Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Personal Firewall

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

Inhalt

- **Grundlagen**
- **Angriffe und Abwehr**
- **Zusammenfassung**

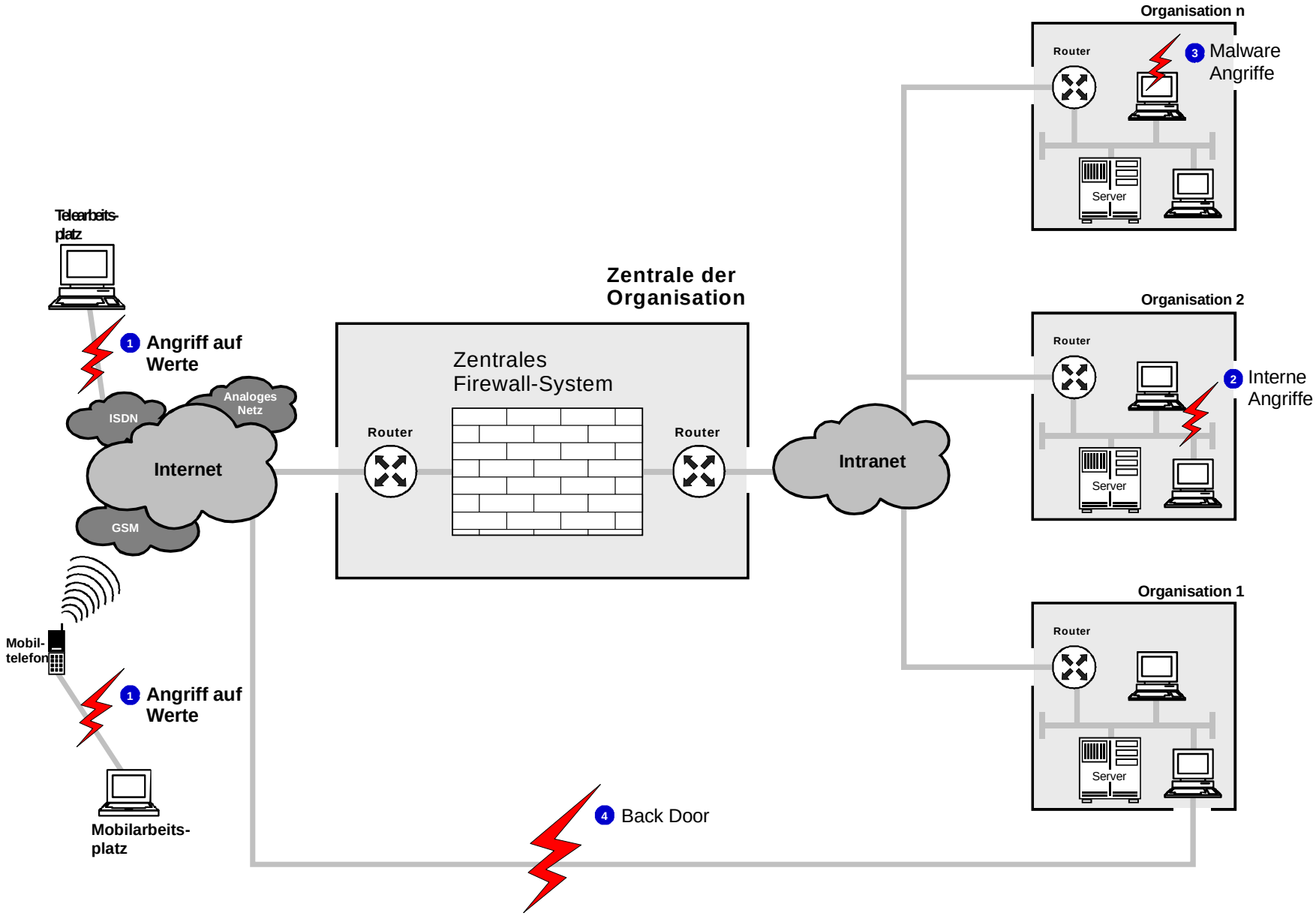
Inhalt

- **Grundlagen**
- Angriffe und Abwehr
- Zusammenfassung

Personal Firewall
→ Ziele der Vorlesung

- Kennenlernen von grundlegende Funktionen von Personal Firewalls
- Einbindung von Personal Firewalls in bereits existierende Strukturen
- Einschätzung der Schutzmaßnahmen einer Personal Firewall

Grundlagen
→ Übersicht



Grundlagen
→ Firewalls und Firewalls

- Grundsätzlich gibt es zwei Arten von Firewalls:
  - Netzwerk-Firewalls als eigenständiges Sicherheitssystem und Knoten im Netzwerk (letzte Vorlesung)
  - **Personal-Firewalls** als Sicherheitsprogramm, das auf einem Computer installiert wird und dort das Betriebssystem und Anwendungen schützt (diese Vorlesung)

- Allerdings sind viele Abgrenzungen nicht einheitlich und Grenzen sind fließend
- **Elisabeth D. Zwicky:** *„Die Welt ist voll von Leuten, die darauf bedacht sind, Ihnen weiszumachen, dass etwas keine Firewall ist.* […] *Wenn es dazu gedacht ist, die bösen Jungs von Ihrem Netzwerk fernzuhalten, dann ist es eine Firewall. Wenn es erfolgreich die bösen Jungs fernhält, ist es eine gute, wenn nicht, ist es eine schlechte Firewall. Das ist alles, was es dazu zu sagen gibt.“*

Grundlagen
→ Idee

- Eine **Personal Firewall** oder **Desktop Firewall** ist eine **Sicherheitssoftware** auf dem Rechnersystem
- Sie **reguliert** den ein- und ausgehenden Datenverkehr eines Rechnersystems **auf dem Rechner selbst**
- Im Gegensatz zu Netzwerk-Firewalls sind Personal Firewalls, nicht eigenständige Sicherheitssysteme
- Die Idee von Personal Firewalls / Desktop Firewalls ist, zwischen dem Betriebssystem/Anwendungen und dem Netz (Internet) die Kommunikation zu reglementieren

Grundlagen
→ Unterschiede

- Es gilt dabei zu beachten, dass die Personal Firewall selbst Ziel eines Angriffes sein kann und das Durchbrechen dieser das komplette Rechnersystem offen legt.
- Allerdings wird angenommen, dass die Personal Firewall im Vergleich zu einem gesamten Betriebssystem/Anwendung weniger Fehler enthält, da sie weniger komplex ist.
- Ein weiterer Unterschied zu Netzwerk-Firewalls ist die recht einfach Möglichkeit der **Regulierung auf Anwendungsebene.**

Grundlagen
→ Hauptbestandteil

- Der Hauptbestandteil einer Personal Firewall ist ein **Paketfilter**
  - Zur Regulierung eigehender und ausgehender Datenpakete
  - Kriterien sind die Adresse (Quell oder Ziel) und die Ports (Quell oder Ziel)

- Zusätzlich ist ein **Anwendungsfilter** (Application Control) Teil des Sicherheitssystems
  - Dieser ermöglicht die Reglementierung auf Anwendungsebene

Grundlagen
→ Weitere Funktionen (1/4)

- **Lernmodus**
  - Regeln für Paketfilter und Anwendungsfilter werden durch direkte Interaktion mit dem Benutzer gelernt.
  - Wenn Anwendungen mit dem Netzwerk kommunizieren wollen und noch keine Regel dafür in der Personal Firewall gesetzt ist, wird die Kommunikation unterbunden, bis der Anwender dieses Anwendung zulässt.

- **Content-Filter**
  - Betrachten der Inhalte von Datenpakete, um Schadcode oder ähnliches zu erkennen und zu entfernen
  - Web Application Firewall / Web Shield für Content Filter zum Schutz gegen Angriffe von fremden Webseiten
  - Häufig auch besondere Filter für E-Mail (Anhänge)

Grundlagen
→ Weitere Funktionen (2/4)

- **Intrusion Detection System / Intrusion Prevention System**
  - Ermöglicht das Erkennen und Verhindern von Angriffen
  - Beispielsweise, wenn Schadsoftware gezielt Personal Firewall Regeln von normalen Anwendungen ausnutzt (Herstellen einer Verbindung über den Browser-Kommunikation (Port 80), etc.)

- **Sandbox**
  - Einschränken der Möglichkeiten für eine Anwendung
  - Soll verhindern, dass eine Schadsoftware Zugriff auf das Rechnersystem und dessen Ressourcen erlangt

Grundlagen
→ Weitere Funktionen (3/4)

- **Protokollierung**
  - Ähnlich der Netzwerk-Firewall bietet auch die Personal Firewall die Möglichkeit der Protokollierung von Ereignissen
  - Oftmals werden Warnungen durch Einblendung von Informationsboxen auch direkt an den Benutzer weitergeleitet

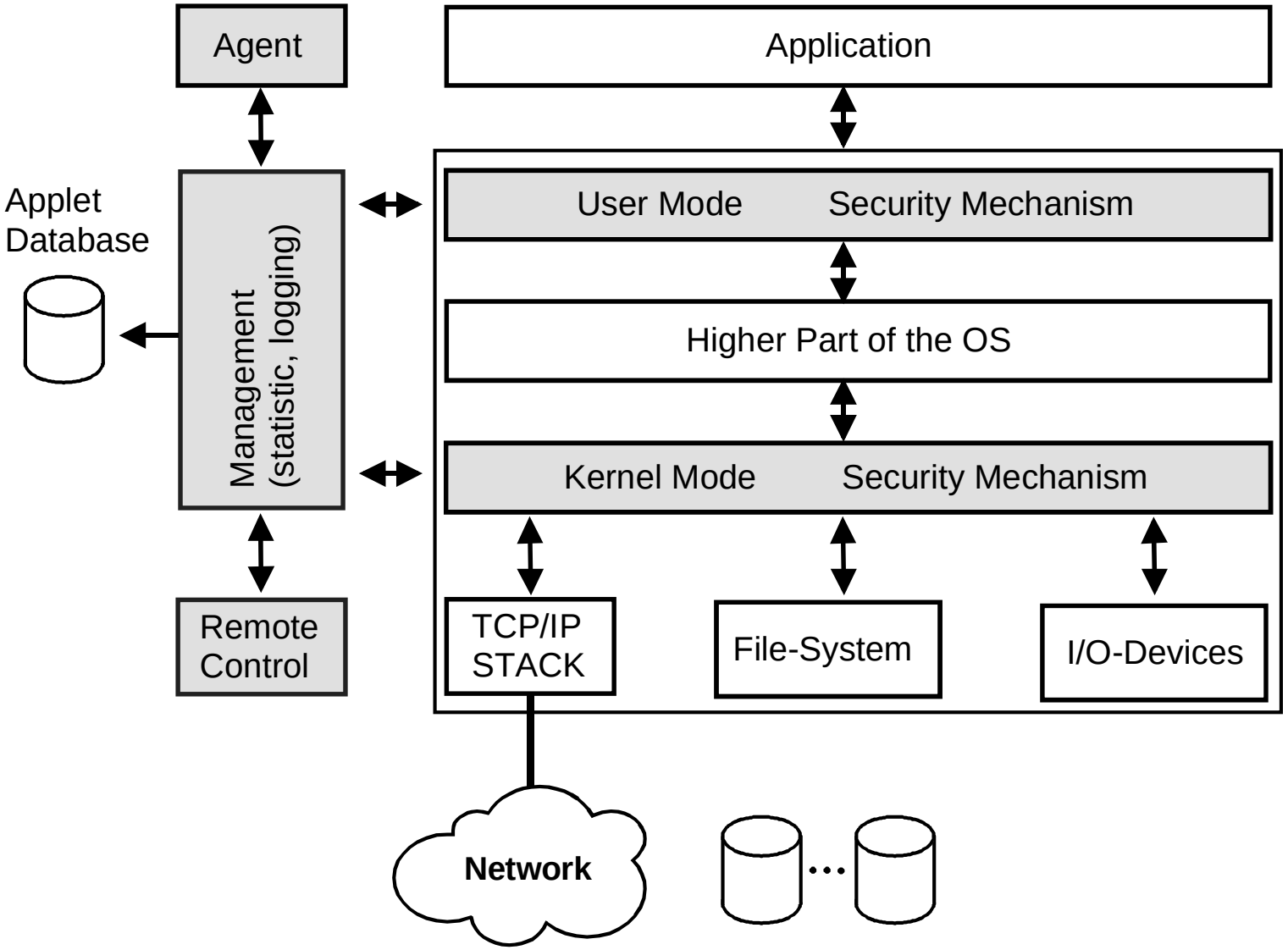
- **Stealth-Modus**
  - Security through Obscurity (Sicherheit durch Verschleierung)
  - Bei Anfragen an Ports, ob dort ein Dienst vorhanden ist, wird durch Ignorieren dieser Anfragen dem Angreifer weniger Informationen über das Rechnersystem überlassen

Grundlagen
→ Weitere Funktionen (4/4)

- **Updates**
  - Personal Firewalls updaten sich in der Regel selbstständig durch regelmäßige Abfragen beim Hersteller

- **Fernwartungszugang / Remote Access**
  - Administratoren haben manchmal die Möglichkeit, von außen auf die Personal Firewall zuzugreifen, um daran Änderungen vorzunehmen (Unternehmenslösungen)
  - Hauptsächlich interessant bei der Betreuung von einer größeren Anzahl von Rechnersystemen (Einführung neuer Software, die eine neue Firewallregel braucht, oder einsehen von Log Files)

Grundlagen
→ Architektur



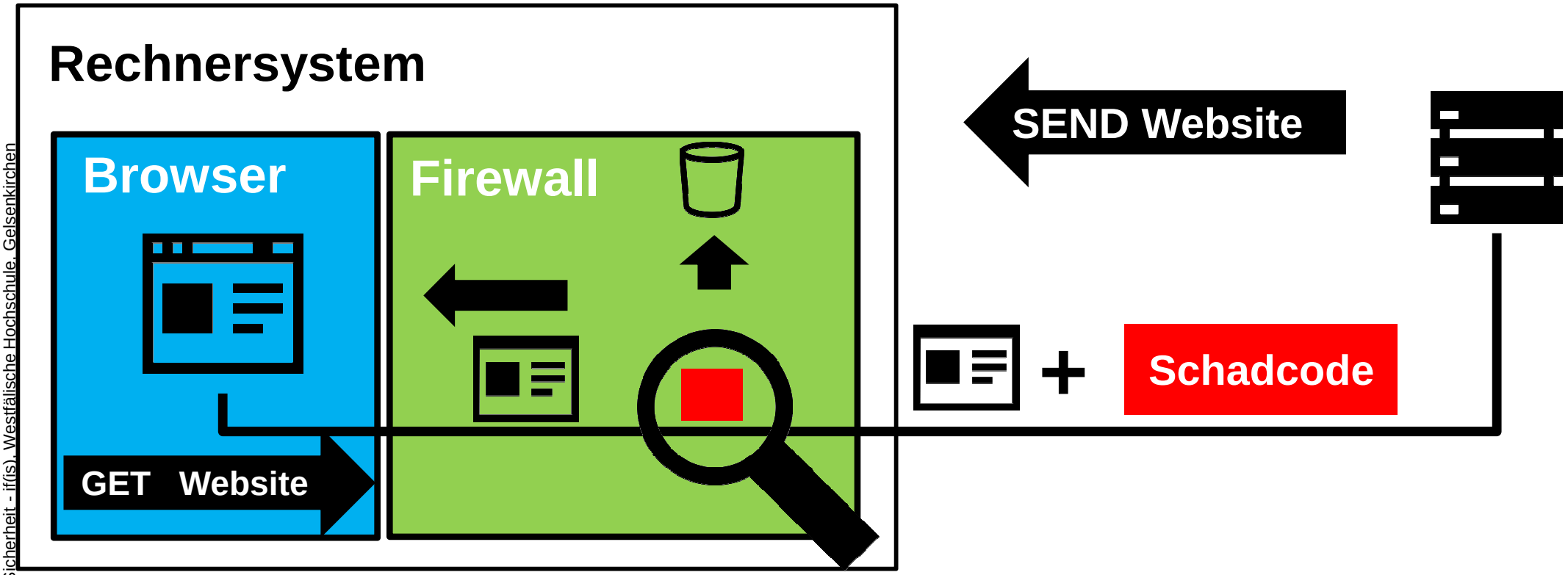
Inhalt

- Grundlagen
- **Angriffe und Abwehr**
- Zusammenfassung

Angriffe und Abwehr
→ Einleitung

- Nachdem erklärt wurde, was eine Personal Firewall ist, sollen nun auf gezeigt werden, wie diese in der Realität arbeitet und wie der Schutz funktioniert.
- Dabei werden einige grundsätzliche Angriffe aufgezeigt sowie dargestellt, wie eine Personal Firewall darauf reagiert.

Angriffe
→ Schadcode



- **Schadcode** bei dem Besuchen von Internetseiten (JavaScript, Cookies, JAVA (Applets etc), ActiveX ...)
- Die **Personal Firewall analysiert** das eingehende Paket auf Schadcode
- **Entfernt** beim Auffinden den Schadcode

Angriffe
→ Schadcode - Praxis

Praxis

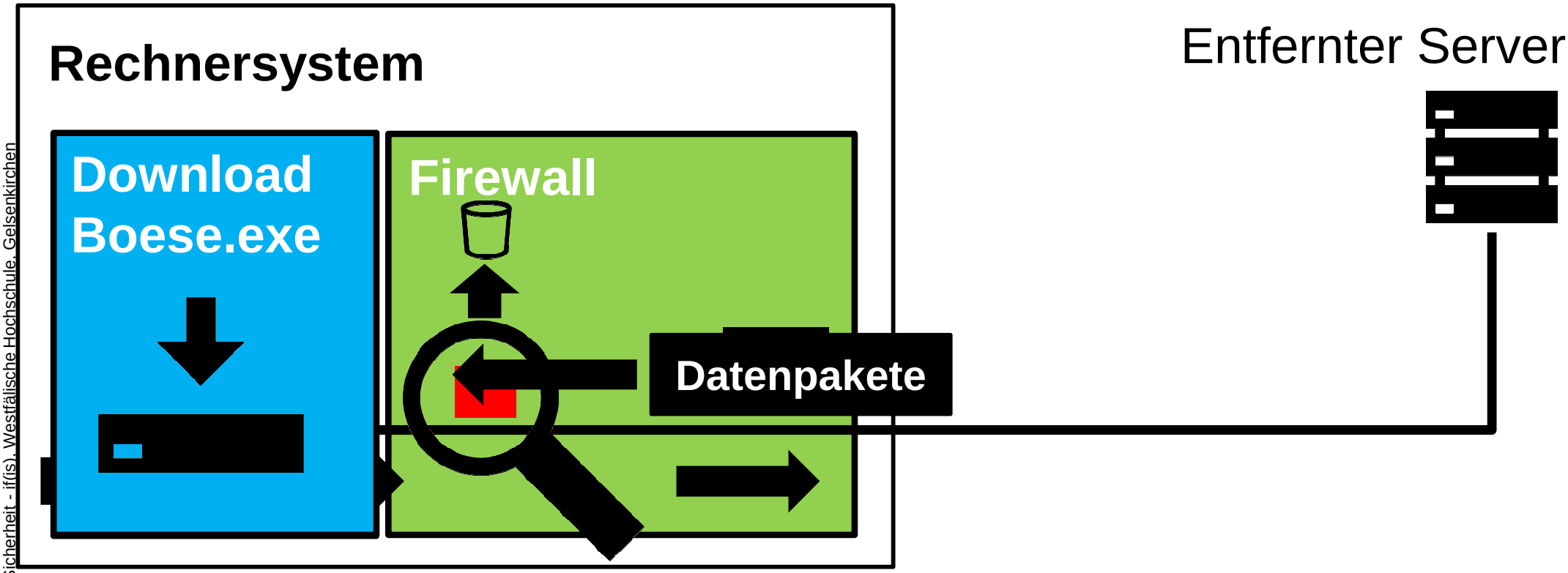
- In der Praxis bedeutet dies, die Personal Firewall muss Schadcode erkennen
- Dies ist aber, ähnlich wie beim Erkennen von Viren / Würmern / Trojanern), ein Kampf gegen Windmühlen
- Daher ist in der Regel die Erkennungsrate entweder sehr niedrig oder die „false positive“ (falsche Erkennung) sehr hoch
- Daher hilft dieser Schutz nur gegen Angriffe, die:
  - bereits länger bekannt sind
  - Leicht zu erkennen sind

Angriffe
→ Schadcode - Alternative

Alternative

- Regelmäßige Updates
- Grund:
  - In der Regel entstehen die meisten der Schadcodes, **nachdem** ein Patch / Update für ein Produkt bekannt wird
  - Dies liegt daran, dass das Finden einer Schwachstelle aufwendig und sehr schwierig ist
  - Bei dem Erscheinen eines Patch / Updates, analysieren die Angreifer innerhalb von ca. 4 Stunden diesen, um dann mit den Erkenntnissen eine Schadsoftware zu schreiben, die diese Schwachstelle ausnutzt

Angriffe
→ Viren, Würmer, Trojaner



- **Viren, Würmer, Trojaner** werden beim Empfangen nur **sehr schwer erkannt** (einzelne Pakete, viele Unterschiede, etc.)
- Bei der **Kommunikation** einer Malware, die schon auf dem Rechner ist**,** wird die Personal Firewall **aktiv und verhindert eine Verbreitung** oder den **Datenaustausch** (Passwörter etc. vom Trojaner)

Angriffe
→ Viren, Würmer, Trojaner - Praxis

Praxis

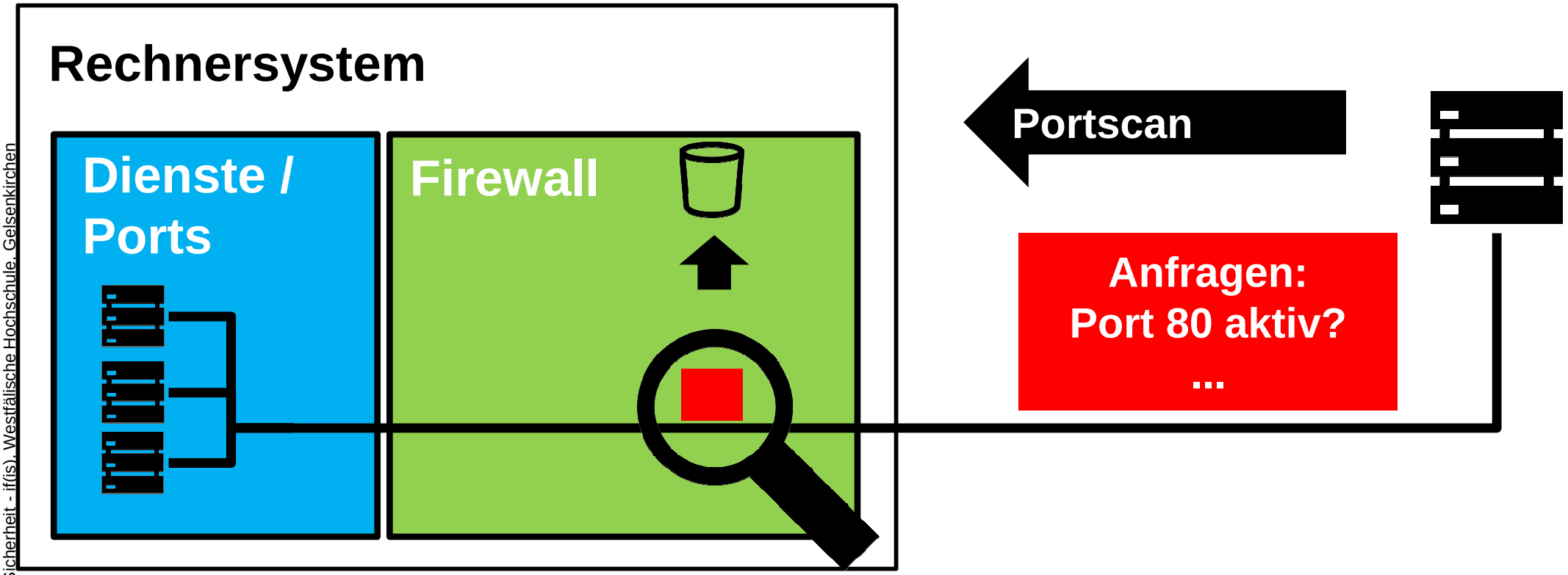
- Eine Personal Firewall kann das Ausführen von Schadsoftware nur schwer verhindern, da dies entweder vom Benutzer „selbst gewollt“ oder durch eine nicht bekannt Sicherheitslücke geschieht
- Eine **Personal Firewall** bietet die Möglichkeit, **Kommunikationen** zu **unterbinden**, **allerdings** ist dies auch **nur sehr eingeschränkt** möglich, denn:
  - Wenn die **Schadsoftware über eine Sicherheitslücke in das System gelangt,** ist eine **Manipulation der Personal Firewall** meist **kein Problem** mehr (Abschalten oder zusätzliche Regel für Schadsoftware)
  - Die **Schadsoftware** kann ihre **Kommunikation verschleiern** (Tunneln, Nutzen von anderen Anwendungen, die erlaubt sind)
- Davon abgesehen ist eine Personal Firewall kein Schutz gegen Malware!

Angriffe
→ Viren, Würmer, Trojaner - Alternative

Alternative

- Ein Virenscanner (Anti-Malware) ist hilfreich!
- Regelmäßige Updates helfen gegen Sicherheitslücken in der Software (Betriebssystem, Anwendungen, …)
- Ein verantwortungsvoller Umgang mit dem Internet minimiert das Risiko unbeabsichtigter Downloads von Schadsoftware
- Gegen unbekannte Sicherheitslücken, die zur Installation der Schadsoftware genutzt werden (Auto USB Installation, etc.) gibt es keinen Schutz, wenn der Nutzer solche Features erlaubt!

Angriffe
→ Portscan



- Rechner wird **gezielt „ausgefragt“ nach „offenen“ Ports**
- Personal Firewall im **Stealth Modus blockiert Antworten** auf solche Anfragen

Angriffe
→ Portscan - Praxis

Praxis

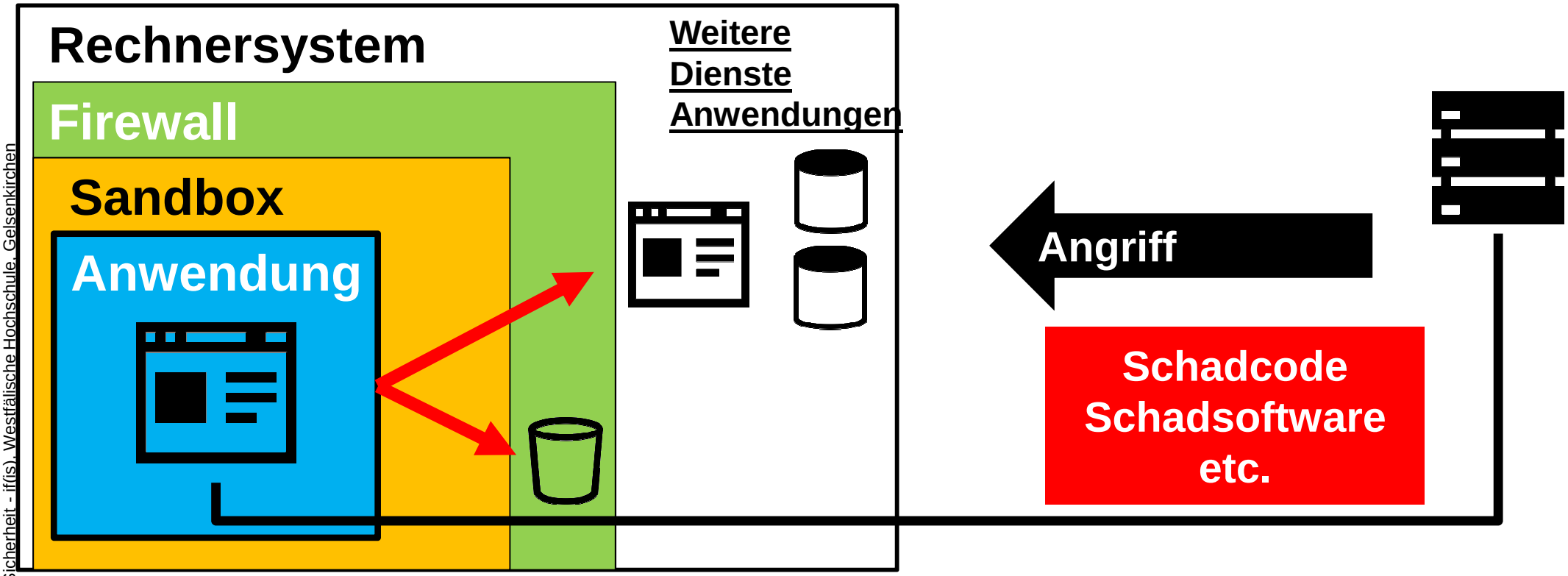
- Das Verwerfen einer Anfrage (ICMP) auf einen Port ist eine gängige Praxis im Internet
- Durch das Verwerfen wird direkt Einfluss auf das „Normalverhalten“ genommen, was Nebeneffekte hat (höhere Belastung des Netzwerkes durch erneute Anfragen, normale Nutzer werden ausgebremst)
- Die Quelle des Portscans bekommt so keine Antworten auf seine Anfragen
- Der Portscanner bemerkt, wenn keine Antwort erhalten wurde!
  Meist erneute Anfrage, um Verlust der Anfrage auf dem Weg zum Ziel zu prüfen
- Ein Portscanner benötigt längere Zeit durch Warten auf „Timeout“. Bessere Portscanner schicken allerdings viele Anfragen gleichzeitig und warten dann auf Timeout

Angriffe
→ Portscan - Alternative

Alternative

- Abschalten von nicht benötigten Diensten, um Angreifern nicht zusätzliche Angriffsvektoren zu geben

Angriffe
→ Sandbox



- Nachdem **Schadsoftware / Schadcode auf** das **Zielsystem** gelangt ist, soll **nun** ein **Zugriff auf** die **weiteren Dienste/Anwendungen** vorgenommen werden
- Die **Personal Firewall blockiert** dies **durch das Sandbox Modell!** Bei dem **Zugriffe** auf **nicht benötigte Teile** des Rechnersystems, wird diese durch die Personal Firewall verhindert werden.

Angriffe
→ Sandbox - Alternative

Alternative

- Sichere Programmierung für Software (nichts worauf ein Endanwender wirklich Einfluss hat)
- Updates / Patches gegen Sicherheitslücken
- Zugriffsrechte des Systems besser nutzen

Angriffe
→ Benutzer

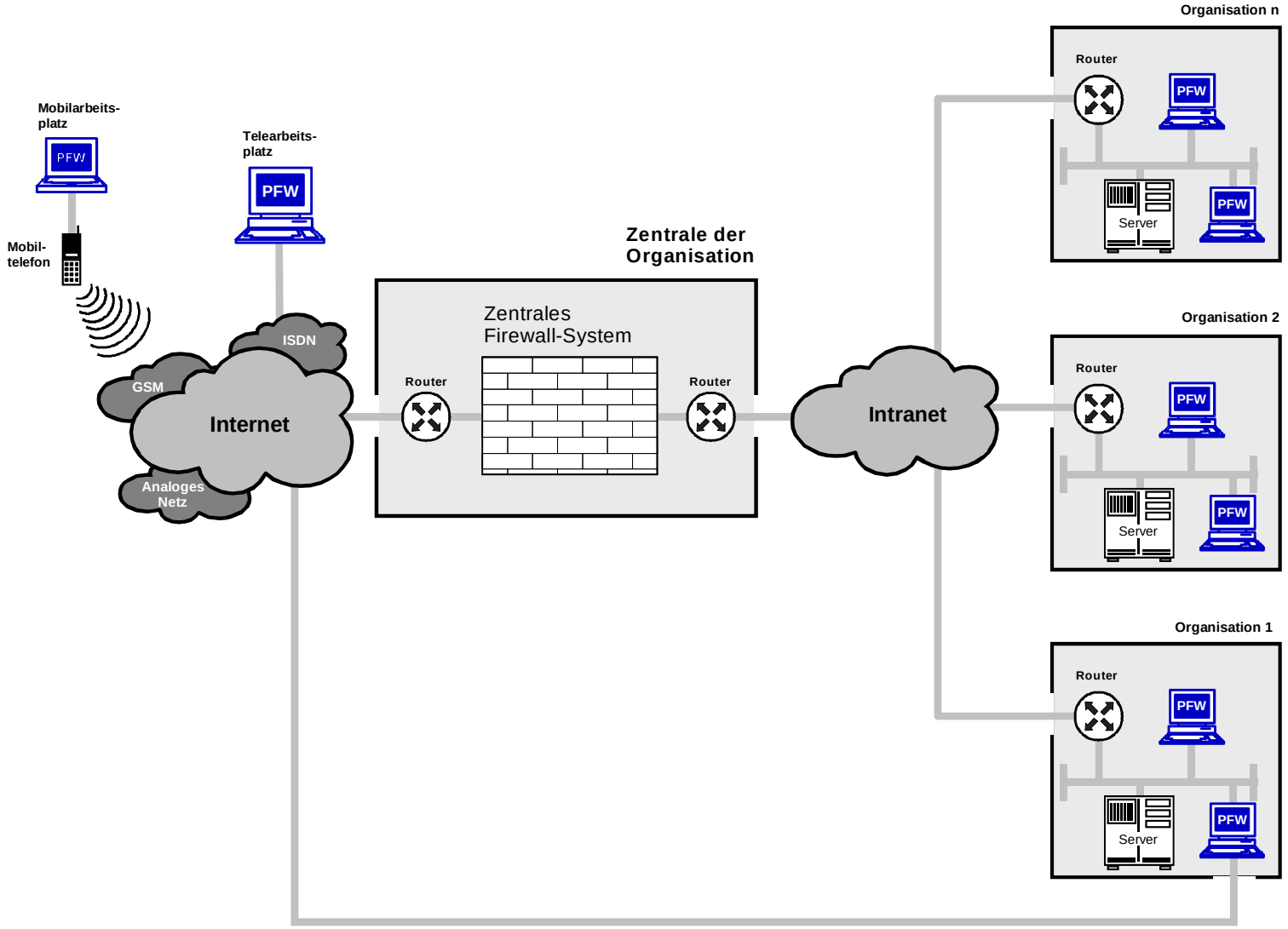
- Eine weitere Voraussetzung für das Funktionieren bei einer Personal Firewall ist das Verständnis der Nutzer
- Die Personal Firewall muss richtig konfiguriert sein und auf Ereignisse entsprechend reagieren
- Dies ist aber nicht so einfach, denn:
  - In der Regel hat der normale Nutzer kein Wissen über TCP/IP sowie andere Protokolle und Dienste
  - Informationen werden selten so aufbereitet, dass sie verständlich sind („update.exe möchte eine Verbindung mit dem Internet herstellen“)
- Personal Firewalls „nerven“ oftmals mit „lästigen“ Fragen
  - Einige Nutzer deaktivieren daraufhin die Personal Firewall

Angriffe
→ Benutzer - Lösung

Lösungen

- Abhilfe sollen verteilte Wissensdatenbanken schaffen
- Darin wird vermerkt, wie andere Nutzer sich, bei der gleichen Anwendung, entschieden haben,
- Diese Informationen kommen aus einem intransparenten System
- Vertrauenswürdigkeit ist dadurch nicht gegeben
- Außerdem gibt es die Möglichkeit der Zertifizierung von Anwendungen (Weiße Listen)
  - Bekannten Anwendungen werden so, ohne weitere Nachfrage, Zugang zum Netzwerk gewährt
  - Welche Anwendung zertifiziert wird, ist nicht eindeutig
  - Hilft nur bei Anwendungen, die weit verbreitet sind und selten für Open Source

Übersicht
→ Personal Firewall in Firmen



Inhalt

- Grundlagen
- Angriffe und Abwehr
- **Zusammenfassung**

Zusammenfassung
→ Übersicht

Auch ohne alle Angriffe und Möglichkeiten durchgegangen zu sein, sollte doch folgendes deutlich werden:

- **Die Installation einer Personal Firewall bietet keinen 100igen Schutz**
- Der **Aufwand** für eine **korrekte Konfiguration** ist hoch
  - Die Zeit könnte auch in die Konfiguration der Anwendungen/ Dienste und anderer Sicherheitstechniken fließen, um den gleichen Effekt zu erhalten
  - Anwender, die eine Personal Firewall **richtig** konfigurieren können, brauchen diese in der Regel nicht

Zusammenfassung
→ Was sagen andere? – tecchannel -(1/3)

- **Generell gilt:** Personal Firewalls sind **kein Allheilmittel** und **stellen keine ernsthafte Sicherheitsstrategie dar**, sondern dienen lediglich als eine Sicherheitskomponente.
- Ein Nutzer, der mit administrativen Rechten surft, wird sich auch mit einer Personal Firewall in Gefahr begeben.
- **Zudem sorgt nur ein sorgfältiger Umgang mit dem Werkzeug auch für entsprechenden Schutz**.
- Wer bedenkenlos alle Dialoge bestätigt, kann auch gleich ohne surfen.
- **Zusätzlicher Schutz durch Antivirus- und Antispyware-Produkte ist ebenfalls unabdingbar**.

Zusammenfassung
→ Was sagen andere? – BSI - (2/3)

- **Man sollte sich vor der Annahme hüten, dass die "einfache" Installation einer Personal-Firewall ausreicht**, um den Rechner vor allen Gefahren des Internets zu schützen.
- **Wichtig ist vor allen Dingen, dass das Betriebssystem, der Webbrowser, der E-Mail-Client und anderen Anwendungen so sicher wie möglich konfiguriert werden**.
- Nicht benötigte Ports müssen geschlossen werden, um hier keine Angriffe zu provozieren.
- Der **Einsatz eines aktuellen Virenscanners ist für die Sicherheit des Systems natürlich unerlässlich**, ebenso wie die Durchführung **regelmäßiger Datensicherungen** und das **Einspielen aktueller Software-Patches** nach bekannt werden von relevanten Sicherheitslücken.

Zusammenfassung
→ Was sagen andere? – BSI - (3/3)

- Dies sollen nur einige Beispiele sein, die verdeutlichen, dass **Sicherheit nicht durch den Einsatz einer einzelnen Sicherheitssoftware erreicht werden kann**, sondern **nur durch ein Zusammenspiel verschiedener Faktoren**.
- **Grundsätzlich gilt aber auch, je sicherer ein Rechner konfiguriert ist, desto kleiner ist der Sicherheitsgewinn durch den Einsatz einer Personal-Firewall**.

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Personal Firewall

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de