Aufbau des lokalen Netzwerks

Netzwerkstruktur:

Üblicherweise sind moderne Schulnetzwerke über eine IT-Infrastruktur vernetzt, bei der pro netzwerkfähigem Gerät eine separate Leitung zu einem Sammelpunkt gezogen wird, an dem eine zentrale Komponente („Switch“) die Kommunikation zwischen den einzelnen Strängen organisiert. Diese Leitungen werden häufig aus Kostengründen als Doppel-Leitungen verlegt, so dass an eine Netzwerk-Dose gewöhnlich zwei Geräte angeschlossen werden können.

Von dem Switch aus wird auch die Anbindung an das Internet für alle angeschlossenen Geräte über eine gemeinsame Datenleitung realisiert.

Funktionsprinzip

- Nicht vernetzte PCs
  Solche Geräte sind am unbedenklichsten, da nur der PC-Nutzer selbst auf die pbD zugreifen kann. Hier muss dafür gesorgt werden, dass die Maßnahmen zur Absicherung eines Arbeitsplatzcomputers (s. u.) umgesetzt sind.

- Peer-to-Peer-System und DSL-Box
  Bei diesem System sind die Arbeitsplatzcomputer über die Netzwerk-Infrastruktur verbunden. Sie teilen sich gemeinsam einige Ressourcen im Netzwerk (Drucker, gemeinsame Ordner). Über die Maßnahmen zur Absicherung der Arbeitsplatzcomputer hinaus muss bei diesem System darauf geachtet werden, dass keine ungewollten Zugriffe über das lokale Netz oder das Internet erfolgen. Da es nur sehr beschränkte Möglichkeiten der Kontrolle gibt, ist ein solches System nur dann zu empfehlen, wenn keine pbD im lokalen Netz oder auf den Arbeitsplatzcomputern gespeichert sind.
  Die DSL-Box stellt den Internetzugang her. Sie muss so konfiguriert sein, dass nur Datenpakete in das lokale Netz gelassen werden, die auch von innen angefordert wurden („Firewall“-Funktionalität). Häufig sind die DSL-Boxen aber ab Werk so konfiguriert, dass sie alle Datenpakete (auch solche, die nicht angefordert wurden) passieren lassen.

- File-Server + DSL-Box
  Ein solches System bietet die Möglichkeit, auf einem zentralen Rechner („File-Server“) Dateien abzulegen. Da auf einem File-Server Benutzerkonten angelegt werden können, ist der Zugriff auf Dateien sehr genau zu regeln. PbD können bei sorgfältiger Konfiguration eines File-Servers als gut geschützt angesehen werden.
  Die DSL-Box stellt den Internetzugang her. Sie muss so konfiguriert sein, dass nur Datenpakete in das lokale Netz gelassen werden, die auch von innen angefordert wurden („Firewall“-Funktionalität). Häufig sind die DSL-Boxen aber ab Werk so konfiguriert, dass sie alle Datenpakete (auch solche, die nicht angefordert wurden) passieren lassen.

- Kommunikations-Server
  Ein Kommunikations-Server bietet die Funktionalität des File-Servers und der DSL-Box sowie möglicherweise weitere Dienste (E-Mail-Server, Web-Server). Da es sich dabei um aufeinander abgestimmte (Software-)Komponenten handelt, kann man die Konfiguration eines solchen Servers sehr genau einstellen, benötigt dazu aber ein hohes Maß an Sachverstand. Häufig bietet ein Kommunikations-Server auch die Erreichbarkeit vom privaten PC aus an.
  Falls Ihre Schule einen solchen Kommunikations-Server betreibt, besprechen Sie bitte die technischen Details dieses Kapitels mit dem zuständigen Administrator oder der zuständigen Support-Einrichtung.

- WLAN
  Funkvernetzung ist aus Kostengründen häufig eine Alternative zur herkömmlichen Verkabelung (s. o.). Dennoch muss auch ein Funknetzwerk so abgesichert werden, dass pbD im lokalen Netz vor unberechtigten Zugriff(sversuch)en geschützt sind. Es besteht die Möglichkeit, den Zugang zum Funknetzwerk abzusichern und den Funkverkehr zu verschlüsseln.

- Anbindung an das Internet
  Schulen sind üblicherweise mit einer ununterbrochenen Anbindung an das Internet versehen. Als Grundregel kann gesagt werden, dass ein Schulnetz dann sicher geschützt ist, wenn nur die Datenpakete aus dem Internet in das lokale Netz gelangen, die von innen angefordert wurden. Die „Firewall“-Funktionalität ist nur der Hauptaspekt bei der Betrachtung der Thematik. Er trifft für alle Schulnetzwerke zu. Weitere Aspekte sind

- die sichere Trennung von Schul- und Verwaltungsnetzwerk. Am besten besteht keine physikalische Verbindung zwischen beiden Netzwerken!
- bei File-Servern und Kommunikations-Servern ein ständig aktualisierter Viren-Filter, um die Manipulation oder feindliche Übernahme eines Servers zu verhindern.
- bei Kommunikations-Servern zusätzlich ein Filter für den E-Mail-Verkehr, um eine Kompromittierung des Servers auf diesem Wege zu verhindern.

Bauliche Gegebenheiten

Es gibt für den Betrieb von PC-Räumen und Servern Regeln, die ein ordnungsgemäßes Funktionieren der Technik garantieren sowie die Manipulation der Hardware verhindern sollen. Dazu gehören:

- abschließbare Türen und verschließbare Fenster, Maßnahmen gegen Einbruchsdienstahl und Vandalismus
- Einhaltung der Brandschutzvorschriften
- eindeutige Regelungen für die Nutzung der Räume

Weitere Informationen finden sich im IT-Grundschutzhandbuch in Schicht 2 (Infrastruktur) und Schicht 3 (IT-Systeme).