Szenario

Das Netzwerk des fiktiven Schulungsunternehmens „*TeachMePlz GmbH*“ beinhaltet einen Intranet-Webserver, auf dem sich eine web-basierte Schulungssoftware befindet und bietet den Kursteilnehmern auch die Möglichkeit einen verfügbaren Internetanschluss mit zu benutzen. In der Vergangenheit wurde dieses Angebot jedoch oftmals zu illegalen Zwecken missbraucht, was dem Unternehmen zuletzt einen Rechtsstreit einhandelte.

Überlegung und Implementation

Es kam die Idee auf, das Netzwerk neu zu designen und den Netzwerkzugang benutzergebunden zu implementieren. Ein Nutzen dieser Maßnahme wäre, dass nur noch angelegte und legitimierte Benutzer Zugriff auf das Netzwerk erhalten. Daraufhin ließe sich im Falle einer wiederholten illegalen Nutzung der zur Verfügung gestellten Internetverbindung nachvollziehen, welcher Benutzer hierfür zur Rechenschaft gezogen werden muss. Hierfür muss jedoch eine rechtliche Absicherung des Unternehmens in Form von neuen Allgemeinen Geschäftsbedingungen erfolgen. Zur Authentifizierung der Teilnehmer wird auf der Firewall eine Erweiterung installiert, die für den Netzwerkzugriff einen Abgleich mit einem Authentifizierungsserver (*dem quelloffenen freeRADIUS*) durchführt. Dieser wird so konfiguriert, dass er basierend auf einer von der Administration stets gepflegten Benutzerdatenbank den Zugriff gestattet oder verbietet.

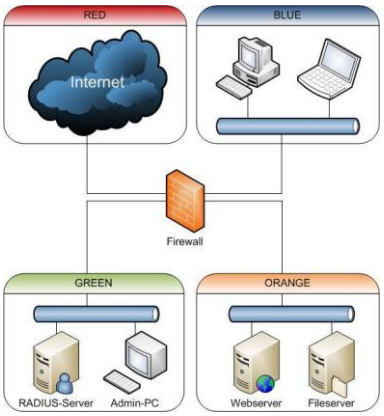

Abbildung 1: Netzwerkplan des neu designten Netzwerks

Das Netzwerk wird in verschiedene Subnetze geteilt: **ROT** (*Internet*), **GRÜN** (*Sicheres Netz mit RADIUS-Server und Verwaltungsrechner*), **ORANGE** (*Demilitarisierte Zone mit Intranet-Webserver*) und **BLAU** (*Fremdrechner der Teilnehmer*). Die Firewall wird so konfiguriert, dass sie sämtlichen Netzwerkverkehr blockiert – es werden lediglich Ausnahmen für die TCP-Kommunikation auf **Port 80** zwischen dem **ROTEN**, **ORANGENEN** und **BLAUEN** Netzwerk konfiguriert.

Wenn von einem Rechner aus dem **BLAUEN** Netzwerk nun eine Anfrage aus dem Webbrowser heraus erfolgt, wird der Benutzer auf eine Anmeldeseite weitergeleitet und muss dort seine Login-Daten eingeben. Stimmen Benutzername und Passwort, wird der Zugriff erlaubt und die Anfrage weitergeleitet. Bis der Benutzer sich über ein geöffnetes Popup-Fenster abmeldet erfolgen sämtliche Anfragen über sein Benutzerkonto.

Internetverweise

- Vollständiger Artikel in meinem Wiki zur Implementation: **http://st-devel.net/secop**
- Projekt-Seite des IPCop-Projekts (*Firewall*): **http://www.ipcop.org**
- Sperren von ausgehendem Netzverkehr unter IPCop mithilfe von „*BlockOutTraffic*“: **http://www.blockouttraffic.de**
- Internetseite des freeRADIUS-Projekts: **http://www.freeradius.org**