

## Schützen des Systems gegen ARP-Angriffe (Address Resolution Protocol)

### Agnitum TechNote

In diesem Dokument werden Angriffsmöglichkeiten innerhalb von LANs beschrieben und der erweiterte Schutz durch die neuen Funktionen von Outpost Firewall Pro V3.0 gegen Angriffe innerhalb des Netzwerks erläutert.

### Beschreibung des Problems

Informationen im Netzwerk werden in Datenpaketen gesendet. Jedes Paket weist einen Absender und einen Empfänger auf und muss an eine bestimmte Hardwareadresse gesendet werden, die auch als MAC-Adresse (Medium Access Control) bezeichnet wird. Die MAC-Adresse ist durch das Netzwerkgerät für jeden Knoten in einem Netzwerk festgelegt, und der Datenverkehr wird entsprechend dieser eindeutigen Hardwareadresse an Geräte gerichtet.

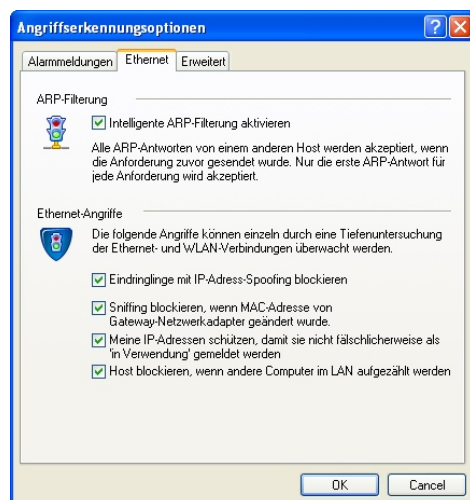
Die innerhalb von Netzwerken zum Senden von Daten verwendeten 32 Bit umfassenden IP-Adressen werden mithilfe eines Prozesses, der als ARP (Address Resolution Protocol, Adressauflösungsprotokoll) bezeichnet wird, in die 48 Bit langen MAC-Adressen für die Netzwerkhardware umgewandelt. Wenn Daten im Netzwerk von einem Computer an einen anderen gesendet werden, übermittelt der sendende Computer eine ARP-Anforderung, um die MAC-Adresse entsprechend der IP-Adresse des Zielcomputers zu ermitteln, und wartet dann auf den Empfang der Ethernet-Adresse des Zielcomputers. Im Zeitraum zwischen der Paketübertragung und der Ethernet-Adressantwort können die Daten manipuliert, abgefangen oder an eine nicht autorisierte dritte Person weitergeleitet werden.

### Lösung des Problems durch Outpost

Für einen zuverlässigen Schutz gegen Angriffe über ARP muss eine Firewall dem Angreifer auf der Ebene des ARP-Protokolls begegnen, indem nicht nur Port-Scans, sondern auch Netzwerk-Scans über ARP-Anforderungen erkannt und blockiert werden. Sie sollte außerdem auch in der Lage sein, andere Ethernet-spezifische Angriffe zu erkennen und zu verhindern.

Das verbesserte Plug-In für Angriffserkennung von Outpost Firewall Pro 3.0 erkennt und verhindert jetzt spezielle Ethernet-Angriffe wie IP-Spoofing, ARP-Scans und ARP-Flächenangriffe durch Untersuchen des Datenverkehrs über Ethernet und WLAN auf ARP-Ebene. Zudem werden ARP-Antworten blockiert, wenn keine entsprechende Anforderung vom System vorlag.

Das Plug-In für Angriffserkennung bietet die folgenden Funktionen:



### Intelligente ARP-Filterung

Die intelligente ARP-Filterung ist eine effektive Maßnahme zum Schutz der Anwender gegen gefälschte Anforderungen zum Auslösen von Kommunikation. Sie schirmt außerdem drahtlose Netzwerke gegen nicht legitime Verbindungen ab.

Angenommen, ein Knoten im Netzwerk sendet eine große Anzahl von ARP-Antworten mit verschiedenen MAC-Adressen über einen kurzen Zeitraum. Auf diese Weise besteht die Möglichkeit, dass die Netzwerkgeräte überlastet werden und nicht mehr eindeutig erkennen können, welche MAC-Adresse wirklich zu dem Knoten gehört.

Durch die ARP-Filterung wird sichergestellt, dass ARP-Antworten verworfen werden, wenn zuvor keine entsprechende Anforderung gesendet wurde. Bei aktivierter ARP-Filterung wird für jede Anforderung nur die erste ARP-Antwort akzeptiert.

Systeme, die nicht durch die ARP-Filterung geschützt sind, können auch so genannten ARP-Cache-Beeinträchtigungen unterliegen. Dabei fängt eine Person Ethernet-Datenverkehr über gefälschte ARP-Antworten ab, um die Adresse der Netzwerkkarte in eine Adresse zu ändern, die sie überwachen kann. Wenn die ARP-Filterung nicht aktiviert ist, können ARP-Flächenangriffe – eine Methode, bei der eine große Anzahl von gefälschten ARP-Antworten an den Zielcomputer gesendet werden – außerdem zum Einfrieren des Systems führen.

### Verhindern von IP-Spoofing

Beim IP-Spoofing handelt es sich um einen Versuch, das Netzwerk durch überflüssige Daten zu überlasten und beim Empfängercomputer ein Aussetzen der Netzwerkdienste (Denial of Service, DoS) hervorzurufen. Das Plug-In für Angriffserkennung von Outpost erkennt eine sehr große Anzahl von IP-Paketen von einem einzelnen Computer in einem bestimmten Zeitraum, die an Computer im Netzwerk gerichtet sind, und blockiert diese Kommunikation, um eine Überlastung des Netzwerks zu verhindern.

### Sniffer-Blockierung

Hacker können durch das Fälschen von ARP-Antworten legitime MAC-Adressen durch eigene ersetzen, sodass legitimer Datenverkehr an einen vom Hacker kontrollierten Computer umgeleitet wird. Dadurch können Sie Pakete lesen („Sniffing“) und die übertragenen Daten einsehen. Mit diesem ARP-Spoofing kann Datenverkehr auch an nicht existierende Hardware gerichtet werden. Dies führt auf dem betroffenen Gerät zu Verzögerungen bei der Datenübertragung oder zu Denial of Service.

Spezielle Sniffing-Programme von Hackern können Datenverkehr auch durch Änderungen der MAC-Adresse am Internet-Gateway abfangen, darunter Chatsitzungen und damit zusammenhängende private Daten wie Kennworteingaben, Namen, Adressen und selbst verschlüsselte Dateien.

Um dieses Abfangen von Datenverkehr zu verhindern und einen Schutz gegen Sniffer-Angriffe zu bieten, überprüft das Plug-In für Angriffserkennung von Outpost, ob die MAC-Adresse mit der Quell-IP-Adresse im ARP-Paket übereinstimmt. Somit wird sichergestellt, dass keine nicht autorisierten Änderungen des Gateway-Netzwerkadapters stattgefunden haben.

### Verhindern von IP-Adressenkonflikten

Ein Angreifer kann einen Computer durch gefälschte ARP-Antworten daran hindern, auf das Netzwerk zuzugreifen. Dabei werden alle IP-Adressen in einem Netzwerk dupliziert und IP-Adresskonflikte erzeugt. Das Plug-In für Angriffserkennung von Outpost blockiert gefälschte ARP-Antworten, die dieselbe IP-Adresse wie der Adapter aufweisen, jedoch eine abweichende MAC-Adresse. Dadurch wird sichergestellt, dass IP-Adresskonflikte vermieden werden und der Computer selbst dann korrekt gestartet werden kann, wenn die IP-Adresse fälschlicherweise als in Benutzung gemeldet wurde.



### Blockieren von Netzwerk-Scans

Einige Viren mit aggressiver Verbreitung infizieren Computer über Massen-Hostaufzählungen, bei denen sie von Computer zu Computer gelangen. Diese Methode wird auch von Scannern und Schwachstellenanalyse-Programmen genutzt. Das Plug-In für Angriffserkennung von Outpost schützt das lokale Netzwerk des Anwenders, indem die Anzahl von ARP-Anforderungen zum Aufzählen von IP-Adressen von einer MAC-Adresse in einem vorgegebenen Zeitraum begrenzt wird und ARP-Netzwerk-Scans verhindert werden.

## Zusammenfassung

Schutz gegen Datendiebstahl und intern generierte Angriffe ist für Anwender in kleinen Unternehmens- und Heimnetzwerken von zunehmender Bedeutung. Dabei spielt es keine Rolle, ob das Netzwerk über Kabel verbunden ist oder es sich um ein drahtloses Netzwerk handelt. Wenn Computer miteinander verbunden sind und Daten austauschen, besteht eine ernstzunehmende Gefahr des Abfangens oder Manipulierens von Daten während der Übertragung und daraus folgenden Offenlegungen von vertraulichen Daten oder Unterbrechungen von Netzwerkdiensten.

Die erweiterten Angriffserkennungs- und Antispoofing-Technologien von Outpost Firewall Pro 3.0 verhindern, dass der Computer übernommen und gegen das eigene Netzwerk eingesetzt wird. Ihre Computer werden vorausschauend gegen kurzfristige Angriffe verteidigt und gegen Schwachstellen von Windows-Betriebssystemen bis zur Veröffentlichung von Patches durch Microsoft geschützt.

Mit dem Schutz durch Outpost auf Ihrem System müssen Sie nicht länger befürchten, dass Ihre Daten über das Netzwerk oder das Internet gestohlen werden. Denken Sie auch daran, Outpost mit sich zu führen, wenn Sie ein Internetcafé mit WLAN-Hotspot besuchen!