ProxyScan
Viren scannen am Web-Proxy

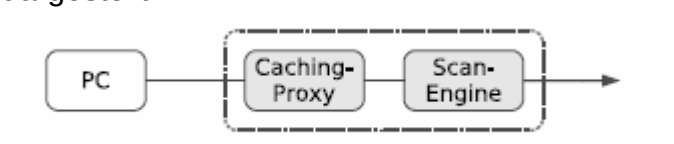
Jeder Download von Software oder anderen Dateien aus dem Internet birgt die Gefahr, dass sich darunter infizierte Dateien befinden können, die geöffnet oder auf dem lokalen Computer ausgeführt zu einer Infektion des Systems führen und sich von dort aus im lokalen Netzwerk ausbreiten. Abhilfe dagegen ist z.B. die Verwendung einer Scan-Engine in Kombination mit einem Caching-Proxy. Im Folgenden wird die an der Universität Innsbruck eingesetzte Methode beschrieben (Grundlage ist das Dokument von **Wolfgang Barth** http://linux.swobspace.net/books/fw/proxyscan/proxyscan.pdf).

Grundprinzip

Über eines muss man sich im Klaren sein: ein gescannter Datenstrom bietet nicht die gleiche Zugriffsgeschwindigkeit wie ein direkter, ungefilterter Zugriff auf das Internet. Um dennoch eine gute Performance beim Surfen im Internet unter Einbindung eines Virenscanner zu erreichen, sind die folgenden 3 Punkte zu beachten:

- *Leistungsfähige Hardware (http://www2.uibk.ac.at/zid/systeme/unix-hosts/v240/proxy.html)*
- *Nur neue Dateien scannen*: speichert man bereits geprüfte Dateien zwischen („Caching“), müssen nur noch unbekannte Dateien geprüft werden, was bei wiederholtem Zugriff auf die gleichen Dateien einen erheblichen Performance-Gewinn bedeutet.
- „*Sichere Dateien“ nicht scannen*: Dateien oder Dateitypen, die als „sicher“ eingestuft werden, werden vom Virenscan ausgeschlossen (in der Regel die MIME-Typen text/html, text/plain, image/gif, image/jpeg und image/png).

In der nachfolgenden Abbildung ist das Grundprinzip für den Virenscan beim Websurfen dargestellt.



Der Anwender greift von seinem Computer aus zunächst auf dem Caching-Proxy zu. Bereits dort abgelegte Dateien sind mit lokaler Netzwerkgeschwindigkeit direkt verfügbar. Der Proxy wird so eingestellt, dass er nicht vorhandene Dateien immer über die Scan-Engine holt. Die Scan-Engine überprüft, ob es sich um einen Dateityp handelt, der als „sicher“ gilt, alle anderen Dateien werden erst auf Viren untersucht, bevor diese an den Browser weitergereicht werden.

Verwendete Methode: Apache2 und mod clamav

(http://software.othello.ch/mod clamav/ und http://www.clamav.net/)

Der Apache2-Server wird im Proxy-Modus als Parent für den Squid (Proxyserver) betrieben. Das Modul *mod clamav* wird direkt in Apache2 eingebunden und benutzt die Library des Virenscanners Clamav (dann muss kein externes Programm aufgerufen werden).

Die Vorteile der verwendeten Lösung sind:

- Direkte Einbindung in Apache, Aufruf externer Skripte oder Programme entfällt.
- Funktionaler OpenSource-Virenscanner Clamav
- Erkennung von „sicheren Dateien“ über MIME-Typen, URLs und Pattern möglich.
- Ausführliche Dokumentation

Beispiel für einen gefundenen Virus