Sicherheitslücke DHCP:

6 Tipps für Ihr sicheres Netzwerk mit DHCP

Sicherlich funktioniert das **D**ynamic **H**ost **C**onfiguration **P**rotocol (DHCP) in Ihrem Netzwerk problemlos, schließlich ist es in wenigen Sekunden auf einem Windows-Server eingerichtet und im Betrieb wartungsfrei.

Doch in puncto Sicherheit vernachlässigen die meisten Administratoren den Einsatz von **DHCP.** Im schlimmsten Fall kann so Ihr ganzes Netzwerk von einem einzigen Client lahm gelegt werden.

Welche konkreten Angriffsmöglichkeiten bestehen und wie Sie sich davor schützen, lesen Sie in diesem Artikel.

Risikoanalyse: Kenne deinen Feind

Eine **DHCP-Verbindung** zwischen Client und Server folgt einem einfachen Prinzip: Der Client sendet ein UDP-Paket auf Port 67 als Broadcast-Anfrage mit seiner MAC-Adresse in das Netzwerk **(DHCPDISCOVER).**

Alle Rechner im Netzwerk empfangen diese Nachricht. Ihr **DHCP-Server** erkennt die Anfrage und sendet ein Angebot an den Client mit einer IP-Adresse und den übrigen TCP/IP-Einstellungen **(DHCPOFFER).**

Daraufhin sendet der Client für das erhaltene Angebot die konkrete Anfrage an den Server **(DHCPREQUEST),** der Server bestätigt diese **(DHCPPACK)** und markiert die IP-Adresse im Zusammenhang mit der MAC-Adresse des Clients als vergeben.

Die Funktionsweise von **DHCP** hat prinzipielle Schwächen, die sich auf die mangelnde Authentifizierung und Autorisierung von Server und Client zurückführen lassen. Schließlich wird an keiner Stelle der Kommunikation zwischen Client und Server die Echtheit des Kommunikationspartners geprüft. In Tabelle 1 (Seite 6) finden Sie mögliche Gefahren.

Wie Sie den Einsatz von **DHCP** in Ihrem Netzwerk effektiv sichern, zeigen wir Ihnen in den folgenden sechs Tipps.

Tipp 1: Verwenden Sie fixe IP-Adressen für Server und Gateways

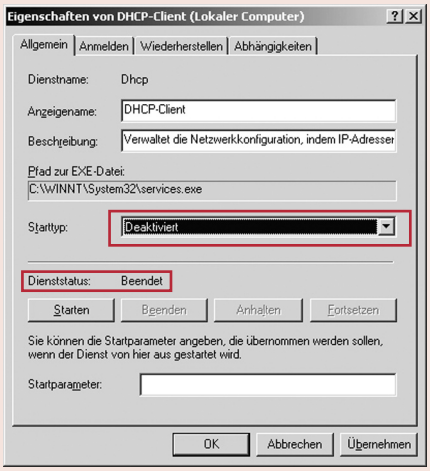
Server, Gateways und andere wichtige Netzwerkkomponenten (Print-Server) sollten Sie mit festen TCP/IP-Einstellungen ausstatten. Nur so sind diese kritischen Systeme gänzlich vor gefälschten **DHCP-Servern** geschützt.

Beachten Sie: Einige Administratoren neigen dazu, die MAC-Adressen ihrer Gateways im **DHCP-Server** zu hinterlegen und einer festen IP-Adresse im IP-Pool zuzuordnen. Bei Servern und Gateways raten wir ausdrücklich von dieser Methode ab, denn die Systeme können weiterhin Opfer von gefälschten **DHCP-Servern** werden.

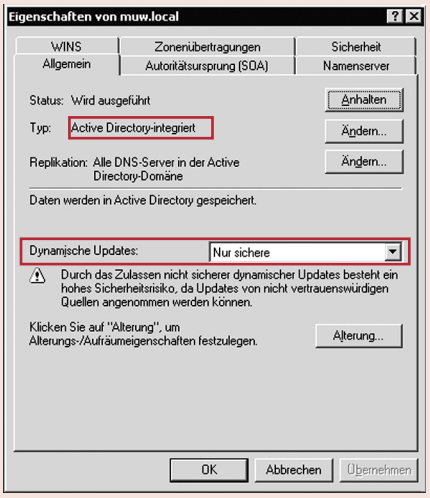
Tipp 2: Beenden Sie den DHCP-Client auf Systemen mit fester IP-Adresse

Auf Systemen mit fester IP-Adresse beenden Sie am besten den Dienst **„DHCP-Client".** Windows kann so keine dynamischen TCP/IP-Einstellungen von einem **DHCP-Server** beziehen.

Tipp der Redaktion: Unter **Windows 2000** und **XP** deaktivieren Sie den **DHCP-Dienst** wie folgt: Klicken Sie in der Systemsteuerung auf **„Verwaltung" -> „Dienste",** wählen Sie hier nun **„DHCP-Client".** Als Starttyp wählen Sie **„Deaktiviert"** bzw. **„Manuell".**



1 DHCP-Dienst deaktivieren: Auf Systemen mit fester IP-Adresse deaktivieren Sie unbedingt den **DHCP-Dienst.** Als Starttyp wählen Sie hierzu **„Deaktiviert".**



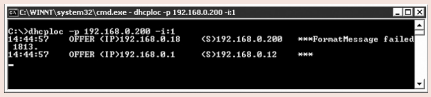
2 Sichere DNS-Updates auf dem Windows-Server: Nur wenn für Ihre lokale Zone die Option **„Nur sichere"** aktiviert ist, können Angreifer Ihren **DNS-Server** nicht über den **DHCP-Dienst** manipulieren.

Tipp 3: Platzieren Sie den DHCP-Server auf einem Member-Server im LAN

Die Windows-Server-Version bringt von Haus aus einen **DHCP-Server** mit sich. Setzen Sie mehrere Windows-Server in Ihrem Netzwerk ein, positionieren Sie den **DHCP-Server** möglichst nicht auf dem Domänen-Controller.

Denn wird der **DHCP-Dienst** auf einem Member-Server geknackt,

3 **Überwachung lebensnotwendig:** Aktivieren Sie auf Ihrem **DHCP-Server** unbedingt die Überwachungsrichtlinie. Sie finden so im Logfile schnell Adresskonflikte, die möglicherweise auf einen zweiten, illegal installierten **DHCP-Server** hindeuten.



4 **dhcploc:** Mit dem kostenlosen Tool **dhcploc** finden Sie **DHCP-Server** innerhalb eines IP-Subnetzes. Im Beispiel sehen Sie, dass neben dem **DHCP-Server** 192.168.0.200 auch die IP-Adresse 192.168.0.12 IP-Adressen verteilt. Ein klares Anzeichen für einen illegal installierten **DHCP-Server** („rogue dhcp-server") im LAN.

wird Ihr **A**ctive **D**irectory (AD) nicht unmittelbar beeinträchtigt.

Beachten Sie: Ein **DHCP-Server** gehört ins interne LAN und niemals auf einen Server, der von außen erreichbar ist.

Tipp 4: Erlauben Sie nur sichere DNS-Updates

Seit Windows 2000 Server unterstützt der **DHCP-Server-Dienst** sogenanntes **D**ynamic **DNS** (DDNS). Hierbei werden die Hostnamen der Clients mit dynamisch bezogenen IP-Adressen automatisch in den Name-Server eingetragen.

Prinzipiell empfehlen wir, die Name-Server-Einträge nicht als Datei, sondern im AD zu speichern. Dies ist standardmäßig auf einem Windows Server 2003 der Fall. Für Ihre DNS-Zone sollten Sie dann unbedingt **„Sichere Updates"** aktivieren. Diese Option finden Sie unter den Eigenschaften Ihrer Zone (z.B. muw.local) im Register **„Allgemein".**

Ein DNS-Eintrag erfolgt zukünftig nur dann, wenn der Rechner dazu berechtigt ist (z.B. Mitglied der Domäne). Clients mit gefälschten **DHCP-Anfragen** sind so nicht in der Lage, den Name-Server beliebig zu beschreiben.

Tipp 5: Beobachten Sie den DHCP-Server-Dienst

Um den Missbrauch Ihres **DHCP-Servers** durch gefälschte Clients frühzeitig zu erkennen, richten Sie ein Monitoring für den **DHCP-Server** ein. Öffnen Sie hierzu die **DHCP-Verwaltungskonsole** und klicken Sie mit der rechten Maustaste auf den **DHCP-Server.** Im Eigenschaften-Dialog aktivieren Sie im Register **„Allgemein"** die Option **„DHCP-Überwachungsprotokoll aktivieren".**

Tipp der Redaktion: In der Ereignisanzeige finden Sie unter **„System"** alle Logs des **DHCP-Servers.** Die Logdateien werden unter **„c:\winnt\system32\dhcp\"** in Textform gespeichert.

Tipp 6: Finden Sie unberechtigte DHCP-Server

DHCP-Server müssen in einem Active Directory zwar autorisiert werden, doch hindert dies keinen fremden **DHCP-Server** (z.B. unter **Linux),** seinen Dienst zu erledigen.

Haben Sie den Verdacht, dass gefälschte **DHCP-Server** im Netzwerk zum Einsatz kommen, verwenden Sie ein Sniffing-Tool wie **Ethereal** und suchen Sie nach UDP-Paketen mit dem Inhalt **„DHCPOFFER".** Alternativ bieten einige managebare Layer-3-Switche das Sperren von bestimmten **DHCP-Nachrichten** an den Client-Ports.

Tipp der Redaktion: Microsoft selbst stellt ein Konsolenprogramm namens **dhcploc** zur Verfügung (auf der Installations-CD im Ordner **„Support").** Hiermit lassen sich zumindest **DHCP-Server** im gleichen Subnet auffinden.

Ergebnis: Ultimative Sicherheit gibt es nicht

Sie sehen: Es gibt keine ultimative Sicherheitslösung für den Einsatz von **DHCP.** Wenn Sie aber regelmäßig die Logfiles Ihres Servers beobachten, Clients gegen unerlaubte Installationen sichern und ungenutzte Netzwerkdosen nicht patchen, haben Sie bereits mit wenig Aufwand viel Sicherheit erreicht.

Ansonsten wird die Zukunft sicherlich mehr Sicherheit bringen: Denn **IPv6** unterstützt standardmäßig die sichere Kommunikation zwischen zwei Hosts.

*** Artikel** unter www.mit-sicherheit.de
Geben Sie folgende ID ein: **MSVO**

Tabelle 1: Gefahren von DHCP

Gefälschter DHCP-Server: Netzwerk lahm legen	Prinzipiell kann jeder Client Ihres Netzwerks einen **DHCP-Server** starten und falsche TCP/IP-Informationen an Ihre Clients verteilen. Die Clients können dann nicht mehr mit dem Netzwerk kommunizieren.
Gefälschter DHCP-Server: Verbindungen ausspionieren	Mit einem gefälschten **DHCP-Server** können Angreifer auch gefälschte Adressinformationen für die Gateway-IP-Adresse verteilen. In Form einer Man-in-the-Middle-Attacke leiten sie Anfragen an das Internet zum richtigen Gateway weiter und spähen währenddessen die Verbindungen aus.
Unzulässige Client-Anforderungen: DoS-Angriff provozieren	Mit spezieller Software lesen Angreifer unter gefälschten MAC-Adressen (Spoofing) beliebig viele IP-Adressen von Ihrem **DHCP-Server.** Die Folge: Der IP-Scope ist ausgeschöpft und Clients erhalten keine weiteren IP-Adressen mehr.