optimieren, ist selbstverständlich, dass man erkennt, um welchen Dienst es sich bei einer Verbindung überhaupt handelt.
DDTA ermittelt die Charakteristika von Sender und Empfänger, sowie den Verlauf der Datenübertragung über eine (kurze) Zeitspanne überwiegend aus Informationen, die der Linux Kernel ohnehin zum Betrieb dieser Verbindung besitzt. Daher wird wenig Rechenzeit benötigt. Das sich aus diesen Informationen ergebende Verbindungsprofil lässt einen sicheren Schluss auf die Art des Dienstes zu. Verschlüsselung und Tarnung bilden kein Problem, erleichtern eher die Identifikation.
„Störende“ - das Netzwerk beeinträchtigende - Nutzer, zu denen Filesharer gehören, werden verlässlich identifiziert. Die Schwellenwerte sind skalierbar. Bei niedrigschwelliger Einstellung besteht lediglich die Gefahr, dass „Störer“ in die falsche Störer-Kategorie eingeordnet werden (z.B. ein intensivst genutzter Tunnel fälschlich als Filesharer klassifiziert wird). Dies ist aber unerheblich, da auch hier eine Reaktion des Netzwerkes notwendig wird, um andere Nutzer nicht zu beeinträchtigen.

Arbeitsweise des Türstehers

Wir verwenden einen gestaffelten Erkennungsalgorithmus: L7-Filter wird zur Vorerkennung und wenn nötig (bei „scharfer“ Einstellung) zur Vermeidung von Fehlklassifikationen eingesetzt. DDTA erledigt den Hauptteil der Analyse.
Ist eine Störer-Identifikation erfolgt, kann nach Kundenvorgabe eine Verbindungs- oder Nutzer-bezogene Reaktion des Türstehers ausgelöst werden. Dies geschieht mittels entsprechender Einträge in seine Netfilter-Firewall. Üblich ist die Kappung der entsprechenden Verbindung, gefolgt mit einer Anzeige im Browser, die den Benutzer über sein Fehlverhalten informiert und die anschließende Beschränkung auf sichere Dienste (er kann weiter Internet-Seiten aufrufen, Emails empfangen und versenden usw.).
Dies alles erfolgt automatisch und wird protokolliert.
Als Nebeneffekte optimiert der Türsteher auch ihren DSL-Anschluss, bietet mit der Netfilter-Firewall einen professionellen Schutz Ihres Netzes nach außen und kann bei Bedarf sogar Virenaktivität in Ihrem Netz ermitteln.

Technik des Türstehers

Der Türsteher ist ein Linux-basierter Netfilter-NAT-Firewall Router. Diese weltweit bewährte Technik wird ergänzt durch unser QOS-Software-Paket plus Filesharing-Modul. Im Interesse von Servicefreundlichkeit und Betriebssicherheit werden nur bewährte Standardbaugruppen von Markenherstellern verwendet. Durch Gehäuse in Formfaktorvarianten passt er sich jeder Umgebung an.

Vorteile des Türstehers

Zuverlässig – Der Türsteher unterbindet sicher Urheberrechtsverletzungen und die Verbreitung verbotener Inhalte.
Leistungsstark – Er ist speziell für DSL-Anbindungen konzipiert, verhindert Störungen und optimiert die Anschluss-Leistung.
Kostengünstig – Wir verzichten darauf, den Türsteher in spezielle Gehäuse zu verpacken. Sie können daher sogar selbst die gesamte Hardware bei Ihrem oder einem von uns empfohlenen Lieferanten einkaufen. Dadurch liegen die Gesamtkosten unter einem professionellen Kleinrouter ohne Türsteher-Funktionalität.
Dokumentenecht – Der Türsteher protokolliert seine Aktivitäten bis zum maximal zulässigen Zeitraum von 6 Monaten, auf Wunsch können auch alle Verbindungsaufbauten – entsprechend der aktuellen Gesetzeslage - dokumentiert werden. Sie können die Protokolle Online einsehen oder sich per Email zuschicken lassen.
Pflegeleicht – Sie müssen nichts konfigurieren oder warten, darum kümmern wir uns.
Aktuell – Verbesserungen und Aktualisierungen werden von uns kostenlos über das Fernwartungsmodul zur Verfügung gestellt.

Was der Türsteher nicht kann

Der Türsteher kann Sie nicht völlig vor **unbegründeten** Abmahnungen schützen. Aus Ihrem Netz ist keine Urheberrechtsverletzung möglich. Es ist jedoch denkbar, dass ein Nutzer eine Verbindung zu einem Filesharing-Netzwerk aufbaut und seinen Willen zur Teilnahme bekundet bevor der Türsteher zuschlägt. (Schließlich kann man nur eine bestehende Verbindung analysieren.) Wenn ein „Ermittler“ aus Gewinninteresse nur die für diesen kurzen Zeitraum sichtbare IP Ihres Anschlusses protokolliert, ohne weitere Daten zu erheben oder sich auf Fehlinformationen des Filesharing-Netzes bezieht (siehe www.freise.it/p2p2.pdf), kann es zu einer fälschlichen Abmahnung kommen.
Dagegen können Sie aber vorgehen, denn die Reaktion des Türstehers wird protokolliert.
Außerdem sinkt die Wahrscheinlichkeit einer unbegründeten Abmahnung drastisch: Wer weiß, dass aus Ihrem Netz kein Filesharing möglich ist, wird es auch nicht mehr versuchen.