Gruppenübung zum Thema „Firewall“: Internet-Anschluß für das Krankenhaus „KliniX“

Lösungshinweise zu Teil 2 – Beurteilung einer bestehenden Firewall

(wird nicht abgegeben!)

Aufgabe 1

Stärke des Schutzes:

- Ein Paketfilter alleine ist sicher nicht stark genug, um die hohen Anforderungen eines Spitals gerade punkto Vertraulichkeit und Integrität der Daten zu gewährleisten.
- Je nach Budget und Verfügbarkeit von Personal zur Wartung der Firewall Lösung empfiehlt sich gegen aussen mindestens die Variante „Screened Subnet mit Single Homed Application Gateway“. Da böswilliges Verhalten von innerhalb des Krankenhausnetzes nicht grundsätzlich ausgeschlossen werden kann, empfiehlt sich sogar die symmetrische Variante Screened Subnet mit Multihomed Application Gateway“. Siehe dazu die drei vorgeschlagenen Varianten im Handout.

Untergliederung in unterschiedliche Schutzzonen:

- In der Ausgangslage wird nur unterschieden zwischen krankenhausintern und –extern. Dies entspricht absolut nicht den unterschiedlichen Schutzanforderungen. Mindestens die Datenbanken sind vom Rest des Intranets zu trennen.
- Je nach Budget und Verfügbarkeit von Personal zur Wartung sind Bereiche mit unterschiedlichen Sicherheitsanforderungen möglichst zu trennen. Idealerweise erhält jeder derartige Bereich auch eine eigene, abgeschlossene Zone im Intranet. Siehe dazu die drei vorgeschlagenen Varianten im Handout.

Angreifbarkeit der Firewall selbst:

- In der vorgegeben Konfiguration laufen diverse Dienste auf dem gleichen Gerät wie die Firewall. Jeder dieser Dienste kann Sicherheitslücken enthalten und ist somit ein potentieller Schwachpunkt, um die Firewall und das Intranet anzugreifen. Je mehr Dienste auf der Firewall laufen, desto grösser wird die Gefahr, dass solche Schwachpunkte vorliegen und ausgenutzt werden. Im Idealfall laufen also überhaupt keine anderen Programme auf der Firewall.
- Die hier gezeigten Dienste gehören in die demilitarisierte Zone des Eingangsbereiches (gelb in den vorgeschlagenen Lösungsvarianten).

Aufgabe 2

Im ersten Teil dieser Firewall Lektionen kommt eine ganze Liste mit Gefahren vor, die nicht mit einer Firewall abgesichert werden können. Ziel dieser Frage ist es, diese Gefahren konkret am Beispiel des Krankenhauses durchzudenken. Diese reichen vom böswilligen Patienten, der die Computer mit Viren verseuchen will, über den schussligen Arzt, der die Patientendaten falsch eingibt bis hin zum Wasserschaden, der die Datenbank vernichtet. Je nach Zeit, die zur Verfügung steht, können für jede von den Schülern vorgebrachte Gefahr Lösungen vorgeschlagen und diskutiert werden. Falls dies geschieht, so sind derartige Lösungen immer im Kontext der vorliegenden Firewall Aufgabe einzugliedern.