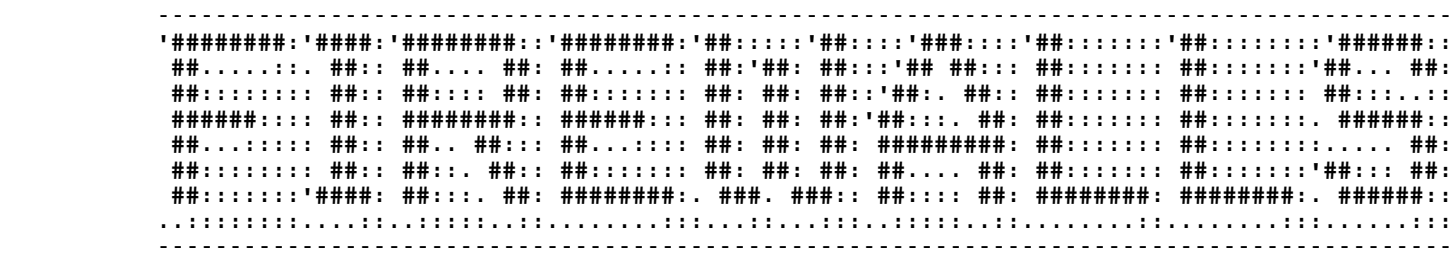

Vortrag auf dem Treffen der Lugrav am 29.10.2009
von Peter Voigt / Bielefeld

Was bewirkt eine Firewall auf technischer Ebene?

- Sie blockiert Netzwerkverkehr aus dem Netz *vor* der Firewall, der an Rechner *hinter* der Firewall gerichtet ist.
- Was blockiert wird, bestimmen Regeln, die der Administrator der Firewall vorgibt.
- Was für Regeln möglich sind, richtet sich nach dem Bautyp der Firewall (siehe unten).
- Die Schutzwirkung der Firewall hängt von ihrem Bautyp und der jeweiligen Konfiguration der Regelsätze ab.
- Eine Firewall kann den Netzwerkverkehr in alle Richtungen gleichzeitig kontrollieren.
- Manche Firewalls bieten weitergehende Möglichkeiten, z.B. das Umlenken, Protokollieren, Umverpacken oder Reparieren von Paketen, die sicherheitstechnische Optimierung aktiver Verbindungen, das beliebige Manipulieren der übertragenen Nutzdaten oder die Möglichkeit, danach zu filtern, welches Betriebssystem auf dem Quellrechner läuft.

Wie kann eine Firewall die Sicherheit eines Netzwerkes verbessern?

- Eigene Rechner mit offenen Ports können davor bewahrt werden, von fremden Rechnern überhaupt nicht oder zumindest nicht auf unerwünschte Weise kontaktiert zu werden.
- Fremde Rechner können davon abgehalten werden, von eigenen Rechnern kontaktiert zu werden, so dass ihre Existenz verborgen oder zumindest der Abfluss von Informationen behindert werden kann.

Wer braucht eine Firewall?

- Jeder Desktop-User, der nicht überschaut, welche Ports auf seinem Rechner offen stehen und welche Folgen das auslöst.
- Wer in seinem Netzwerk irgendwelche Netzwerkdienste ausprobieren, sprich Ports öffnen will, ohne gleich befürchten zu müssen, fremden Rechnern den Zugriff auf die eigenen Rechner zu ermöglichen.
- Wer auf Rechnern in seinem eigenen Netzwerk bestimmte Netzwerkdienste für die Außenwelt anbieten will, d.h. Ports öffnen will, ohne gleich den Zugriff auf das eigene Netzwerk schrankenlos freizugeben.

Wo liegen die Grenzen des Schutzes durch eine externe Firewall?

- **Der Wahrnehmungshorizont der Firewall endet an ihrer Netzwerkkarte. Das hat Konsequenzen:**

  Was nicht an ihrer Netzwerkkarte vorbei fließt, nimmt die Firewall nicht wahr. Datenverkehr zwischen Rechnern, die nicht an der Netzwerkkarte der Firewall vorbeiläuft, kann von ihr nicht kontrolliert werden.

  Die Firewall erkennt allein, ob Pakete ankommen. Woher sie kommen, kann sie nur vermuten. Alle identifizierenden Merkmale der Pakete, insbesondere IP/MAC-Adressen und Sequenznummern lassen sich fälschen. Selbst die OS-Erkennung bleibt wackelig.

  Ebenso wenig erkennt eine externe Firewall, welche lokale Prozesse bzw. welche lokale Nutzer des Quellrechners Traffic erzeugt haben.

- **Ursprünglich dienten die Vorgänger der Firewalls als Routing Devices der Erleichterung des technischen Netzwerkbetriebes. Sicherheitsaspekte kamen erst später ins Spiel. Deshalb prüfen "normale" Firewalls Pakete nach rein technischen Kriterien. Die transportierten Nutzdaten spielen keine Rolle. Nach schädlicher Nutzlast wie Viren und Trojaner wird nicht gesucht. Ausnahmen bilden Firewalls mit DPI (und eingeschränkt Firewalls mit Proxies).**

- **Externe Firewalls behandeln jedes einzelne Paket (Stateless Inspection) bzw. jede einzelne Verbindung (Stateful Inspection) als isoliertes Ereignis. Sie bewahren keine Informationen über die Lebenszeit dieser Paketen/Verbindungen hinaus auf. Neuere Firewalls bieten an dieser Stelle rudimentäre Funktionen. Wer mehr will, ist auf Zusatz-Software angewiesen.**

- **Lässt eine Firewall auch nur ein Netzwerkprotokoll auf nur einem Port durch, lässt sich unerwünschter Datenverkehr in der zugelassenen Richtung kaum unterbinden. Denn man kann beliebige Netzwerkprotokolle als Nutzlast in anderen Protokollen verstecken (Huckepack-Verfahren,auch als Tunneling bekannt). Unerwünschte Verbindungsaufnahmen von außen nach innen sind möglich, wenn innen ein Rechner falsch konfiguriert oder von Schadsoftware befallen ist.**

- **Es gibt Angriffsvektoren, um sich in laufende Verbindungen einzuklingen, welche die Firewall bereits frei geschaltet hat. Laufende Verbindungen können daher unter Umständen von Fremden für schädliche Zwecke ausgenutzt werden.**

- **Es gibt Angriffsvektoren, um Rechner hinter der Firewall auszuspionieren, selbst wenn eingehenden Verbindungen blockiert werden (Firewalking).**

- **Gewisse sicherheitstechnische Mängel der "alten" Internet-Protokolle sind konstruktionsbedingt und können durch Firewalls selbst mit Zusatz-Software nur abgemildert werden.**

- **Werden der Firewall so viele Regelsätze oder so viele weitere Aufgaben aufgebürdet, dass die Hardware überfordert ist, kann Netzwerkverkehr unkontrolliert passieren. Das ist ein typisches Problem von Firewalls, die mit DPI, IDS oder IPS ausgestattet sind und auf hohe Netzlast treffen.**

Welche Maßnahmen bieten sich alternativ/begleitend an?

- **Bei der Auswahl des eigenen Desktop steht eine Frage im Vordergrund: Reichen die eigenen Kenntnisse und Fähigkeiten, das gewählte Betriebssystem sicher zu betreiben?**

  Die vorhandenen technischen Unterschiede der Betriebssysteme wirken sich in der Praxis kaum aus. Von Bedeutung ist eher, wie „beliebt" ein Betriebssystem bei bösen Hackern und Script-Kiddies ist:

Windos 7	**technisch ok, als beliebtes Angriffsziel gefährdet**
Mac OS X	**technisch ok, als seltenes Angriffsziel recht sicher**
Linux	**technisch ok, aber weil schwerer zu bedienen mitunter gefährdet**

- **Der Ausweg Live CD zeigt auch Tücken. Die Live CD muss sicher konfiguriert sein, was nicht immer der Fall ist. Automatische Service-Funktionen, nicht gesetzte Passworte, offenstehende Ports und der nach kurzer Zeit veraltete Patchlevel können ein Sicherheitsrisiko bilden.**

- **Keine Ports offen lassen, d.h. alle Prozesse ausschalten bzw. erst gar nicht starten lassen, die anderen Rechnern Dienste anbieten. Das verringert die Angriffsfläche der betroffenen Rechner. Softwarefehler in Anwendungen, die sich vom Desktop aus ins Internet verbinden (z.B. Browser), bleiben weiterhin gefährlich.**

- **Sich nicht darauf verlassen, was Handbuch oder graphische Oberfläche sagen. Insbesondere mittels 'netstat -anf inet' auf dem betroffenen Rechner oder noch besser mit 'nmap -T4 IP-Adresse' von einem anderen Rechner aus alle offenen Ports ermitteln.**

- **Rechner mit Internet-Anschluss vorsorglich als Opfer betrachten. Jeder Auffälligkeit nachgehen.**

- **Vorbeugend Schadensbegrenzung betreiben, d.h. die wirklich benötigten Netzwerk-Funktionen auf verschiedene Rechner verteilen. Nach Möglichkeit keine Geräte einsetzen, die mehrere Dienste bündeln (à la Fritsbox & Konsorten).**

- **Sicherheitsstufen definieren und das Netzwerk entsprechend aufteilen. Nach Möglichkeit Verbindungsaufnahmen aus einem Segment mit niedriger Sicherheit in eine Zone mit höherer Sicherheit via Firewall unterbinden. (Beispiel: Demilitarisierte Zone DMZ).**

- **Zeitnah alle neu erscheinenden Patches einspielen, um das Risiko von angreifbaren Softwarefehlern möglichst auf Zero Day Exploits zu begrenzen.**

- **Laufend loggen und regelmäßig Logfiles lesen !!!**

- **Das Netz *hinter* der Firewall als genauso gefährlich ansehen, wie das Netz *vor* der Firewall.**

Welche Vor- und Nachteile zeigen die verschiedenen Firewall-Typen?

- **Interne Firewall**
  - läuft auf dem zu schützenden Rechner
  - können lokale Prozesse filtern

- **Externe Firewall**
  - läuft auf externer Hardware
  - schwer angreifbar
  - Addons probematisch
  - Selbstbau leicht möglich
  - Open Source Fertig-Lösungen

- **Stateless Inspection**
  - veraltetes Konzept
  - prüft jedes Paket isoliert
  - Sicherheitsgewinn begrenzt

- **Stateful Inspection**
  - aktueller Standard
  - prüft zusammengehörende Pakete
  - Sicherheitsgewinn hoch
  - verständliche Howtos
  - Betrieb automatisch
  - ohne Addons kaum angreifbar

- **Proxies**
  Application Layer Firewall
  - Standard in administrierten Netzen
  - prüft auch Protokolle
  - agiert wie ein Stellvertreter
  - Sicherheitsgewinn recht hoch
  - erfordert Netzwerk Know how
  - Betrieb automatisch

- **DPI**
  Deep Package Inspection
  - für administrierte Netze
  - prüft auch die Nutzlast
  - Missbrauchsmöglichkeiten
  - erfordert Netzwerk Know how
  - Konfiguration und Betrieb aufwendig
  - Sicherheitsgewinn abhängig von Konfiguration und Betriebsweise
  - fehleranfällig
  - erfordert sehr leistungsfähige Hardware

- **IDS / IPS**
  Intrusion Detection System
  Intrusion Prevention System
  - für administrierte Netze (?)
  - beobachtet Zeitabläufe
  - erkennt Angriffsszenarien
  - bei überschaubaren Verhältnissen geringer Nutzen
  - erfordert Netzwerk Know how
  - aufwendiger Betrieb
  - sehr fehleranfällig
  - mitunter angreifbar
  - erfordert leistungsfähige Hardware

- **Personal Firewalls**
  - können lokale Prozesse filtern
  - ggfs. inklusive DPI, Sandbox, IDS, IPS, GUI
  - auf Win$-Rechnern beliebtes Angriffsziel
  - früher Einwände ob des Nutzwertes

- **Graphische Firewalls**
  - . als externe Firewall sinnvoll
  - . Trennung von Verarbeitung und Darstellung
  - . erfordert Netzwerk Know how
  - . hoher Sicherheitsgewinn in schwer überschaubaren Netzen

- **Hidden Firewalls**
  - . Bridges mit beliebiger Firewall
  - . Sicherheitsgewinn abhängig von verwendeter Firewall (also hohe Sicherheitsgewinne realisierbar)
  - . ohne eigene IP-Adresse kaum angreifbar
  - . einsetzbar ohne Konfiguration weiterer Rechner
  - . Selbstbau leicht möglich
  - . in *jeder* Situation als *Sofort-Lösung* geeignet

Anmerkung Hardware-Anforderungen

Den begrenzenden Faktor für die Durchsatzleistung von Firewalls bildet die Bandbreite des Busses, mit der die Netzwerkkarte an die CPU angebunden ist. CPU-Leistung, RAM-Ausbau und Plattendurchsatz bleiben zweitrangig. Also ent- entscheidet die Auslegung des Mainboards.

Die Leistung von Firewalls wird in Paketen pro Sekunde gemessen. Die Länge der Pakete bleibt zweitrangig (solange man keine DPI betreibt).

Beispiel: **Alix-Board**

500 Mhz Stromspar-CPU
256 MB RAM
3 Nics à 100 Mbit

150,00 EUR

ausreichend als Stateful Inspection Firewall für 50...70 Firmen-Rechner

Falls Verschlüsselung, DPI oder IDS/IPS hinzu kommen, stößt man bald an die Leistungsgrenze der CPU. Aus sicherheitstechnischer Sicht sollten solche Aufgaben möglichst auf andere Geräte verlagert werden, um die Angriffsfläche der Firewall klein zu halten.