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

Lösungshinweise zu Teil 1 – Beurteilung des Einsatzes einer Firewall

Aufgabe 1

a)

- Reduzierte Angriffspunkte durch die Abschottung interner Systeme
- Effiziente Umsetzung der Sicherheitspolitik an zentraler Stelle
- Vollständige und einfache Protokolliermöglichkeit der gesamten Kommunikation
- etc.

b)

i. Angreifbare Programme auf Rechnersystemen im zu schützenden Netz (wie Sendmail) können durch ein Application Gateway mit einem Proxy (Stellvertreter) entkoppelt werden. Dadurch ist gegen aussen nur der Proxy sichtbar, welcher eine zweite Verbindung nach innen herstellt. Sendmail ist so nicht mehr direkt erreichbar und die geprüfte Minimalsoftware (Proxy) bietet idealerweise keine Angriffsmöglichkeit.

ii. Die aktuelle IP Version bietet keine Möglichkeit IP-Spoofing komplett zu verhindern. Es können allerdings Pakete vom externen Interface (Input Filter) verworfen werden, welche als Source-Adresse eine Adresse des internen Netzwerkes besitzen. Dazu muss ein Paketfilter unterschieden können, von welcher Seite ein Paket stammt.
Begriffserklärung zu Tcp-Syn-Flooding: Bei TCP Verbindungen erfolgt ein sogenannter Three-Way-Handshake zum Verbindungsaufbau. Das Client-Programm startet den Verbindungsaufbau durch Senden einer SYN-Nachricht zum Server. Der Server bestätigt den Empfang dieser Nachricht durch eine SYN, ACK-Nachricht, die wiederum der Client mit ACK bestätigt. Die Verbindung ist nun aufgebaut. Beim Tcp-Syn-Flooding Angriff sendet der Client die letzte ACK-Nachricht nicht und es entsteht eine halb offene Verbindung. Durch ständiges Erzeugen solcher Verbindungen kann ein System lahm gelegt werden.

iii. Ein Ping erfolgt via ICMP als "Echo Request", der mit Type=8 verschickt wird (vgl. Abbildung: Format der ICMP Echo-Anforderung/Antwort). Entsprechende Pakete von aussen können mit einem Paketfilter verworfen werden. Hinweis: ICMP-Daten werden immer mit einem vollständigen IP-Header verschickt.

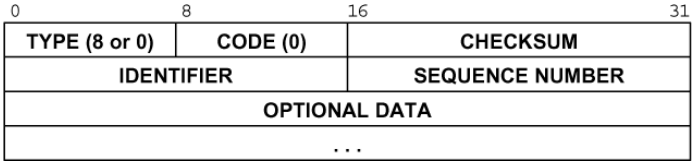

Abbildung: ICMP Echo-Anforderung/Antwort

c)

- Am sichersten ist gar keine Verbindung! Eine Netz mit extrem heikler Information soll nicht mit dem Internet verbunden werden.
- Eine Firewall kann zwar einen Netzübergang sichern, sie hat aber keinen Einfluß auf die Sicherheit der Kommunikation innerhalb dieser Netze.
- Es werden Protokolle überprüft, nicht die Inhalte. Eine Protokollprüfung bestätigt beispielsweise, daß eine E-Mail mit ordnungsgemäßen Befehlen zugestellt wurde, kann aber keine Aussagen zum eigentlichen Inhalt der E-Mail machen.
- Attacken, welche die Firewall umgehen (z.B. Diskette, via Modem, etc.).
- Die Filterung von aktiven Inhalten ist unter Umständen nur teilweise erfolgreich. z.B. Viren, wenn sie verschlüsselt eingeschleust werden.
- Angriffe und Fehler auf der Ebene der Anwendungssoftware.
- Menschliches Versagen, Social Engineering.
- Neue oder unbekannte Gefahren.
- Bei statischen Paketfilter: Richtung des Verbindungsaufbaus bei UDP.

- Sobald ein Benutzer eine Kommunikation über eine Firewall herstellen darf, kann er über das verwendete Kommunikationsprotokoll beliebige andere Protokolle tunneln. Damit könnte ein Innentäter einem Externen den Zugriff auf interne Rechner ermöglichen.
- Eine Einschränkung der Internetzugriffe auf festgelegte Webserver ist in der Realität unmöglich, da zu viele WWW-Server auch als Proxies nutzbar sind, so daß eine Sperrung bestimmter IP-Adressen leicht umgangen werden kann.
- Die Filterung von Spam-Mails ist noch nicht ausgereift. Keine Firewall kann zweifelsfrei feststellen, ob eine E-Mail vom Empfänger erwünscht ist oder nicht. Spam-Mails dürften erst dann verschwinden, wenn die Absender zweifelsfrei nachweisbar sind, was noch einige Zeit dauern wird.
- Firewalls schützen nicht vor allen Denial-of-Service-Attacken.
- etc.

Aufgabe 2

a)

	Zum Beispiel:
S: Sicherheitsforderungen:	1
K: Kommunikationsanforderungen:	2
O: Massnahmen: Organisation:	10
P: Massnahmen: Personal:	6
I: Massnahmen: Infrastruktur:	12

b)

- Regelungen zur Protokollierung von sicherheitsrelevanten Ereignissen
- Anforderung zum ständigen Beobachtung und Behebung von neuen Sicherheitslücken
- Personalaspekte im Bereich Security Management
- etc.

c)

- Fehlerhafter Authentikationsprozess (falscher Benutzername und/oder Passwort, mehrere Versuche, etc.)
- Verstoss gegen Regelwerk (unerlaubte Kommandos, Dienste, Zeiten, etc.)
- Angriffe auf Firewall-System selber (Fehlerhafte Authentikation, Überschreitung des Füllstands eines Logbuches, etc.)
- Nicht vorgesehenes Fehlverhalten der Firewall (Defekte der Hardware, Softwarezustand, etc.)
- Speicherung ausgewählter zulässiger Aktionen (z.B. Zugriff auf geschützten Bereich)
- Aktivitäten mit dem Security Management (Rechtevergabe, Logbuch löschen, etc.)
- etc.