TCP/IP für Anfänger

Vortrag: *Pirx* <pirx@ccc.de>

Bericht: *Nico Lumma* <nico@goe.net>

Im Workshop TCP/IP für Anfänger wurden die Grundzüge von TCP/IP in knapp zwei Stunden dargestellt. Der Referent Pirx benutzte dafür mehr als 50 Folien, die auch alle auf dem FTP-Server (ftp://ftp.congress.ccc.de/ des CCC bereit liegen.

Der Workshop wurde in folgende Teile gegliedert:

1. TCP/IP und das Internet
2. Protokolle - Schichtenmodell - IP, UDP, TCP und ARP
3. Routing und Congestion Control
4. Anwendungen
5. Angriffspunkte

Im ersten Abschnitt wurde kurz das Wesentlichste zum Thema Internet und dessen Entstehung gesagt. Dabei ging der Referent insbesondere auf die Notwendigkeit ein, ausfallsichere Netzwerke zu schaffen, einer Voraussetzung, die maßgeblich zur Entwicklung der Internet-Protokolle beitrug. Hervorgehoben wurden ausserdem die paketweise Übertragung der Daten sowie der Verzicht auf zentrale Verwaltungsstellen und Knoten. Abschließend wurde auf die sog. RFCs (Requests for Comments) verwiesen, die zwar keinen offiziellen Standard darstellen, aber weitgehend akzeptiert werden.

Der zweite Abschnitt des Workshops widmete sich den Protokollen. Am Anfang der Ausführungen stand eine Darstellung des Schichtenmodells, wobei es wie folgt dargestellt wurde:

4. Schicht	Application Layer: Benutzerprozesse	--> FTP, HTTP, NFS, DNS
3. Schicht	Transport Layer: Paketsicherung	--> TCP | UDP
2. Schicht	Network: Paketzustellung, Routing	--> IP {ICMP}
1. Schicht	Link: Hardware, Geraetetreiber	--> Ethernet, Token Ring

Nach einem kurzen Exkurs zum Thema Ethernet wurden alle Schichten erläutert und der Aufbau der jeweils eingesetzten Protokolle beschrieben. Weiterhin wurde der sog. 3-Way-Handshake beim Verbindungsaufbau zwischen Client und Server erläutert, bei dem zuerst der Client beim Server eine SYN-Anfrage stellt, die vom Server mit SYN+ACK bestätigt wird, die wiederum vom Client mit einem weiteren ACK bestätigt wird. Als dritter Punkt wurde Routing und Congestion Control angeschnitten. Neben der Einteilung von Netzwerken in Class A, B und C Netze wurde kurz erklärt, wie sich Netzmasken zusammensetzen. Einführend wurde das Routing zwischen den Netzen erläutert und einige Protokolle für das dynamische Routing angesprochen (RIP, EGP, BGP). Auch der DNS (Domain Name Service) wurde in diesem Abschnitt erklärt. Der Referent ging abschließend auf die Vermeidung von Überlast ein und stellte zwei Mechanismen vor, die unter TCP eingesetzt werden. Der sog. Slow Start beginnt beim Verbindungsaufbau nicht gleich mit der größtmöglichen Paketgrösse, sondern fängt mit einer kleinen an und steigert sich dann bei erfolgreicher Paketübermittlung automatisch. Die sog. Congestion Avoidance setzt beim Paketverlust ein und halbiert automatisch die Paketgrösse, die erst langsam mittels Slow Start wieder hoch gesetzt wird.

In einem weiteren Abschnittt wurden von Pirx dann noch die gängigsten Applikationen vorgestellt, die aber dem Publikum auch schon weitgehend bekannt waren. Ausser beispielsweise NFS, DNS oder Tracroute, die auf UDP aufsetzen, sind die meisten Anwendungen tcp-basiert, wie etwa Telnet, SSH, FTP, HTTP, SMTP/POP3, o.ae.

Im letzten Abschnitt ging Pirx auf die Angriffsmoeglichkeiten von TCP/IP ein. Zu den gängigen Methoden gehören hier sog. Denial of Service Attacken (DoS), die berechtigte NutzerInnen vom Arbeiten mit dem System abhalten, das Ausspähen von Daten durch Mitlesen, die Verfälschung von Daten während der Übertragung, den aktiven Eingriff in Netzknoten (Rechner, Router) ermöglicht. Ebenso gehört zu diesen Methoden das sogenannte IP-Spoofing, bei dem IP-Adressen verfälscht werden.

Für weitere Beschäftigung mit dem Thema wurde auf weitere Workshops auf dem Chaos Congress verwiesen.

Als Literaturhinweise schlug Pirx folgendes vor: - W. Richard Stevens, TCP/IP Illustrated, Addison Wesley - Olaf Kirch, Linux Network Administrators Guide, LDP/O´Reilly - Douglas Comer, Internetworking with TCP/IP, Prentice Hall

Alles in einem war dieser Workshop sehr gut und vor allem auf das Wesentliche beschränkt. Absoluten Anfängern in Sachen TCP/IP wurde ein sehr guter Einstieg geboten, der sicherlich zum Verständnis von anderen Workshops beiträgt.