# Personal Firewall (PFW) und Virenscanner

Präsentation von Gunawati A.-Tillmann, Miguel Lopez und Andreas Angelkorte

# Gliederung

- Personal Firewall

1. Zweck einer Firewall
2. Funktionsweise einer Firewall
3. Personal Firewall als Schutzmaßnahme
4. Beispiele für Personal-Firewall-Software

- Virenscanner

5. Zweck eines Virenscanners
6. Typen von Antiviren-programmen
7. Erfolgswahrschein-lichkeit
8. Aktualisierung der Antivirensoftware

# 1. Zweck einer Personal Firewall

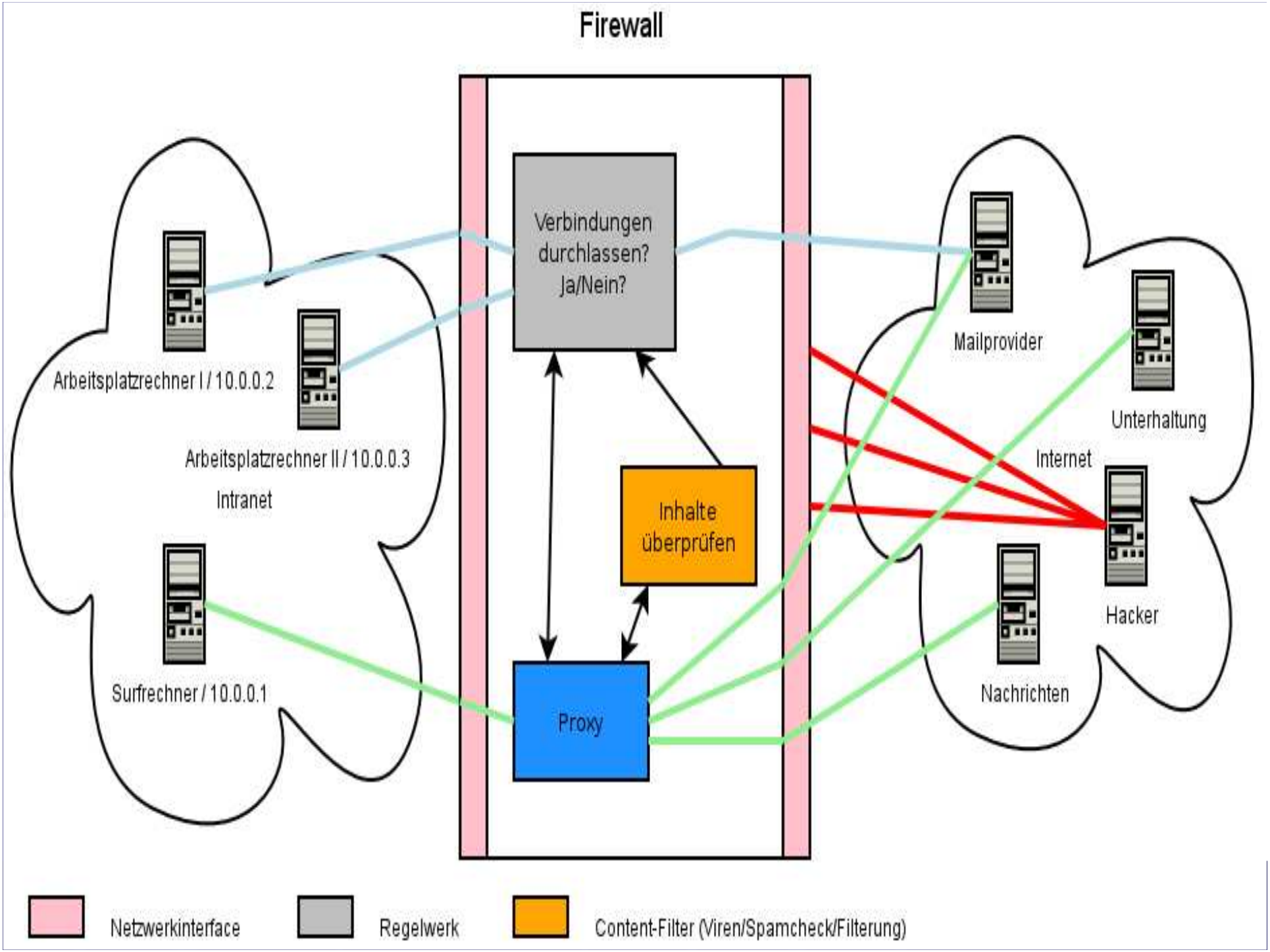
- Schutz eines Host vor Gefahren aus dem Netz:
  - Kontrolle und Abwehr vor Zugriffen von außen (Würmer, Cracker)
  - Absicherung gegen ungewollte Verbindungen (Backdoors, Spyware)

# 2. Funktionsweise einer Personal Firewall

- Die Funktionsweise basiert auf einem Paketfilter, der ein- und ausgehende Datenpakete nach bestimmten Kriterien (Quell- und Zieladresse, Protokoll, etc.) anwendungsorientiert blockiert.
- Einige PFWs verfügen über einen Lernmodus, der es erlaubt noch nicht registrierten Datenverkehr zu konfigurieren.

- Zum Teil verfügen Personal Firewalls über einen Content-Filter, der es ermöglicht, Datenpakete zu überprüfen und beispielsweise Werbebanner aus HTML-Seiten herauszufiltern.
- In der Regel können „Automatische Updates“, vom Hersteller ins Netz gestellt, von der Personal Firewall selbständig installiert werden.

- Einiges PFWs bieten einen Stealth-Modus, d.h. Anfragen werden auf ungenutzte Ports unbeantwortet verworfen, um Angriffe zu erschweren und Informationen über das eigene System zu verschleiern (Security through Obscurity).


Firewall
Verbindungen durchlassen? Ja/Nein?
Arbeitsplatzrechner I / 10.0.0.2
Arbeitsplatzrechner II / 10.0.0.3
Intranet
Surfrechner / 10.0.0.1
Inhalte überprüfen
Proxy
Mailprovider
Unterhaltung
Internet
Hacker
Nachrichten
Netzwerkinterface
Regelwerk
Content-Filter (Viren/Spamcheck/Filterung)

# 3. Personal Firewall als Schutzmaßnahme

- Nach Aussage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wird empfohlen, die Personal Firewall nur im Zusammenspiel mit Viren- und Spywarescannern, regelmäßiger Datensicherung (Backup) und baldigem Aktualisieren (Update) als sichere Schutzmaßnahme anzusehen.

- Angriffen von außen richten sich meist gegen Programme, die von Netzwerkdiensten (Nachrichtendienste) angeboten werden.
- Der Paketfilter einer PFW schützt vor Angriffen, indem er alle Datenpakete aus dem Internet verwirft, die an den Port gerichtet sind, an dem der Server lauscht.

- Bei Angriffen von innen gelangt Schadsoftware über einen Pufferüberlauf in einer Anwendung oder als Trojanisches Pferd auf den Rechner.
- Eine Personal Firewall soll hier die spätere Kommunikation der Malware aufdecken und vereiteln.
- Unbemerkte Manipulationen am Betriebssystem können dieses kompromittieren, d.h. es kann durch die PFW nicht mehr gesichert werden.

- Personal Firewalls werden dazu eingesetzt, Spyware zu erkennen, die noch nicht in der Datenbank eines Spywarescanners enthalten sind.
- Problematisch ist die Unterscheidung zwischen ungefährlichen Programmen, die nach Updates suchen und Schadsoftware, die als nützlicher Systemprozess getarnt ist.

# 4. Beispiele für Personal Firewall

- Windows Firewall (Microsoft): die bereits aktivierte Standardkonfiguration verwirft eingehende Verbindungen. Über das Sicherheitscenter kann man Ausnahmelisten für bestimmte Ports und Programme erstellen.
- Zone Alarm (ZoneLabs): kostenlose Internetversion, die getrennte Sicherheitseinstellungen für zwei verschiedene Zonen (lokales Netz und Internet) erlauben.

# 5. Zweck von Antivirenprogramme

- Ein Antivirenprogramm (auch Virenscanner genannt) ist eine Software, die bekannte Computerviren, Computerwürmer und Trojanische Pferde aufspürt, blockiert und ggf. beseitigt.

# 6. Typen von Antivirenprogrammen

- Echtzeitscanner:
  - Er scannt im Hintergrund alle Dateien, Programme, den Arbeitsspeicher und ggf. den HTTP- und FTP-Verkehr, um Verdächtiges zu löschen, verschieben oder zu reparieren.
  - Man unterscheidet zwischen den Strategien Scannen beim Lesevorgang und Scannen beim Schreibvorgang.

- Manueller Scanner:
  - Er muss vom Benutzer von Hand gestartet werden (On-Demand).
  - Bei Erkennen von schädlicher Software erscheint die Option zur Reinigung, Quarantäne oder Löschung der befallenen Datei.

- Online Virenscanner:
  - Programmcodes und Viren-Muster  werden im On-Demand-Modus online geladen.
  - Sie sind zum Reinigen nicht aber zum präventiven Schutz eines Systems geeignet.

# 7. Erfolgswahr-scheinlichkeit

- Im Hinblick auf die ständige Weiterentwicklung von Malware kann kein Virenscanner vor allen erdenklichen Viren und Würmern schützen.

## Für die Erfolgswahrscheinlichkeit des Virenscanners sind die Scanengines sowie die Verfahrenstechniken verantwortlich.

- Unter Scanengines versteht man den Programmteil eines Virenscanners, der für die Untersuchung eines Computers auf Malware verantwortlich ist.
- Sie bestimmen somit unmittelbar die Effizienz der Antivirensoftware.
- Scanengines sind Softwaremodule, die unabhängig vom Rest eines Virenscanners aktualisiert und eingesetzt werden können.

Grundsätzlich kann bei der Erkennung von Malware zwischen zwei Techniken unterscheiden:

1. Reaktiv: der Schädling wird erst erkannt, wenn eine entsprechende Signatur seitens des Herstellers der AV-Software zur Verfügung steht *(klassische Art).*
2. Proaktiv: Erkennung von Viren, ohne dass eine entsprechende Signatur zur Verfügung steht. Proaktive Verfahren sind die Heuristik oder die SandBox Technologie.

## Heuristik

- Einige Virenscanner verfügen über die Möglichkeit, auch nach allgemeinen Merkmalen zu suchen (Heuristik), um unbekannte Viren zu erkennen.
- Hierbei suchen Virenscanner nach verdächtigen Codes, die z. B. die Festplatte formatieren oder unerwartete Online-Verbindungen aufbauen.
- Die Wichtigkeit dieser proaktiven Art der Erkennung nimmt stetig zu, da die Zeiträume, in denen neue Viren auftauchen, immer kürzer werden.

# SandBox

- Um die Erkennung von unbekannten Viren und Würmern zu erhöhen, wurde eine neue Technologie entwickelt, bei der die Programme in einer gesicherten Umgebung, der SandBox, ausgeführt werden.
- Die SandBox erwartet bei der Ausführung der Datei eine dateitypische Verhaltensweise. Weicht die Datei von dieser zu einem gewissen Grad ab, klassifiziert die SandBox diese als potentielle Gefahr.

- Als Ergebnis liefert sie zudem eine Ausgabe,die zeigt, welche Aktionen die Datei auf dem System ausgeführt hätte und welcher Schaden angerichtet worden wäre.
- Diese Informationen können auch nützlich sein, um eine Bereinigung eines bereits infizierten Computersystems vorzunehmen.

# 8. Aktualisierung der Antivirensoftware

- Von besonderer Bedeutung sind die Auto-, Internet-, oder auch Live-Updatefunktionen, mit der automatisch beim Hersteller aktuelle Virensignaturen heruntergeladen werden, um sicher zu gehen, dass das Programm auf dem aktuellen Stand ist.
- Die Qualität der Updates besteht darin, dass bei einer bestehenden Bedrohung möglichst zeitnah eine entsprechende Signatur veröffentlich wird (Reaktionszeit).

# Wir bedanken uns für

# Eure Aufmerksamkeit!

ENDE