Internet und Security

Mirko Dziadzka
dziadzka@gmx.net

Übersicht

- Bestandsaufnahme
- Ursachen der Security Probleme
- Lösungsmöglichkeiten
- Ausblick
- Diskussion

Bestandsaufnahme (1)

- Das Internet hat sich in den letzten 8 Jahren von einem Forschungsnetz in ein kommerziell genutztes Netz gewandelt.
  - Firmen benutzen das Internet zur Kommunikation
  - Firmen verdienen Ihr Geld im Internet

Bestandsaufnahme (2)

- “Denial of Service” Angriffe gegen Yahoo, eBay, …
- E-Mail Viren “ILOVEYOU”
- regelmässig werden Websites “gehackt”
- Kundendaten werden entwendet
- professionelle Industriespionage

Übersicht

- Bestandsaufnahme
- **Ursachen der Security Probleme**
- Lösungsmöglichkeiten
- Ausblick
- Diskussion

Ursachen der Security Probleme

- Unsichere Protokolle
- Unsichere Software
- Schlechte Administration
- Ungeschulte Benutzer

Unsichere Protokolle

- Das Internet war nie als sicheres Medium geplant
- Ziel des IP Protokolls ist der effiziente Transport von Daten
- Ein grosser Teil der Internetprotokolle entsteht aus Prototypen

Unsichere Software (1)

- Software hat Fehler
- Im normalen Betrieb ist ein Applikation die zu 99.99% korrekt läuft aktzeptabel
- Ein Angreifer wird die 0.01% Instabilität ausnutzen

Unsichere Software (2)

- Beim Softwaredesign stehen Funktionalität und Wartbarkeit im Vordergrund
- Securityexperten werden zu spät konsultiert
- Die eingesetzten Programmiersprachen (C und C++) verleiten zum unsauberen Programmieren
- Es gibt nicht genügend qualifizierte Programmierer

Schlechte Administration

- Administration von Netzwerken und Firewalls ist komplex und setzt viel Erfahrung voraus
- Es gibt nicht genügend qualifizierte Admins
- Graphische Benutzeroberflächen versuchen komplexe Sachverhalte (zu) einfach darzustellen

Ungeschulte Benutzer

- Den Benutzer interessiert Bequemlichkeit mehr als Sicherheit
- Die Folgen waren bei Melissa, ILOVEYOU und Macro-Viren zu beobachten
- Der Anteil der nicht technisch interessierten Benutzer ist stark gestiegen

Übersicht

- Bestandsaufnahme
- Ursachen der Security Probleme
- **Lösungsmöglichkeiten**
- Ausblick
- Diskussion

Lösungsmöglichkeiten

- Sichere Protokolle
- Firewalls
- Intrusion Detection Systeme
- Nutzerschulung
- Open Source Software

Sichere Protokolle

- Verschlüsselte und authentisierte Netzwerkverbindungen (VPN, IPsec,…)
- Verschlüsselte E-Mails (PGP, S-MIME)
- Gesicherte Verbindungen zu Servern (Mail, WWW) über SSL
- von vielen Benutzern / Firmen noch ignoriert

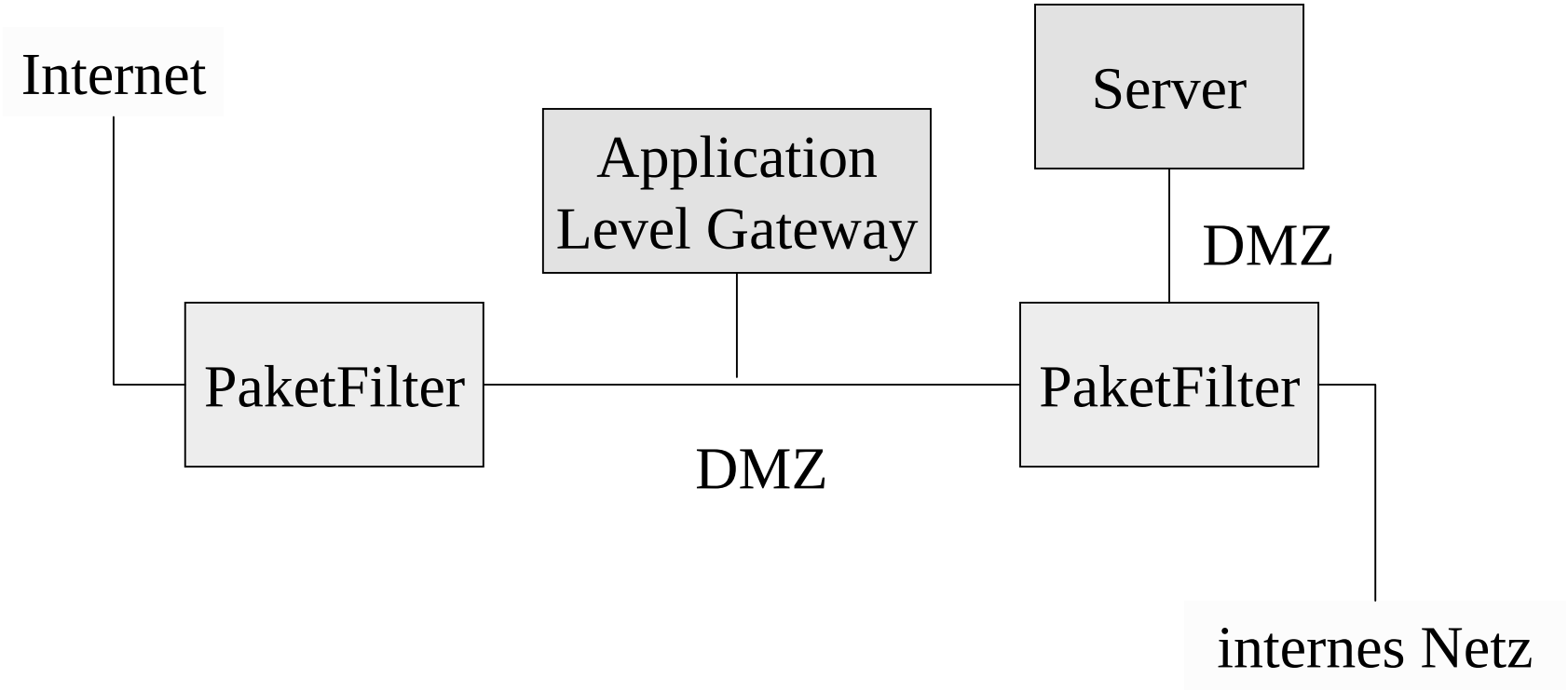
Firewalls (1)

- bieten einen definierten Übergang zwischen zwei Gebieten mit verschiedenen Securityanforderungen
- können den Datenverkehr analysieren und filtern (“active content”)

Firewalls (2)

- werden inzwischen von den meisten Firmen aktzeptiert, aber die Qualität der einzelnen Lösungen schwankt beträchtlich
- ein guter Firewall ist komplex und verursacht hohe laufende Kosten (Updates, Admin)

Firewalls (3)


Internet
Server
Application
Level Gateway
DMZ
PaketFilter
PaketFilter
DMZ
internes Netz

Intrusion Detection Systeme

- Detektieren annormales Verhalten auf einem System oder in einem Netzwerk
- Notwendig zur Überwachung der Systeme eines Firewalls
- Sinvoll zur Überwachung aller Server im internen Netz und des Netzwerkes selber
- **Aber**: viel know-how beim Admin notwendig

Schulung der Nutzer

- Ist zeitaufwendig, aber in letzter Konsequenz die beste Wahl gegen Viren
- "*Du sollst keine fremden Programme ausführen*"
- Ist notwendig, um beim Nutzer ein Sicherheitsbewusstsein auch auf anderen Gebieten zu schaffen

Open Source Software

- “Peer review” der securityrelevanten Teile der Software ist notwendig
- im Open Source Bereich ist dies einfacher als im closed Source Bereich
- **Aber**: Open Source heisst nicht, dass keine Fehler vorhanden sind

Übersicht

- Bestandsaufnahme
- Ursachen der Security Probleme
- Lösungsmöglichkeiten
- **Ausblick**
- Diskussion

Ausblick

- Authentisierung / PKI
- Digitale Unterschrift
- Biometrie
- Ecash
- WAP, transportable Geräte

Diskussion