

Aufgabe 1:

Sicherheitspolitiken

Im Rahmen der letzten Lehrveranstaltung wurden Sicherheitspolitiken als ein zentraler Bestandteil von Firewalls bzw. ganz allgemein von gegen Angriffe zu schützenden IT-Infrastrukturen dargestellt. Informieren sie sich über die Folien, die benannte Literatur und insbesondere das Grundschutzhandbuch des BSI¹ zur Wiederholung nochmals kurz über die wichtigsten, im Rahmen einer Sicherheitspolitik zu beantwortenden Fragen und bearbeiten sie die folgenden Aufgabenstellungen:

1. Führen sie für ein Rechnernetz ihrer Wahl (z.B. das Netz der FHB im WWZ) eine Strukturanalyse durch.
2. Wie ist der Schutzbedarf der einzelnen Komponenten bzw. Komponentengruppen des Netzwerks?
3. Erstellen sie gruppenorientierte Kommunikationsprofile für die Benutzer des Netzwerks.
4. Welche Komponenten des Netzes werden bereits durch Sicherheitskomponenten geschützt? Was leisten diese Komponenten? Wo besteht zusätzlicher Handlungsbedarf?
5. Überlegen sie sich für jede Schnittstelle ihres Netzes zu einem Netz mit anderem Schutzbedarf eine Sicherheitsstrategie.
6. Falls sie Firewalls einsetzen wollen: Welche Art von Filtersystem soll eingesetzt werden? Begründen sie ihre Entscheidung. Geben sie einige Filterregeln (Syntax: Deutsch) als Beispiele an.

¹siehe <http://www.bsi.bund.de/gshb/deutsch/index.htm>

Aufgabe 2:

Router-Sicherheit

Auf der Homepage der NSA finden sie den *NSA/SNAC Router Security Configuration Guide*². Die kurze *Executive Summary Card* enthält eine Reihe von Hinweisen zur Konfiguration von *Cisco* Routern. Bearbeiten sie hierzu die folgenden Aufgabenstellungen:

1. Bekommen sie heraus, was die Einstellungen unter „Specific Recommendations: Router Access“, Punkte 1 bis 3, bewirken.
2. Untersuchen sie die unter „Specific Recommendations: Access Lists“, Punkte 4, 5 und 6 gemachten Vorschläge. Welche Angriffe können dadurch vermieden werden?
3. Im gleichen Abschnitt unter Punkt 9 finden sich einige Beispielregeln. Welche ICMP-Dienste werden dadurch unterbunden? Warum ist es wichtig, diese Dienste zu blockieren? Warum kann nicht die gesamte ICMP-Protokollfamilie blockiert werden?
4. Was können sie gegen direkte Angriffe gegen einen Router oder eine Firewall machen? Durch welche zusätzlichen Sicherheitsmechanismen können sie ihre Infrastruktur für den Fall schützen, daß ein Router oder eine Firewall kompromittiert wurde? Was müssen sie dabei möglicherweise in Kauf nehmen?

²siehe <http://www.nsa.gov/snac/> bzw. http://www.nsa.gov/snac/routers/cisco_exec_sum.pdf