# Desktop Personal Firewall und Virenscanner

# Desktop Personal Firewall
# und
# Virenscanner

Präsentation im Rahmen der Lehrveranstaltung Informations- und Kommunikationssysteme

# Desktop Personal Firewall und Virenscanner

- Desktop Personal Firewall
  - Was ist eine Firewall und wie kann diese unterschieden werden?
  - Wie funktioniert eine Firewall?
  - Was ist zu beachten?
- Virenscanner

# Desktop Personal Firewall und Virenscanner

- Was ist eine Firewall?

# Desktop Personal Firewall und Virenscanner

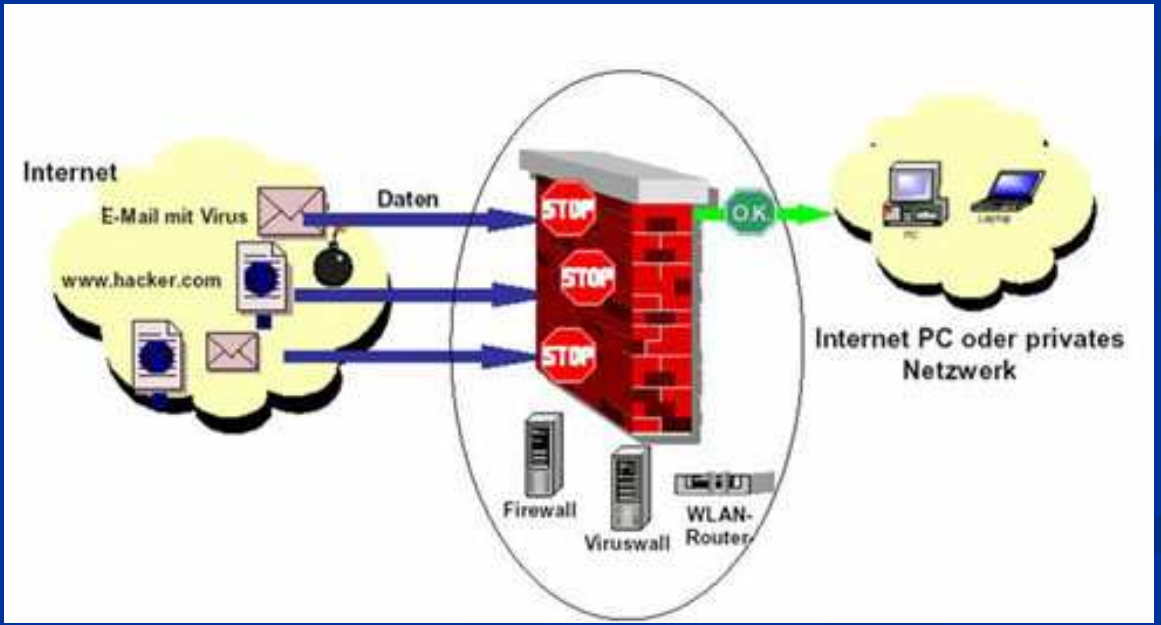
- Was ist eine Firewall?
  - standortbezogenes Sicherheitskonzept zur Trennung von Netzwerkbereichen
  - Firmen- oder ein privates Netzwerk vor unerlaubten Zugriff schützen
  - Schutz des Computers vor Würmern, Trojanern und Viren bei Nutzen beim Umgang mit dem Internet oder in einem lokalen Netzwerk

# Desktop Personal Firewall und Virenscanner

- Wie kann eine Firewall unterschieden werden?
  - Desktop Firewall
    - eine lokal auf dem Computer installierte Firewallsoftware
    - Verhindern von ungewollten Netzwerkzugriff nach außen und auf den eigenen Rechner
    - Programme z.B. Norton Internet Security, Zonealarm
  - Externe Firewall
    - Wird auch als Hardwarefirewall bezeichnet
    - Haben keine Befugnisse auf den lokalen PC
    - Beispielhaft: Firewall in einem Router

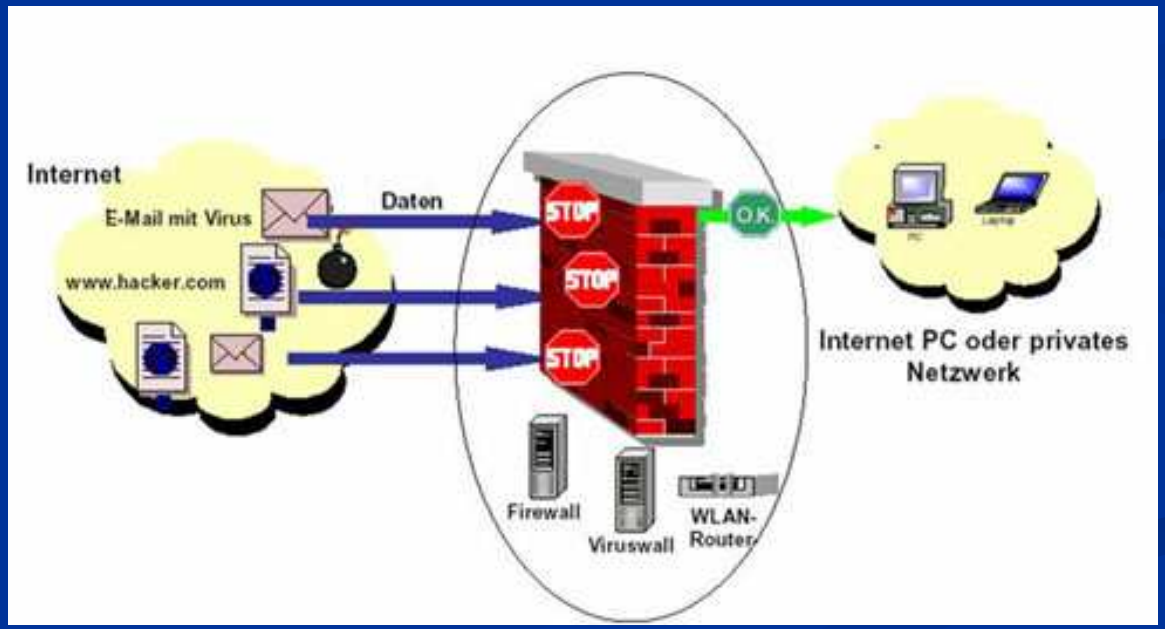
# Desktop Personal Firewall und Virenscanner

- Wie funktioniert eine Firewall?
  - ständiger „Datenverkehr“ im Netzwerk z.B. über E-Mail, Onlinespiele, Multimedia, Onlineshopping oder im Bereich des LAN



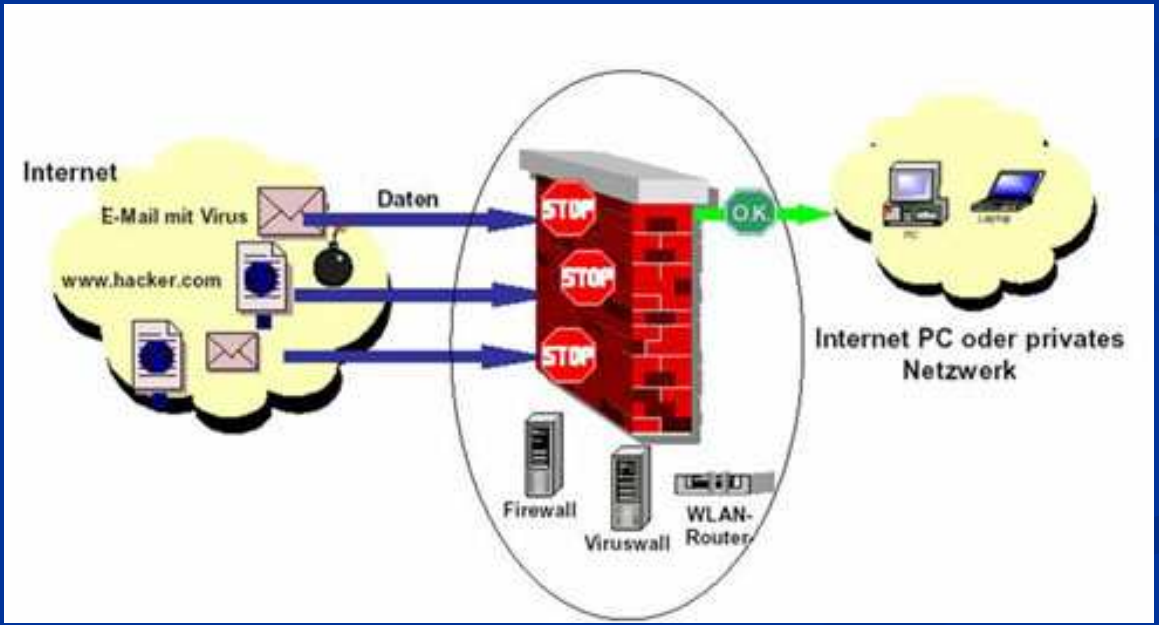
# Desktop Personal Firewall und Virenscanner

- Wie funktioniert eine Firewall?
  - Austausch von Datenpakte, die mit einer Quell-Portnummer kommen und eine Ziel-Portnummer ansteuern



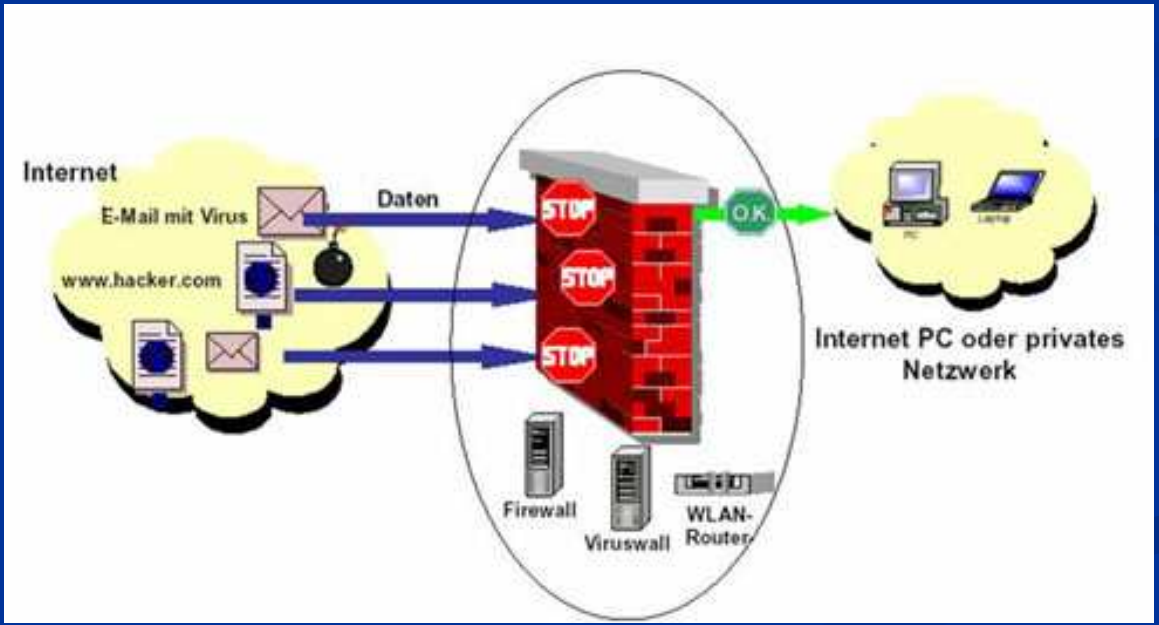
# Desktop Personal Firewall und Virenscanner

- Wie funktioniert eine Firewall?
  - die Firewall riegelt alle Ports ab und überwacht diese
  - bei jedem Zugriff entsteht eine Warnmeldung an der Firewall



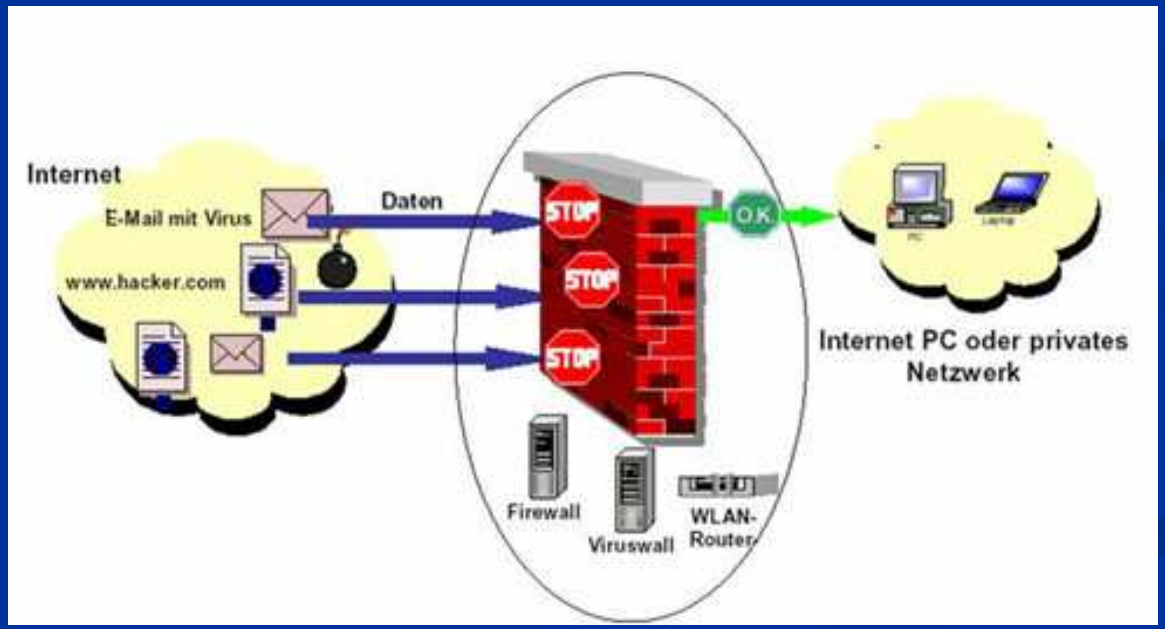
# Desktop Personal Firewall und Virenscanner

- Wie funktioniert eine Firewall?
  - je nach Einstellung kann der Zugriff erlaubt oder verweigert werden, was entweder manuell bzw. als Regel hinterlegt werden kann (sog. Lernmodus)



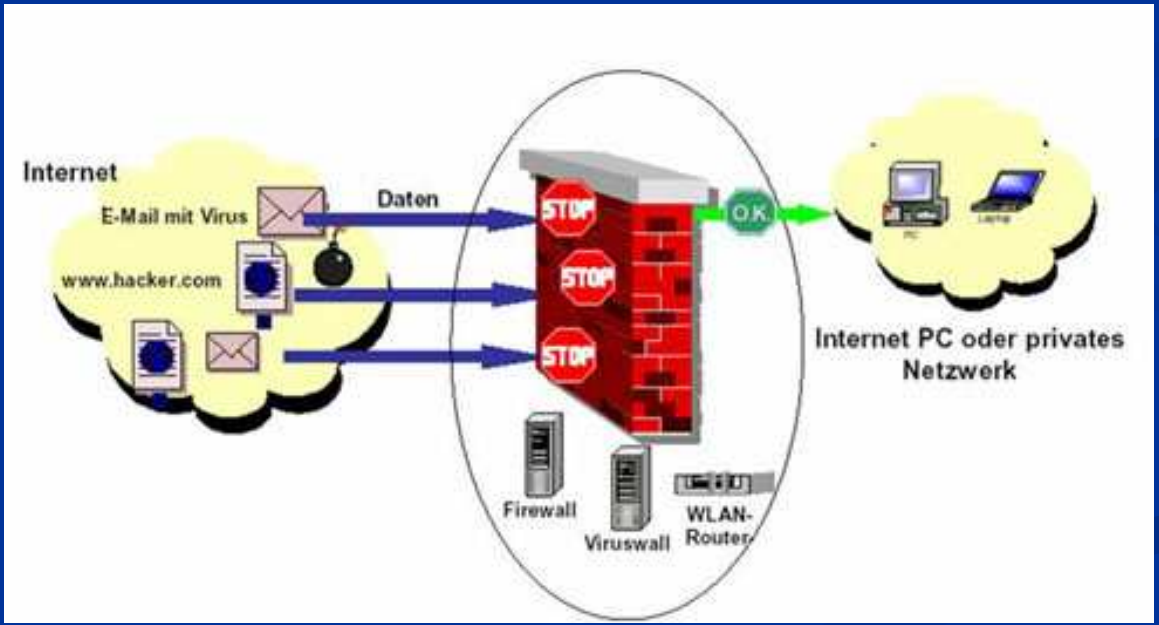
# Desktop Personal Firewall und Virenscanner

- Wie funktioniert eine Firewall?
  - Anwendungen, denen kein Zugriff gestattet werden soll, stehen auf der schwarzen Liste (Blacklisting)



# Desktop Personal Firewall und Virenscanner

- Wie funktioniert eine Firewall?
  - **Gefahr:** bei Netzwerkdiensten (z.B. Onlinespiele) können diese ebenfalls abgeschaltet und bei falscher Einstellung (Regel) unterbunden werden



# Desktop Personal Firewall und Virenscanner

- Welche unterschiedlichen Firewall-Technologien gibt es?
  - Paketfilter
    - Filterung von Datenpaketen anhand von Ziel-Port, Quell- und Ziel-Adresse (Grundfunktion von Netzwerk-Firewalls)
    - Prüfung erfolgt anhand von aufgestellten Regeln

# Desktop Personal Firewall und Virenscanner

- Welche unterschiedlichen Firewall-Technologien gibt es?
  - Stateful Inspection
    - eine erweiterte Form der Paketfilterung
    - jedes Paket wird einzeln betrachtet und bewertet, ob es gültig ist oder nicht
    - Die zustandsgesteuerte Filterung merkt sich den Status einer Verbindung und kann ein neues Datenpaket einem zusammenhängenden logischen Datenstrom zuordnen
    - Diese Information dient als weiteres Filterkriterium

# Desktop Personal Firewall und Virenscanner

- Welche unterschiedlichen Firewall-Technologien gibt es?
  - Application-Layer-Firewall
    - beachtet zusätzlich zu den reinen Verkehrsdaten wie Quelle, Ziel und Dienst noch den Inhalt der Netzwerkpakete
    - Content-Filter
      => Eine Firewall kann mit Hilfe eines Inhalts- oder Content-Filters die Nutzdaten einer Verbindung auswerten

# Desktop Personal Firewall und Virenscanner

- Welche unterschiedlichen Firewall-Technologien gibt es?
  - Application-Layer-Firewall
    - beachtet zusätzlich zu den reinen Verkehrsdaten wie Quelle, Ziel und Dienst noch den Inhalt der Netzwerkpakete
    - Wird unterschieden in:
      - Content-Filter
      - Proxy

# Desktop Personal Firewall und Virenscanner

- Welche unterschiedlichen Firewall-Technologien gibt es?
  - Intrusion Detection und Intrusion Prevention Systeme
    - erkennen einen Einbruchsversuch anhand von Kommunikationsmustern
    - Intrusion Detection System erkennt einen Angriff
    - Intrusion Prevention System versucht diesen zu blockieren

# Desktop Personal Firewall und Virenscanner

- Was muss ich beim Umgang mit einer Firewall beachten?
  - Regelmäßige Updates und Upgrates
  - Keine Verbindungen zulassen, die einem nicht bekannt sind
  - Prüfen, welche Software auf dem Rechner installiert wird
  - Keine unsichern Daten auf dem Rechner installieren oder aus dem Internet herunter laden

# Desktop Personal Firewall und Virenscanner

## Sicher im Internet Surfen

# Desktop Personal Firewall und Virenscanner

- Desktop Personal Firewall
  - Was ist eine Firewall und wie wird sie unterschieden?
  - Wie arbeitet eine Firewall?
  - Was ist zu beachten?
- Virenscanner

# Desktop Personal Firewall und Virenscanner

- Desktop Personal Firewall ✓
  - Was ist eine Firewall und wie wird sie unterschieden?
  - Wie arbeitet eine Firewall?
  - Was ist zu beachten?
- Virenscanner
  - Was ist ein Virenscanner? (Definition, Unterschiede)
  - Wie arbeitet ein Virenscanner?
  - Was ist zu beachten?

# Antivirenscanner

# Was ist ein Antivirenprogramm?

- Ein Antivirenprogramm dient zum aufspüren, blockieren und ggf. beseitigen von bekannt Computerviren, Computerwürmern und Trojanischen Pferden
- Warum braucht man eine Solche Software?

  Die Anzahl der Bedrohungen, die Häufigkeit und die Ausbreitungsgeschwindigkeit der Attacken nehmen von Tag zu Tag zu. Deshalb ist Viren-Schutz für jeden User ein absolutes Muss.

# Welche Unterschiede gibt es bei der AV-Software?

- Echtzeitscanner
  - Arbeitet im Hintergrund als Systemdienst bzw. Daemon
- Manueller Scanner
  - Wird von Hand gestartet (On-Demand)
    - Online-Virenscanner
      - Der Programmcode und Viren-Muster werde über das Netzwerk geladen.
      - Nur im On-Demand Modus
- Sonstige Scanner
  - Analyse des Netzwerkverkehrs (Datenstrom scannen)

# Wie arbeiten Virenscanner? - Datenbanken

- Jeder Virusscanner hat eine Datenbank mit den Namen und Signaturen der Viren
- namhaften Virenscannerproduzenten unterhalten eigene *Virenlabors* und Spürtrupps
- Oft werden den Virenlabors Exemplare von betroffenen Anwendern zugesendet
  - Das Resultat dieser Analyse wird zum einen für akute Viren-Cleaner verwendet
  - kleine Stand-Alone Virenscanner für einen speziellen Virus,
  - Auch Signaturen werden gewonnen, die dann in der Signaturdatenbank eingepflegt werden

# Wie arbeiten Virenscanner? - Scannermodul

- das Aufspüren von Viren
- Durchleuchtung von potentiellen Opfer-Dateien und -Programmen, komprimierten Archiven, die Startbereiche der Datenträger und den Arbeitsspeicher
- Fund eines Musters oder einer Anomalie → Vergleich dieser mit Signaturen der Datenbank ("Pattern Matching").
- heuristische Analyse = zusätzlich emulierte Virenstrings und -verhaltensweisen ( siehe Heuristik) entdecken
- Fund eines Virus → Warnmeldung in audio-visueller Weise
  → Übergabe Ergebnis an Desinfizierer

# Wie arbeiten Virenscanner? - Virenschild

- speicherresidentes (also im Hintergrund arbeitendes) Scanmodul
- so einstellbar, dass in Realzeit alle Dateioperationen überprüft werden
- führt zu Einbußen in der Systemperformance

# Wie arbeiten Virenscanner - Desinfizierer

- Virus festgestellt → Desinfiziermodul tritt in Aktion
- Mehrere Möglichkeiten der Bereinigung
  - Datei vom Virenprogrammcode zu reinigen
  - Datei isolieren, durch verschieben in Quarantäneverzeichnis
  - Datei umbenennen oder ganz löschen

# Wie arbeiten Virenscanner? - Desinfizierer

- Bei heuristischer Analyse:
  - Möglichkeit die Datei von der Analyse auszuschließen oder zu überspringen, sollte aktiviert sein, da Fehlalarmen möglich
- netzwerkfähige Varianten:
  - werden in SMTP-Gateways, Proxyserver und Firewalls implementiert
  - zentral vom Systemadministrator gewartet
  - meist mit lokalen Virenscanmodulen auf einzelnen Arbeitsstationen verbunden

# Welche Technik wird angewandt?

- Reaktive Technik
  - Schädling wird erst erkannt, wenn im Hersteller entsprechende Signatur im AV-Programm hinterlegt
  - Klassische Antivirensoftware
- Proaktive Technik:
  - Zukunft der Virenerkennung
  - Bezeichnet die Erkennung von Viren ohne eine entsprechende Signatur (mit Heuristik o. SandBox)

# Was ist eine Heuristik oder eine Sand-Box?

- Heuristik
  - Suchen nach allgemeinen Merkmalen, um unbekannte Viren zu erkennen
  - Rudimentäres Intrusion System – IDS (für Grossrechner oder Netzwerk)
- SandBox
  - Gesicherte Umgebung für die Ausführung von Programmen
  - Datei wird aufgeführt und analysiert welche Aktionen sie ausführt

# Probleme bei Virenscannern

- Evtl. haben Anwendungen Probleme beim einscannen (Echtzeitscann).
  - Zeitliche Probleme: für einige Applikationen sind Scanns zu groß → Fehlermeldung
  - Datenbanken: Versuch des ständigen Zugriffs auf Datenmasse → Timeout, völliger Stillstand System
  - Mailserver: vom Mailserver werden infizierte Dateien gelöscht und werden von diesem nicht wiedergefunden → Funktionsstörungen