Partnerübung zum Thema „Firewall“

Internet-Anschluß für das Krankenhaus „KliniX“

Teil 1 – Beurteilung des Einsatzes einer Firewall

Fallbeispiel

Aufgrund der zunehmenden Bedeutung des Internets in der Medizin, wurde vor kurzem entschlossen, das Krankenhaus „KliniX“ an das Internet anzubinden.

Bislang haben berechtigte Sicherheitsbedenken die Verantwortlichen von einem Anschluß absehen lassen: Mit einem Internetanschluss sind die Daten des Spitals erhöht vor unbefugtem Einblick oder Manipulation gefährdet. Das Krankenhaus hat jedoch hohe Datenschutzanforderungen, insbesondere im Bereich der Patientendaten.

Mit geeigneten Massnahmen und Technologien, insbesondere einer Firewall-Lösung, soll nun die sichere Anbindung an das Internet gewährleistet werden.

Hinweise zur Übung

Die Übung ist in zwei zusammenhängende Teile gegliedert, welche sich je auf eine der zwei Lektion beziehen. Im vorliegenden Teil geht es um die Funktion und Wirkung von Firewalls, sowie das Thema Sicherheitspolitik. In Teil 2 wird es darum gehen, eine geeignete Firewall-Lösung auf der technischen Ebene zu diskutieren.

Die folgenden Aufgaben sind in Zweiergruppen zu lösen. Halten Sie Ihre Ergebnisse stichwortartig fest.

Am Schluss werden die Ergebnisse in der Klasse besprochen.

Aufgabe 1: Funktion und Grenzen von Firewalls

a) Einigen Sie sich auf zwei zentrale Gründe, im vorliegenden Fall eine Firewall einzusetzen.

b) Während des Projektverlaufs wurde im Rahmen einer Gefahrenanalyse auf verschiedene Schwachstellen und Gefahren hingewiesen. Im folgenden sind drei davon aufgeführt.

Kann eine Firewall zum Schutz vor diesen Gefahren eingesetzt werden? Falls ja, welcher Typ (Packet Filter, Application Gateway)? Begründen Sie Ihre Antwort stichwortartig.

i. Implementierungsfehler einer Anwendung nutzen: In den vergangenen Jahren wurden beim Mail-Transport-Agent-Programm (MTA) „sendmail" mehre Sicherheitslücken entdeckt, die es ermöglichten, auf dem entfernten Rechnersystem beliebige privilegierte Kommandos ausführen zu lassen, mit denen Angriffe durchgeführt werden konnten.

ii. Source IP Address Spoofing: Es sind Attacken bekannt, bei denen der externe Angreifer seine IP-Absenderadresse fälscht und eine IP-Adresse eines internen Rechners des geschützten Netzes verwendet. Werden Dienste angeboten, die zur Authentisierung nur die IP-Adresse nutzen (z.B. NFS), kann ein Angreifer mit dieser Methode Zugang zu diesen Services erlangen. Insbesondere bildet IP-Spoofing die Grundlage für zahlreiche weitere Angriffe, wie z.B. SYN-Flooding.

iii. Analyse des Netzes und der Rechnersysteme: Es können z.B. mit Hilfe des „ping"-Befehls die aktiven IP-Adressen eines Netzwerk analysiert werden, indem ein Angreifer „ping"-Befehle an alle möglichen IP-Adresse des Adressbereichs schickt.

c) Beschreiben sie mindestens 3 Schwachstellen, resp. Angriffsmöglichkeiten, welche für das Spital im Zusammenhang mit der „IT-Security" relevant sind, wogegen eine Firewall jedoch wenig oder keinen Schutz bietet.

Aufgabe 2: Sichheitspolitik

a) Vor der Einführung der Firewall wurden im Spital in gemischten Arbeitsgruppen Sicherheitsanforderungen diskutiert. Ein Auszug erster Ideen ist der untenstehenden Tabelle abgebildet.

Im folgenden finden Sie die in der Lektion besprochenen Inhaltsbereiche einer Sicherheitspolitik (vgl. auch Folie „Erstellung der Sicherheitspolitik und folgende). Finden Sie zu jedem dieser fünf Bereiche jeweils eine Notiz, welche sich zu diesem zuordnen lässt.

S: Sicherheitsforderungen
K: Kommunikationsanforderungen
O: Massnahmen: Organisation
P: Massnahmen: Personal
I: Massnahmen: Infrastruktur

No.	Notiz
1	Datenschutz und Schweigepflicht erfordern, dass ausserhalb des durch den Firewall geschützten Bereiches keine personenbezogenen Daten ungeschützt gespeichert, verarbeitet oder übermittelt werden dürfen.
2	Die Informationsangebote des Spitals für externe Stellen sollen via Web-Dienst bereitgestellt werden können.
3	Werden via Web sensitive (z.B. personenbezogene) Daten bereitgestellt, so ist ein wirksamer Zugriffsschutz mit verschlüsselte Verbindung einzurichten, damit Informationen und Passwörter gesichert übertragen werden.
4	Aktive Inhalte wie Java und ActiveX dürfen nicht übertragen werden.
5	Die Nutzung von E-Mail soll für bestimmte Mitarbeitergruppen möglich sein.
6	Bei ausgehender Mail sind Datenschutz und die ärztliche Schweigepflicht zu beachten. Ein entsprechendes Verbot sollte in die Verpflichtungserklärung für Mitarbeiter aufgenommen werden.

No.	Notiz
7	Für eingehende Mail ist ein Filter gegen Schadprogramme („Viren-Filter“) einzurichten.
8	Es ist zu beachten, dass die codierte (z. B. chiffrierte) Zusendung von Viren und anderen Schadprogrammen von außen z.T. nicht erkannt werden können. Deshalb sollen alle E-Mail-Berechtigten über diese Gefahr informiert werden und nicht unbedacht Programme, Macros o. ä. starten, die auf diesem Weg zu ihnen gelangt sind.
9	Es sollen alle Dienste gesperrt werden, welche nicht explizit erlaubt sind.
10	Für den Betrieb der Firewall ist die IT-Abteilung verantwortlich. Detaillierte betriebsintern Richtlinien und Zuständigkeitsregelungen sind zu definieren.
11	Die Systemverwaltung der Firewall-Komponenten soll über einen gesicherten Zugang erfolgen.
12	Da der Application Gateway-Rechner aus Sicherheitsgründen möglichst einfach gehalten werden soll, ist dieser nicht mit Server-Prozessen (z.B. Web-Dienst) zu belasten.
13	Individuelle Verbindungen, welche die Firewall umgehen, sind zu verhindern.

b) Gibt es in der obigen Tabelle einen wichtigen Punkt der in die Sicherheitspolitik aufgenommen werden müsste und hier ausser Acht gelassen wurde? Hinweis: vgl. hierzu die Folie „Erstellung einer Sicherheitspolitik“ und folgende.

c) Nehmen wir an, das Firewall-System soll mit Logging-Funktionalität ausgerüstet werden. Welche Art Daten würden Sie protokollieren, und warum? Nennen Sie mindestens 2 Punkte.