Schutz vor OOB-Attacken

Franz Bachler

Im TCP/IP-Subsystem von Windows95 befindet sich ein Fehler ("Bug"), welcher dazu führt, dass sogenannte OOB-Datenpakete ("out of band") nicht verarbeitet werden können. Bei einem mehrmaligen Auftreten von geschickt platzierten OOB-Paketen verabschiedet sich Windows95 mit dem berühmt-berüchtigten "Blue Screen" (betrifft sowohl die ältere A- als auch die neuere B-Version). Dabei ist es egal, ob diese Datenpakete über das interne Netzwerk via Netzwerkkarte oder aber über das Internet via DFÜ-Adapter in den Rechner kommen.

Das TCP/IP-Protokoll zerteilt die zu übertragenden Daten in kleine Pakete, welche sich selbständig den Weg durch das Netzwerk suchen. Gerade im weltweiten Internet ist dies von Vorteil: Ist ein Netzwerkknoten überlastet oder ist er gar ganz ausgefallen, dann nehmen die Datenpakete eben einen anderen Weg. Im Gegensatz dazu wird z. B. bei einem Telefonferngespräch ein fixer Leitungsweg zwischen den einzelnen Vermittlungsstellen aufgebaut.

Aus diesem Grund kann es vorkommen, dass zwar die Pakete 1, 2 und 3 nacheinander gesendet werden, aber beim Empfänger in der Reihenfolge 1, 3 und 2 ankommen. Dies stellt aber kein Problem dar, da die TCP/IP-Software die korrekte Reihenfolge wieder herstellt.

Beispiel für "normale" Datenpakete

```
Paket 1:      Bytes 1 - 200
Paket 2:      Bytes 401 - 600
Paket 3:      Bytes 201 - 400
```

Ein OOB-Paket sieht dagegen so aus:

```
Paket 1:      Bytes 1 - 200
Paket 2:      Bytes 301 - 500
Paket 3:      Bytes 201 - 400
```

Im normalen Netzwerkbetrieb treten solche OOB-Pakete niemals auf. Berühmt-berüchtigte Programme namens "Winnuke" oder "Teardrop" produzieren dagegen gezielt solche Datenpakete mit dem Ziel, das Betriebssystem eines anderen Computers zum Absturz zu bringen. Die Hard- und Software des attackierten Rechners wird dabei zwar nicht gefährdet, aber der Computer muss neu gebootet werden und dabei gehen nicht gespeicherte Daten verloren.

Aber auch als Windows95-User kann man sich vor solchen Attacken schützen: Es gibt ein kleines, nur ca. 25 kB großes Windowsprogramm namens "Antinuke", welches die OOB-Pakete abfängt, so dass diese keinen Schaden anrichten können. Das Programm hat auch noch zwei Nebenfunktionen: Es zeigt die IP-Adresse desjenigen, der die Attacke versucht hat (erleichtert das Ausforschen des Übeltäters) und die eigene IP-Adresse sowohl der Netzwerkkarte als auch der aktuellen Internetverbindung an.

Die eigene IP-Adresse benötigt man z. B. um eine direkte und schnellere Verbindung bei der Internet-Telefonie aufzubauen (ohne zeitverzögernden Umweg über einen Telefonieserver). Da die weltweiten IP-Adressen für das Internet begrenzt sind, wird bei den meisten Providern folgendermaßen vorgegangen: Es sind z. B. 100 Internetuser beim Provider angemeldet und 20 Modems stehen zur Einwahl bereit. Da niemals alle Internetuser gleichzeitig online gehen, ist dies ausreichend. (In Europa kann es sich ein normaler Internetuser im Gegensatz zu den USA kaum leisten, ständig im Netz zu hängen.) Daher genügen 20 IP-Adressen für die 100 User (80 Adressen eingespart!), welche beim Verbindungsaufbau dynamisch aus dem Pool vergeben werden. Somit hat man nach jedem Einwählen eine andere IP-Adresse, welche nun bequem von "Antinuke" angezeigt wird.

Man findet "Antinuke" im Internet unter mit dem Stichwort "Antinuke".

Hinweise: Windows 3.11 reagiert auf OOB-Pakete ebenfalls mit einem Absturz. "Antinuke" ist aber 32bit-Programm, so dass es unter Windows 3.11 nicht verwendet werden kann. Windows98 und Windows NT 4 ab Servicepack 2 sind gegen solche Attacken "immun". OOB-Pakete kommen erst gar nicht hindurch. Hier zeigt "Antinuke" nur die aktuellen IP-Adressen an. Ebenso richten diese Pakete unter Unix (Linux) keinen Schaden an.