Firewalls im Zusammenhang einer Sicherheitsarchitektur

Firewalls gehören heutzutage zu den entscheidenden Basistechnologien zum Schutz vor Angriffen im Internet. Die grundlegende Aufgabe einer Firewall ist, vereinfacht formuliert, die Trennung des sicheren internen Netzwerks von der unsicheren Außenwelt. Dort wo ausreichende Schutzmaßnahmen fehlen, werden nicht nur die eigenen Systeme gefährdet. Vielfach wird nicht mit in Betracht gezogen, dass von Systemen, für die ein Schutz durch eine Firewall nicht für notwendig erachtet wird, meist auch andere Kommunikationspartner gefährdet werden. Daher kann eine Verbindung zum Internet ohne zusätzliche Schutzmaßnahmen (u.a. Firewalls) als grob fahrlässig gewertet werden.

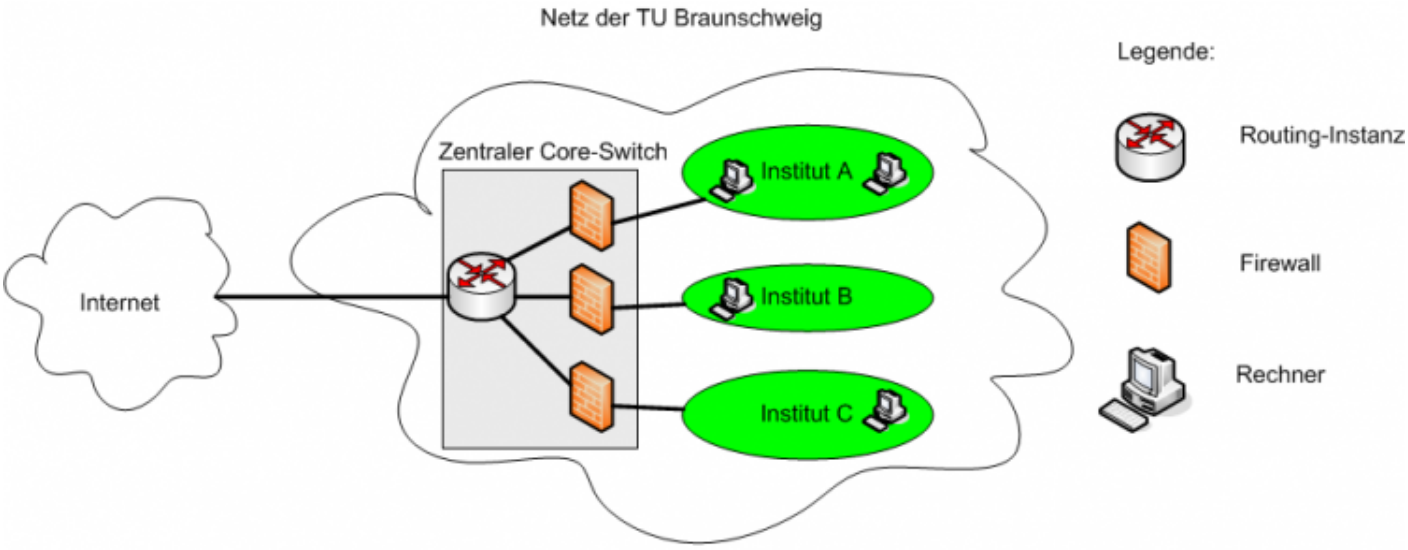

Abb. 1: Zentral bereitgestellte Firewall zum Schutz der Netze von Instituten innerhalb der Netzinfrastruktur der TU Braunschweig

Mehrstufige Sicherheitsstrukturen

Zur Realisierung von Firewall-Funktionalitäten gibt es verschiedene Ansätze. Sogenannte Paketfilter werden in Form von sogenannten Access Control Lists (ACL) auf Routern abgebildet. Die Regelwerke dieser ACLs sind statisch und berücksichtigen lediglich Angaben von Quelle und Ziel bei Ports und IP-Adressen sowie ggf. Einschränkungen auf Protokollgruppen (TCP, UDP und ICMP). Vorteile durch hohe Geschwindigkeit bei der Filterung durch ein statisches Regelwerk sind heutzutage jedoch nur noch bedingt zutreffend. ACLs werden daher meist nur noch als Ergänzung eingesetzt, so auch an der TU Braunschweig.

Zusätzlichen Schutz sollen sogenannte Personal Firewalls bieten, die Sie als DV-Koordinator auf den von Ihnen betreuten Rechnern einsetzen sollten. Ein auf dem eigenen Betriebssystem basierter Schutz (Stichwort: Windows- oder Personal Firewall, unter Linux „iptables“), ist als sinnvolle, aber lediglich zusätzliche Maßnahme zu sehen. Sie ergänzt eine obligatorische Anti-Virus-Lösung für Ihre Rechner und ist wie diese ein weiterer Teil eines Gesamtschutzes. Personal Firewalls und Anti-Virus-Lösungen bergen die Gefahr, dass sie durch Benutzerhand bewusst oder unbewusst deaktiviert werden und sind Ziel von Angriffen durch Trojaner und Viren.

Daher stellt eine eigene Firewall für Ihr Institutsnetz ein zentrales Element Ihrer Sicherheitsstrategie dar. Moderne Firewalls arbeiten nach dem sogenannten „stateful inspection“ Verfahren, so auch die zentrale Firewall-Infrastruktur an der TU Braunschweig. Weitere Schutzmaßnahmen auf organisatorischer und technischer Ebene sind zusätzlich anzustreben.

Revision #1
Created 15 May 2024 13:09:30 by Tina Strauf
Updated 15 May 2024 13:19:08 by Tina Strauf