

NetChekker

© 2010 Hans-Georg Joepgen (Redaktionsbuero@joepgen.com) / 29.08.2010

NetChekker ist ein Testprogramm zur Überprüfung von Computernetzen. Es dient der Fehlersuche an Hardware- und Softwarekomponenten in örtlichen Netzen und im Internet. Außerdem lässt sich NetChekker als Versuchswerkzeug bei der Einarbeitung in die Netztechnik und in der Ausbildung einsetzen.

Mit NetChekker testen Sie beispielsweise die Netzwerkelektronik eines Rechners, prüfen die Übermittlungswege im Heimnetz oder zu externen Servern irgendwo auf der Welt und untersuchen ihre Wirkungsweise. Außerdem ermöglicht NetChekker, die Einstellung von Routern, Firewalls, Browsern und E-Mail-Programmen zu kontrollieren und zu korrigieren. Die folgenden Seiten schildern die Arbeitsweise des Programms, erläutern die Einstellmöglichkeiten und bringen Anwendungsbeispiele.

Programm-Installation

NetChekker gehört zu einer modernen Art von Programmen, der *Portablen Software*. Solche Programme kommen ohne invasive Installation aus und sind auch von frisch angesteckten USB-Sticks aus sofort lauffähig. Statt der Registry benutzt Portable Software eine Datei im eigenen Arbeitsordner zur Zwischenspeicherung von Einstellungen. Deswegen beschränkt sich die im folgenden geschilderte Installation im Wesentlichen auf das Auspacken dreier Dateien und optional dem Erzeugen eines Desktop-Symbols und je eines Eintrags unter *Start* und *Programme*.

Wenn Ihnen die aktuelle Version bereits als Datei *NetChekkerPaket.exe* vorliegt, dann starten Sie zur Installation bitte diese Datei. Andernfalls suchen Sie die Webseite www.DatenBurg.com auf, klicken dort *NetChekker installieren* an, wählen *Ausführen* und beantworten eventuelle Sicherheitsanfragen.

Es meldet sich das NetChekker-Installationsprogramm und schlägt Ihnen einen Arbeitsordner für NetChekker vor. Möchten Sie dem Vorschlag nicht folgen, klicken Sie *Arbeitsordner wechseln* an. Beachten Sie, dass der Nutzer während der Installation und auch später während des Betriebes im vorgewählten Ordner über das Schreibrecht verfügen muss.

Befindet sich bereits eine Version von NetChekker in diesem Ordner, so brauchen Sie diese Fassung vor der Installation einer Neuversion nicht zu löschen.

Klicken Sie bitte auf *Installieren* und nach erfolgter Installation auf *Programm beenden*.

Auf dem Desktop erkennen Sie nun ein Symbol namens *NetChekker*. (mit Punkt als letztem Zeichen), über das Sie das Programm künftig starten können. Damit ist NetChekker zwar bereits einsatzbereit. Sie können sich jedoch zusätzliche Prüfmöglichkeiten freischalten, wenn Sie Ihre Firewall speziell einrichten.

Geben Sie dazu ankommenden und abgehenden Verkehr auf Port *6669* generell frei und ermächtigen Sie das Programm *NetChekker.exe*, ungehindert abgehenden Verkehr auf sämtlichen Ports abzuwickeln. Was dafür zu unternehmen ist, hängt davon ab, welche Firewall Sie verwenden. Das folgende Beispiel schildert das Vorgehen im Falle der zu Windows 7 gehörenden Firewall.

Firewall-Einrichtung unter Windows 7

Öffnen Sie als Administrator die *Windows-Firewall mit erweiterter Sicherheit* und klicken *Eingehende Regeln* an. Klicken Sie auf *Neue Regel*, wählen Sie *Port* an und klicken auf *Weiter*. Danach aktivieren Sie *TCP* und tragen unter *Bestimmte lokale Ports* bitte *6669* ein. Danach klicken Sie auf *Weiter*, aktivieren *Verbindung zulassen* und klicken erneut auf *Weiter*.

Unter *Wann wird diese Regel angewendet?* aktivieren Sie alle drei Angebote *Domäne*, *Privat* und *Öffentlich*. Klicken Sie auf *Weiter*. Als Name tragen Sie *NetChekker-Port* und unter Beschreibung bitte *Port 6669* ein. Danach klicken Sie *Fertigstellen* an.

Darauf klicken Sie bitte auf *Ausgehende Regeln*, *Neue Regel* und aktivieren als Regeltyp *Programm*. Klicken Sie auf *Weiter*, danach auf *Durchsuchen* und navigieren im NetChekker-Arbeitsordner zur Datei *NetChekker.exe*; klicken Sie dann auf *Weiter* und aktivieren Sie *Verbindung zulassen*. Nach Anklicken von *Weiter* aktivieren Sie die drei Angebote *Domäne*, *Privat* und *Öffentlich* und klicken auf *Weiter*. Darauf tragen Sie unter Name den Programmnamen *NetChekker* und unter Beschreibung *Ausgehend alle Ports* ein.

Mit dem Anklicken von *Fertig stellen* wird die Arbeit abgeschlossen. Damit ist sichergestellt, dass die Firewall von NetChekker ausgehende Verbindungsversuche über alle Ports passieren lässt und dass von außen kommende Verbindungswünsche auf Port *6669* ungehindert an NetChekker weitergeleitet werden.

So arbeitet NetChekker

NetChekker stellt Ihnen einen *Client* und einen *Server* zu Verfügung, die Sie einzeln oder gemeinsam einsetzen. Der Client und der Server arbeiten nach dem Protokoll *TCP (Transmission Control Protocol)*; siehe Literaturverzeichnis). In der Netztechnik sind Clients Software-Module oder Geräte, die Anfragen (*Requests*) an einen Server schicken und dessen Antworten verarbeiten. Server sind Software-Module oder Geräte, die auf Anfragen von Clients warten und diese Anfragen beantworten.

Das Arbeitsprinzip von NetChekker in jedem Fall: Ein Client versucht eine Anfrage an einen Server zu senden und dessen Antwort zu deuten. Ob und wie dies gelingt, wird dem Nutzer mitgeteilt - bisweilen ergänzt durch aufschlussreiche Zusatzinformationen. Die Ergebnisse der Tests werden in zwei Tagebüchern (*Logs*)

mitgeschrieben, je einem für den Client und den Server. Der Nutzer kann wählen, wie ausführlich die Tagebücher geführt werden. Jeder Eintrag beginnt mit der sekundengenauen Uhrzeit des protokollierten Ereignisses. Der Tagebuch-Inhalt kann mit einem eingebauten Editor bearbeitet, durchsucht und abgespeichert werden.

Außerdem werden die wichtigsten Meldungen zusätzlich in menschlicher Sprache als Stereosignal ausgegeben. Dabei sind Meldungen, die den Client betreffen, linksbetont, und Meldungen des Servers rechtsbetont. Das erleichtert die Arbeit mit mehreren Rechnern, weil man nicht mehrere Bildschirme gleichzeitig beobachten muss. Die Benutzeroberfläche ist zwischen Deutsch und Englisch umschaltbar. Netzbezogene Meldungen des Betriebssystems in den Logs erfolgen dagegen immer in der genormten englischen Nomenklatur.

Einsatzmöglichkeiten

Die Arbeitsmöglichkeiten mit Netzchecker lassen sich in vier Gruppen einteilen:

1. **Einsatz des Servers alleine**
Sie starten den NetChekker-Server, um beispielsweise die Reaktion der Firewall auf das Öffnen eines Ports zu überprüfen.
2. **Einsatz von NetChekker-Client zusammen mit NetChekker-Server**
Sie starten auf Ihrem PC den NetChekker-Server und schicken an diesen Server dann von einem NetChecker-Client auf dem gleichen oder einem anderen Rechner aus eine Anfrage.
3. **Einsatz von NetChekker-Client zusammen mit Fremdserver**
Sie richten mit dem NetChekker-Client eine Anfrage an einen Fremdserver, etwa an einen Webserver oder einen SMTP-Server auf dem eigenen Rechner oder auf einem Computer außerhalb im Intra- oder Internet.
4. **Einsatz von Fremdclient zusammen mit NetChekker-Server**
Sie richten mit einem fremden Client auf Ihrem Rechner, etwa einem Browser, einem Email-Client oder einem FTP-Client, eine Anfrage an den NetChekker-Server auf Ihrem Rechner.

Weiter unten finden Sie Beispiele für konkrete Tests aus allen vier Gruppen. Für die Arbeit mit NetChekker sollten die Begriffe Adresse, Portnummer, Protokoll, FTP, Telnet, SMTP und HTTP bekannt sein. Sie werden deswegen hier kurz erläutert.

Adressen

Computer in Netzen wie dem Internet und den meisten LANs kommunizieren miteinander über Adressen und Portnummern. Adressen können auf dreierlei Art angegeben werden:

1. Als IP-Adresse (*Internet Protocol Address*)
2. als URL (*Uniform Ressource Locator*)
3. als Domain-Name.

So ist beispielsweise *http://www.ard.de* der URL und *ard.de* der Domain-Name einer vielbesuchten Website, deren IP-Adresse *95.140.225.118* lautet.

Portnummern und Protokolle

Einige Portnummern sind für bestimmte Serverarten reserviert, andere dagegen frei wählbar. So gehört Port 21 beispielsweise zu FTP-Servern, Port 23 zu Telnet-Servern, Port 25 zum Dienst SMTP und Port 80 zu HTTP-Servern. NetChecker benutzt in seiner Grundeinstellung die Portnummer 6669. Man benennt Server oft nach den Protokollen, mit denen sie arbeiten: FTP-Server arbeiten nach dem *File Transfer Protocol*, Telnet-Server nach dem *Tele Network Protocol* und SMTP-Server nach dem *Simple Mail Transfer Protocol*. Webserver dagegen tanzen, was die Benennung angeht, aus der Reihe: Sie arbeiten nach dem *Hypertext Transfer Protocol* (HTTP).

Der Server

Im Feld *Empfang* auf: stellen Sie den Port ein, auf dem der Server lauschen soll. Das kann durch Eintragen einer Zahl, durch Anklicken der Schaltflächen Keil aufwärts und Keil abwärts oder durch Anklicken der Buttons 21, 23, 25, 80 und 6669 geschehen.

Im Feld *Kennung* steht die Zeichenfolge, mit der sich der Server bei einem anrufenden Client meldet. Sie können die Kennung nach Belieben ändern.

Das Feld *Schnittstelle* zeigt die Adresse des Netzanschluss-Bausteins in Ihrem Computer an. Wenn mehrere Netzanschlüsse vorhanden sind, etwa für LAN und WLAN, können Sie durch Anklicken des Keils ein Klappmenü öffnen und dort den gewünschten Netzanschluss auswählen.

Durch Anklicken der Buttons *Start* und *Stop* aktivieren und deaktivieren Sie den Server.

Der Client

Unter *Senden auf*: wählen Sie den Port, an den der Client seine Anfrage absendet. Die Portnummer können Sie von Hand eintragen, durch Anklicken der Keile ändern oder über einen der Buttons 21, 23, 25, 80 und 6669 anwählen. Im Feld *Senden an*: ist einzutragen, mit wem der Client Verbindung aufnehmen soll. Eingetragen werden können sowohl IP-Adressen wie *283.24.177.8* oder auch URLs und Domain-Namen aus dem Internet oder LAN, beispielsweise *datenburg.com* oder *MeinLaptop*.

Die Felder *Schnittstelle* und *Kennung* haben die gleiche Bedeutung wie beim Server. Unter *Ticks* lässt sich die Pausenzeit bei der Betriebsart Wiederholen ändern. *Verbinden* startet den Server, *Trennen* setzt ihn zurück.

Wenn Sie den Button *Voreinstellungen* anklicken, öffnet sich ein Fenster mit einer Liste, in der unter den Spaltenüberschriften *Senden an*, *Senden auf* und *Empfangen auf* die sieben zuletzt benutzten Einstellungen zu finden sind. Durch Doppelklick in eine Zeile starten Sie die betreffende Verbindung, durch einfaches Anklicken wählen Sie eine Zeile aus. Anklicken von *Weiter* führt zur Übertragung der entsprechenden Werte in die Felder *Senden auf*, *Senden an* und *Empfangen auf* des Hauptfensters. Anklicken von *Abbrechen* beendet die Aktion vorzeitig.

Anklicken des Buttons *IP* führt zur Ermittlung und Anzeige der aktiven lokalen und der globalen IP-Adresse des Systems. Unter der lokalen IP-Adresse ist das System im LAN zu erreichen und unter der globalen IP-Adresse tritt es im Internet auf. Wenn beide Adressen gleich sind, dann bedeutet dies entweder, dass kein Router vorhanden ist, ein vorhandener Router NAT (Network Address Translation) nicht beherrscht oder dass im Router NAT ausgeschaltet wurde.

Die Tagebuch-Fenster

Verbindungsversuche und ihre Ergebnisse notiert NetChekker in den Log-Fenstern von Client und Server. Durch Rechtsklick in diese Fenster öffnen Sie ein Kontextmenü mit folgenden Angeboten:

1. Löschen
2. Aufruf eines Editors zum Bearbeiten, Abspeichern und Drucken
3. Umschaltung in Kurzform ohne vorangestellte Uhrzeit

Einstellelemente im Fußbereich

Warten unterdrückt die selbsttätige Beendigung einer Verbindung und entscheidet darüber, ob der Client nach dem Dialog mit einem Server die Verbindung beendet oder auf das Anklicken von *Trennen* wartet. Ist *Synchron* gesetzt, reagiert der Client auf einen Verbindungsabbruch durch den Server sofort durch den Verbindungsabbau auf seiner Seite; ansonsten lässt der Server den benutzten Port noch eine Zeitlang offen.

Wiederholen zwingt den Client, seine Verbindungsversuche selbsttätig ständig fortzusetzen, bis Sie *Trennen* anklicken; die Länge der Pause zwischen den Versuchen sind durch den Wert der Ticks festgelegt. Ein *Tick* entspricht ungefähr einer Drittel Sekunde. Ist *Diagnose* aktiviert, werden die von Client und Server in ihren Protokollfenstern geführten Tagebücher zur Fehlersuche und zum Systemstudium in erweiterter Form geschrieben. *Debug* führt zu zusätzlichen Mitteilungen.

Ist *Synchron* gesetzt, lösen Verbindungsabbrüche durch den Client auch Verbindungsabbrüche auf der Clientseite der Verbindung aus.

Wenn Sie *HTTP* aktivieren, richtet der Client bei der Verbindungsaufnahme einen HTTP-GET-Request an den Server. Benutzen Sie diese Option zur Anforderung von Webseiten.

Mit *Hints* schalten Sie Hilfetexte aus und ein, die erscheinen, wenn der Cursor auf einer Schaltfläche verharrt. Durch Deaktivieren von *Sound* unterbinden Sie die Ausgabe von akustischen Mitteilungen in menschlicher Sprache.

Über *Deutsch* und *English* ändern Sie die Arbeitssprache der Benutzerführung von NetChekker.

Wenn in der Firewall des getesteten Rechners die Protokollführung aktiviert und NetChekker entsprechend eingerichtet ist, öffnet ein Linksklick auf den Button *Firewall-Tagebuch* die entsprechende Logdatei. Anklicken dieses Buttons mit der rechten Taste öffnet ein Menü mit den Angeboten *Auto*, *Default*, *Reset* und *Select*. Dabei versucht *Auto* die Standard-Firewall-Logdatei von Windows *pfirewall.log* automatisch zu finden. *Select* ermöglicht das Navigieren zu einer frei wählbaren Logdatei beliebigem Namens und wird eingesetzt, wenn statt der Standard-Firewall des Betriebssystems ein anderes Firewall-Produkt eingesetzt wird.

Anklicken von *Reset* setzt das Programm auf seine Grundeinstellungen zurück.

Über den Button *Check* können Sie im Eintrag *Firewall Logfile* prüfen, ob eine Firewall-Tagebuchdatei von NetChekker erkannt wurde, wie ihr erweiterter Name lautet und in welchem Verzeichnis sie liegt.

Anklicken des *Clone*-Buttons startet zusätzlich zur laufenden NetChekker-Version eine Sonderfassung des Programms unter einem speziellen Namen, der bei jedem Start neu erzeugt wird und sich nicht wiederholt. Damit ist sichergestellt, dass die Firewall dieses Programm nicht kennt und somit ihre Reaktion auf Angriffe durch unbekannte Clients getestet werden kann.

Die Bedienungsanleitung wird nach Anklicken von *Handbuch* angezeigt; sie kann durchsucht und ausgedruckt werden. Voraussetzung dafür ist, dass auf dem betreffenden System ein PDF-Reader installiert ist, beispielsweise der Adobe Reader.

Der Button *Update* dient zur Aktualisierung der Schnittstellenliste des Computers, auf dem Sie gerade arbeiten. Klicken Sie diese Taste an, wenn Sie beispielsweise im laufenden Betrieb einen WLAN-Adapter zugeschaltet oder auf andere Weise ihre Netzwerk-Konfiguration geändert haben. Die Anzahl der aktuell vorhandenen Listeneinträge wird unter *Schnittstellen* angezeigt.

Anwendungsbeispiele

NetChekker ermöglicht sehr viele höchst unterschiedliche Prüfungen in Netzwerken - weitaus mehr, als auf vier Seiten dargestellt werden können. Deswegen sind hier nur einige wenige Anwendungen beispielhaft aufgeführt.

Soweit nicht im Einzelfall anderes gesagt, sollten beim Starten der Beispiele die Kästchen *Warten*, *Wiederholen*, *Synchron*, *Diagnose*, *HTTP* und *Debug* deaktiviert sein sowie *Senden auf* und *Empfang auf* in ihrer Grundstellung 6669 stehen.

Durch Anklicken des Reset-Buttons können Sie die Einstellungen auf diese Grundwerte zurücksetzen. Bitte beachten Sie, dass bei den Tests häufig Stereo-Ausgaben von Mitteilungen in menschlicher Sprache erfolgen und die Lautsprecher deswegen eingeschaltet sein sollten

1 Winsock prüfen

Mit diesem Test stellen Sie fest, ob der für TCP-Betrieb zuständige Teil des Betriebssystems namens *WinSock* installiert und bereit ist. Klicken Sie auf *Start* und dann auf *Verbinden*. Wenn Winsock funktioniert, hören Sie Ansagen, die den Verbindungsaufbau und Verbindungsabbau begleiten: *Client verbunden* und einige Sekunden darauf *Client getrennt*. Ansonsten wird *Misserfolg* gemeldet. Sie beenden den Test durch Anklicken von *Stopp*.

2 Firewall prüfen

Klicken Sie auf *Clone* und dann im neuen Clone-Fenster auf *Start*. Die Firewall muss daraufhin Alarm schlagen, wenn sie konfiguriert wurde wie weiter oben beschrieben. Beenden Sie den Test, indem sie im Clone-Fenster auf *Stop* und danach auf *Ende* klicken.

3 Interkonnektivität im LAN prüfen

Benötigt werden zwei Maschinen im LAN, beispielsweise zwei Rechner mit den Netznamen LAPTOP und DESKTOP. Starten Sie NetChekker auf DESKTOP und klicken Sie auf *Start*. Starten Sie NetChekker auf LAPTOP, tragen Sie unter *Senden an* DESKTOP ein und klicken Sie auf LAPTOP *Verbinden an*. Wenn kein Fehler vorliegt, melden die Lautsprecher den Aufbau und den Abbau einer Verbindung.

4 Kommunikation mit externen Emailservern prüfen

Setzen Sie *Senden auf* auf den Wert 25 und tragen Sie unter *Senden an* bitte *mail.gmx.net* ein. Klicken Sie *Verbinden an*. Im Erfolgsfall wird eine Verbindung zu GMX auf- und abgebaut. Wiederholen Sie den Test mit weiteren Einträgen für *Senden an*: *smtp.web.de*, *mail.arcor.de*.

Sodann wiederholen Sie diesen Test mit dem Eintrag *smtp.de.aol.com* und lesen Sie im Client-Tagebuchfenster, wie grimmig die Reaktion ausfällt. Tragen Sie danach unter *Senden auf* die Zahl 587 ein und klicken Sie erneut *Verbinden an*. man sieht, dass AOL auch Verbindungswünsche auf diesem speziellen Port entgegennimmt. Ändern Sie die Portnummer auf 599 und klicken erneut *Verbinden an*. Es setzt einen ausgewachsenen *Misserfolg*.

5 Kommunikation mit externem Webserver untersuchen

Wählen Sie unter *Senden auf* bitte 80, tragen unter *Senden an* ein *www.ard.de* und aktivieren *HTTP*. Nach dem Anklicken von *Verbinden* wird im Client-Tagebuchfenster sichtbar, dass Sie eine recht ausgedehnte Sendung empfangen. Wenn die Ansage "Client getrennt" verklungen ist, klicken Sie bitte mit der rechten Maustaste in das Client-Tagebuchfenster und wählen mit der linken Taste *Edit*. Sie haben den in den Sprachen HTML und Javascript geschriebenen Quelltext der ARD-Begrüßungsseite vorliegen. Kundige erkennen an den *e-tracker*-Eintragungen, dass die ARD ihren Besuchern hier sehr aufmerksam auf die Finger schaut.

Die Zeilen im Protokoll beginnen alle mit der Angabe von Stunde, Minute und Sekunde der Uhrzeit bei der Aufzeichnung der betreffenden Zeile. Wenn das stört, klicken Sie vor dem Anklicken von Edit auf *Kurzform*. Damit gehen die Uhrzeitangaben des aktuellen Protokolls allerdings auf Dauer verloren - einen Weg zurück gibt es nicht. Die nächste Aufzeichnung erfolgt wieder mit vorangestellter Uhrzeit.

6 Browser-Test

Sie beobachten immer wieder Störungen beim Besuch von Webseiten und möchten gern wissen, ob Ihr Browser beschädigt ist oder etwas mit der Verbindung zum Webserver nicht klappt? NetChekker hilft Ihnen bei der Fehlereingrenzung.

Starten Sie NetChekker, setzen Sie *Empfang auf* auf den Wert 80 und klicken Sie *Start* an. Starten Sie einen Browser und geben Sie als Adresse `http://DESKTOP` ein, wenn der Netzname Ihres Rechners DESKTOP lautet. Ersetzen Sie DESKTOP gegebenenfalls durch einen anderen Namen. Sie hören die Ansage *Server verbunden* und es erscheint eine Seite auf dem Schirm, mit der sich NetChekker als Webserver meldet. Drücken Sie die F5-Taste, um zu prüfen, ob auch die Aktualisierung klappt. NetChekker reagiert mit den Meldungen, dass die Verbindung abgebaut und wieder aufgebaut werde - also genau das macht, was man sich beim Aktualisieren wünscht. Beachten Sie, wie sich der *Zeitpunkt der Erfassung* dabei ändert.

7 NAT prüfen und globale IP-Adresse ermitteln

Einen sehr wirksamen Schutz gegen unprovokierte Überraschungsangriffe aus dem Netz stellt NAT dar, die *Network Address Translation*. Ist sie wirksam, bleibt die wahre (lokale) IP-Adresse Ihres Rechners anderen Systemen im Internet verborgen, sie "sehen" nur eine "globale" Adresse, über die sie von sich aus keine Verbindung aufnehmen können. Das klingt gut und klappt gut, doch leider: Nicht jeder Internet-Zugang ist mit NAT ausgestattet. Wie sieht es damit bei Ihnen aus?

Starten Sie den NetChekker und klicken Sie *IP* an. Sind Software und Hardware in Ordnung, kommt es zur Verbindung mit einem externen NetChekker-Server im Internet und zum Erscheinen einer Tafel, auf der Ihnen die lokale und die globale IP-Adresse Ihres Systems gemeldet wird. Sind beide gleich, haben Sie Pech gehabt: NAT steht Ihnen nicht zur Verfügung.

Bei den meisten Internet-Zugängen ersetzen Provider die globalen IP-Adressen ihrer Kunden spätestens nach 24 Stunden durch eine andere Adresse aus dem Vorrat der für sie registrierten Adressen. Wer langfristig über eine konstante Adressangabe erreichbar sein will, kann sich eines Alias-Domainnamens bedienen, wie er beispielsweise von www.dyndns.org kostenlos angeboten wird.

8 Port Forwarding testen

Manche Router verfügen über die Fähigkeit des "Port Forwarding", der Aufteilung eingehender Verbindungsversuche auf verschiedene Maschinen im örtlichen Netz. In einem LAN mit den Maschinen ANNE, DIDO, THOR haben wir den Router - in unserem Falle eine FritzBox 7270 - beispielsweise so eingerichtet, dass einlaufende Verbindungsversuche auf Port 6665 auf Port 6669 an ANNE, Versuche über Port 6666 auf Port 6669 an DIDO und Versuche über Port 6667 auf Port 6669 an THOR weitergeleitet wurden.

Danach starteten wir auf allen drei Maschinen durch Anklicken von *Start* den NetChekker-Server und nahmen von einem vierten System aus über das Internet per NetChekker-Client Verbindung zur gemeinsamen globalen Adresse von ANNE, DIDO und THOR auf. Je nach Portnummer kam es dabei jeweils zum Verbindungsaufbau mit dem gewünschten Rechner - der Nachweis der Wirksamkeit des eingerichteten Port Forwarding war erbracht.

9 Portsperrern nachweisen

Manche Internet-Provider sperren bestimmte Portnummern, um Verkehr zu unterbinden, der ihnen nicht passt. Oft ist lediglich im Kleingedruckten des Vertragstextes versteckt, dass der Kunde für sein gutes Geld nur einen dergestalt kastrierten Anschluss erhält. Mit NetChekker weisen Sie solche Machenschaften gerichtsfest nach. Sorgen Sie dafür, dass keine Firewall die zu prüfende Portnummer blockiert und dass der Router unter dieser Portnummer hereinkommende Daten an ihren Rechner weiterleitet. Stellen Sie durch Anklicken von *IP* ihre augenblickliche IP-Adresse fest. Dann legen Sie unter *Empfang auf* die Portnummer fest und klicken *Start an*.

Anschließend bitten Sie einen Freund an einem anderen Internetanschluss, auf seiner Maschine NetChekker zu starten, unter *Senden auf* die gleiche Portnummer zu wählen, unter *Senden an* Ihre globale IP-Adresse einzugeben und *Verbinden* anzuklicken. Der Lautsprecher verrät, ob es zu einer Verbindung kommt.

10 FTP-Client prüfen

Viele Windowsversionen sind mit einem eingebauten FTP-Client ausgestattet, den man manchmal aber erst nachinstallieren muss, um ihn nutzen zu können. Da kann es nützlich sein, schnell zu erfahren, ob der Windows-FTP-Client funktionsbereit ist. Starten Sie dazu den NetChekker-Server auf Port 21, öffnen ein Kommandozeilenfenster, tippen *ftp* und den Netznamen Ihres Rechners ein (für einen Rechner namens DESKTOP beispielsweise *ftp DESKTOP*) und drücken die Return-Taste. Klappt die Verbindung, meldet NetChekker im rechten Stereo-Lautsprecher "Server verbunden". Klicken Sie zur Beendigung dieses Versuchs *Stopp an*.

11 Lügende Provider-Computer überführen

Wenn Sie beim Surfen versehentlich einen nicht existierenden Domain-Namen eingeben, muss der DNS-Service Ihres Internetproviders dies Ihrem Browser durch einen speziellen Code mitteilen, damit eine korrekte Fehlermeldung ausgegeben werden kann. Manche Provider leiten, statt eine solche Meldung abzusen- den, den Nutzer auf eine eigene Webseite mit Eigenwerbung oder sogar bezahlter Reklame. Das bringt solchen Unternehmen zehntausende von Extraclicks ein.

Weil eine solche unbestellte Umleitung regelwidrig und in der Internet-Technik nicht vorgesehen ist, bedienen sich manche Provider einer Lüge. Sie lassen ihren Webserver behaupten, die falsch getippte Adresse sei zu ihnen "umgezogen".

Mit dem NetChekker können Sie innerhalb weniger Sekunden feststellen, wie es Ihr Provider in dieser Hinsicht hält, und dabei ein Protokoll des Geschehens als gerichtsverwertbaren Beweis anfertigen und ausdrucken.

Gehen Sie dazu so vor: Aktivieren Sie *HTTP* durch Anklicken der entsprechenden Checkbox.. Unter *Senden auf* wählen Sie *80*, im Feld *Senden an* geben Sie bitte *Reiner.Quatsch* ein und klicken dann auf *Verbinden*. Im Client-Protokollfeld können Sie nun studieren, wie es mit der Wahrheitsliebe Ihres Internetproviders steht, und die Niederschrift nach Rechtsklick und Anwählen von *Editor* ausdrucken..

Bei diesem Test teilte uns der Webserver unseres DSL-Providers mit, die Adresse *Reiner.Quatsch* sei tatsächlich gefunden worden ("302 Found"), aber leider umgezogen ("The document has moved") und jetzt erreichbar über "<http://navigationshilfe1.t-online.de>". Überflüssig, zu sagen, dass es eine Top Level Domain namens Quatsch noch nie gegeben hat und vermutlich auch nie geben wird. Wem das nicht gefällt, kann sich im T-Online-"Kundencenter" dagegen verwahren und diesen Trick unterbinden lassen.

SmartSniffer, CurrentPorts und WireShark

Zum Studium spezieller Details der Netzwerktechnik und zur Erweiterung der Fehlereingrenzungsmöglichkeiten lässt sich NetChekker zusammen mit *CurrentPorts* und *SmartSniffer* (beide von www.nirsoft.net) betreiben. Diese Programme zeigen die in einem System jeweils geöffneten Ports an und protokollieren den Datenverkehr über sie. Sehr detaillierte Protokolle über das Geschehen an Netzwerkadaptern liefert *Wireshark* (www.wireshark.org).

Deinstallation

Löschen Sie den NetChekker-Ordner einschließlich Inhalt und, soweit vorhanden, das Desktopsymbol, den Starteintrag und den Programmeintrag zu NetChekker.

Stattdessen können Sie auch als Nutzer mit Administratorrechten die Installationsdatei *NetChekkerPaket.exe* erneut starten und *Deinstallieren* wählen. Entfernen Sie gegebenenfalls den Programmnamen NetChekker und die Portnummer 6669 aus den Firewallinstellungen.

Literatur

(1) "Transmission Control Protocol/Internet Protocol" (Gute deutsche Übersicht):
<http://de.wikipedia.org/wiki/TCP/IP>

(2) "TCP/IP-Grundlagen für Microsoft Windows":
<http://www.microsoft.com/germany/technet/datenbank/articles/600579.msp>

(3) "TCP/IP Tutorial and Technical Overview" (Systematisches Standardwerk):
<http://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf>.