



Netzwerk. Aber sicher!

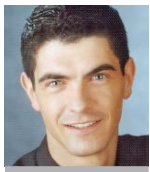
Netzwerke gibt es allerorten, aber was genau ist ein Netzwerk und wie funktioniert es? In der ersten Folge zu diesem Thema geht es um die Grundlagen.

Neben dem Internet als dem einen großen Netzwerk (Wide Area Network - WAN), welches uns alle verbindet, gibt es viele weitere Netzwerke, die privat genutzt werden und als Local Area Network (LAN) bezeichnet werden. In Firmen, zu Hause oder in der Arztpraxis.

Neuer, schneller, besser

Das Internet Protocol (IP) in der Version 4 wurde 1981 definiert und die mit ihm abbildbare Anzahl an eindeutigen Adressen (ca. 4,3 Mrd.) in einem Netz stellt für die weitere Ausdehnung des Internets einen Flaschenhals dar – spätestens mit Einzug des Internets der Dinge, bei dem Uhren, Heizungsthermostate und Autos eigene IP-Adressen haben.

Auch der Nachfolger – IP in der Version 6 – ist bereits seit gut 15 Jahren spezifiziert, aber erst jetzt kommt die Umstellung ins Rollen. Mit der exorbitanten Anzahl an Adressen (ca. 340 Sextillionen, eine Zahl mit 36 Nullen) geht aber leider auch eine kryptischere Schreibweise einher, die auf dem Hexadezimalsystem basiert und Adressen daher bspw. so aussehen können: 2001:0db8:85a3:08d3:1319:8a2e:0370:7344. Dass man bei solchen Zeichenketten die Verwaltung lieber den Systemen überlässt, liegt auf der Hand.



Christian Kierdorf
IT-Sicherheitsbeauftragter
Deutscher Hausärzteverband

Im Laufe der Jahre hat sich Ethernet als Standard faktisch durchgesetzt und bildet die Grundlage für die Kommunikation, indem beispielsweise die Steckerform (sog. „RJ-45“-Stecker) sowie Verkabelung und deren Schirmung definiert sind – und dies für unterschiedliche Geschwindigkeiten. Weit verbreitet ist das „Fast Ethernet“ mit einer theoretischen, maximalen Übertragungsrate von 100 Mbit/s (entspricht ~12,5 Mbyte/s), für neuere Installationen wählt man in der Regel Gigabit-Ethernet, bei dem die theoretische Datenrate bei 1.000 Mbit/s beträgt. Aufbauend auf der physikalischen Verbindung besteht dann die Möglichkeit, Endgeräte wie Computer und Server miteinander

zu verbinden (ein privates Netz) und auch den Weg in andere Netze – privat wie öffentlich – zu finden.

Hierfür müssen die Endgeräte über Adressen verfügen, die in Form von vier Oktetten die IP-Adresse definieren (bei IPv4 meistens beginnend mit „192.168.xxx.xxx“; Näheres dazu siehe Kasten) und im jeweiligen Netzwerk eindeutig sein müssen.

Um die Adressen nicht manuell den einzelnen Geräte zuweisen zu müssen, kann auf einem zentralen System wie dem Praisserver oder -router zumeist ein Dienst (Dynamic Host Configuration Protocol – DHCP) aktiviert werden, der neu angeschlossenen Gerä-

ten dynamisch neue Adressen zuweist und sie somit automatisch in das Netzwerk integriert und Adresskonflikte unterbindet. Für Serversysteme und Router sollte von der dynamischen Adressvergabe abgesehen werden, um fixe Kommunikationspartner regelmäßig wiederzufinden. Diese Adressen sind auch aus dem

zur Vergabe durch DHCP vorgesehenen Adressbereich auszuschließen.

Um den ungewollten Zugang durch unbekannte Endgeräte zum Netzwerk zu verhindern, gibt es diverse Sicherungsmethoden, wovon die einfachste auch zugleich eine der effektivsten ist: Jede Netzwerkdose, die nicht gepatcht (i. e. mit dem zentralen Switch verbunden) ist, kann auch nicht zum Zugriff auf das Netzwerk verwendet werden. Wenn die Kabel bei Ihnen von einem zentralen Patchpanel zu den jeweiligen Netzwerk Dosen in den Praxisräumen verlaufen, dann schalten Sie nur solche Netzwerk Dosen vom Patchpanel auf den Switch auf, die Sie auch in Gebrauch haben.