Zentrale Paketfilter

J.-U.Winks
winks@cms.hu-berlin.de

Die HU betreibt ein relativ offenes Netz. Dieses ist immer mehr Angriffen ausgesetzt, Attacken auf Rechner und Dienste nehmen zu. Um dem zu begegnen, hatte das Rechenzentrum bereits vor einiger Zeit eine Routerpolicy eingeführt und betreibt einen Router mit Firewall-Funktionalität.

Was tun wir?

Anfang 2002 wurde eine aktive Komponente im Netz der HU ausgetauscht. Es handelte sich um den WiN-Router, welcher die HU ans Internet anbindet. Dieser wurde gegen ein neueres Modell ausgewechselt.

Der alte Router vom Typ Cisco 7500 hatte Filterregeln, die nur bestimmte Protokolle gefiltert haben und den Rest des Verkehrs, der von außen kam, durchließen. Dieses Prinzip wurde mit dem Austausch umgekehrt und damit eine neue Routerpolicy angewandt.

Das Regelwerk des neuen Routers bestimmt nun die Protokolle, die von außen kommen und ins HU-Netz dürfen. Der restliche Verkehr aus externen Netzen wird abgeblockt.

Den in dieser Policy erlaubten Protokollen sind Standard-Anwendungen zugeordnet. Darunter fallen Protokolle wie z. B. SSH und HTTP.

Weiterhin wird fast alles, was von innen kommt, also aus dem HU-Netz herausgeht, durchgelassen. Ausnahmen bilden die bekannten Ports von Tauschbörsen. Der Verkehr der Gegenrichtung, also alles, was aufgrund einer internen Initiierung an Verkehr zurückkommt, wird ebenfalls ins HU-Netz hereingelassen.

Und natürlich gibt es jede Menge Ausnahmen. Einige Administratoren haben Server, auf denen Anwendungen laufen, die Nicht-Standard-Ports benutzen. Des Weiteren gibt es Anwender, die ihre speziellen Anwendungen und Dienste auch von anderen Netzen aus erreichen möchten. Diese Ausnahmen sind natürlich regelbar und mit dem CMS zu vereinbaren.

Es gab damals mehrere Gründe, die Policy zu ändern. So wurde beispielsweise mit der Einführung und Umsetzung einer solchen Policy das Sicherheitsniveau angehoben. Das spart letztendlich Arbeitszeit und Nerven, nicht nur im CMS, sondern auch bei den Anwendern und Administratoren in den Einrichtungen.

Weiterhin erreichte der kostenpflichtige Internet-Verkehr damals zum Zeitpunkt der Änderung eine kritische Marke. Mit der Einführung der Policy wurden bekannte Ports von Tauschbörsen blockiert, was eine Reduzierung des Gesamtverkehrsaufkommens um knapp 30 Prozent brachte.

An der Policy wird ständig geschraubt und gefeilt, es finden laufend Ergänzungen statt. So wird die Kommunikation bestimmter Dienste nur noch zielgerichtet bestimmten Servern erlaubt, so wie es z. B. beim SMTP-Protokoll realisiert wurde. Hier dürfen nur noch bestimmte Server auswärtige kontaktieren bzw. von diesen kontaktiert werden.

Bei anderen Diensten wird zumindest über gleichartige Restriktionen nachgedacht.

Was tun wir nicht?

Oder was können wir nicht tun.

Natürlich ist so eine zentrale Firewall immer nur ein erster Schritt, um ein Netz abzusichern. Sie kann am Eingang eines großen, offenen Netzes immer nur eine grobe Filterung vornehmen. Das Feintuning muss an anderer Stelle geschehen, denn es gibt zu viele Ausnahmen und viel zu viele Protokolle, die zunächst ungefiltert ins Netz gelangen.

Weiterhin schützt eine Eingangsfirewall nicht vor Attacken, die aus dem internen Netz kommen. Es gibt offene Zugangspunkte, wie beispielsweise Einwahlknoten, offene Dosen, PC-Pools, über die (auch unbeabsichtigt) Attacken oder Angriffe laufen können. Eine Firewall kann auch nicht das Einschleppen von Viren und Würmern verhindern, wenn diese über mobile, schlecht gewartete Laptops, also quasi an der Firewall vorbei, ins Netz gelangen.

Einrichtungen, die für sich selbst einen erweiterten Schutzbedarf sehen, sollten über eine Institutsfirewall nachdenken. Der CMS unterstützt an dieser Stelle gerne in beratender Weise.

Und letztlich entbindet eine zentrale Firewall den Nutzer eines Rechners oder den Administrator eines Servers nicht von der Pflicht, sorgfältig mit seinem System oder seinen Diensten umzugehen. Anwendern, die für ihren PC ein hohes Schutzbedürfnis sehen, ist eine Personal Firewall zu empfehlen. Hier gibt es verschiedene, auch frei nutzbare Produkte, z. B. ZoneAlarm oder die Kerio Personal Firewall. In Verbindung mit einem aktuellen Virenscanner und einem aktuellen Patchlevel ist so ein System nur schwer angreifbar.

Was planen wir?

Auch in diesem Bereich befindet sich der CMS in einer Umstellungsphase. Es gibt verschiedene Ansätze, die verfolgt werden. Sie reichen vom angedachten Einsatz von Highend-Systemen bis hin zu kostengünstigen, kleineren Systemen.

Der CMS wird den Netzzugang verschiedener kleinerer Netze, wie z. B. das Netz der Gebäudeleittechnik, mittels Firewall vom übrigen Netz separieren. Hier werden kleinere Systeme beschafft und der Zugang zu diesen Netzen über VPN realisiert. Ebenso ist geplant, demnächst wichtige zentrale Server im CMS hinter einer separaten Firewall zu platzieren.