

# Präsentation IKS

- Desktop Personal Firewall (DPF)
- Virens Scanner

## Was ist eine Desktop Personal Firewall (DPF)?

- Software zum filtern von ein- und ausgehendem Datenverkehrs eines PC's
- Dient zum Schutz des Computers vor Würmern, Trojanern, Viren bei Nutzen des Internets oder eines lokalen Netzwerkes

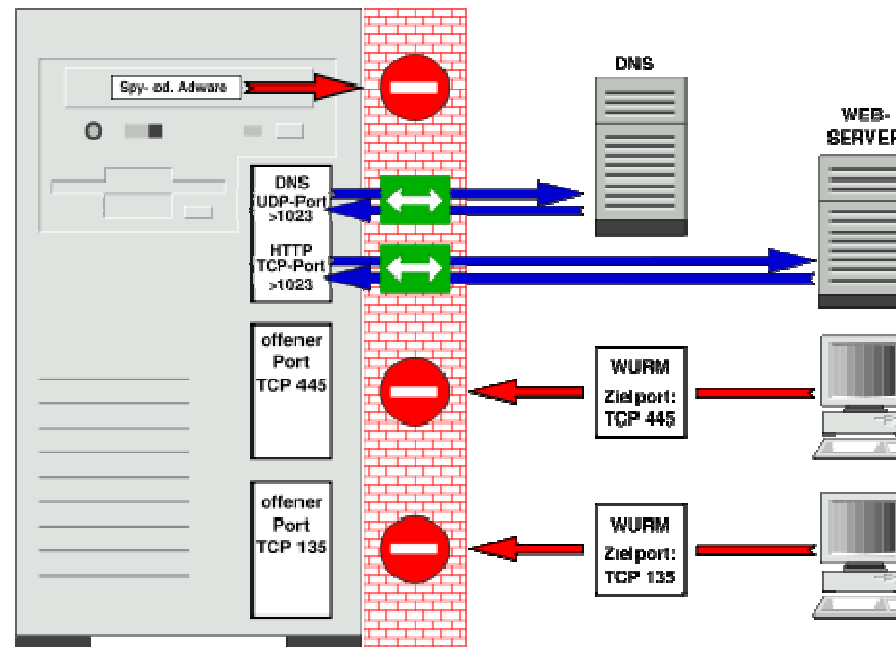
## Wie funktioniert eine Desktop Personal Firewall (DPF)?

- Datenpakete werden über das Netz zu anderen Rechnern gesendet
- Datenpakete haben eine Quell-Port-Nummer und eine Ziel-Port-Nummer
- Port-Nummern erlauben dem Betriebssystem die Zuordnung zu Anwendungsprogrammen

## Wie funktioniert eine Desktop Personal Firewall (DPF)?

- Der Paketfilter (TCP/IP) der DPF ermöglicht das Blockieren von ein- und ausgehenden Datenpaketen nach vorgegebenen Regeln
- Filterkriterien können Quell-und Zieladresse, Protokolle, sowie Quell- und Zielpport sein
- Ein Unterschied zu einer externen Firewall ist, dass einzelne Anwendungsprogramme (Word, Excel,etc) von der Netzkommunikation ausgeschlossen werden können

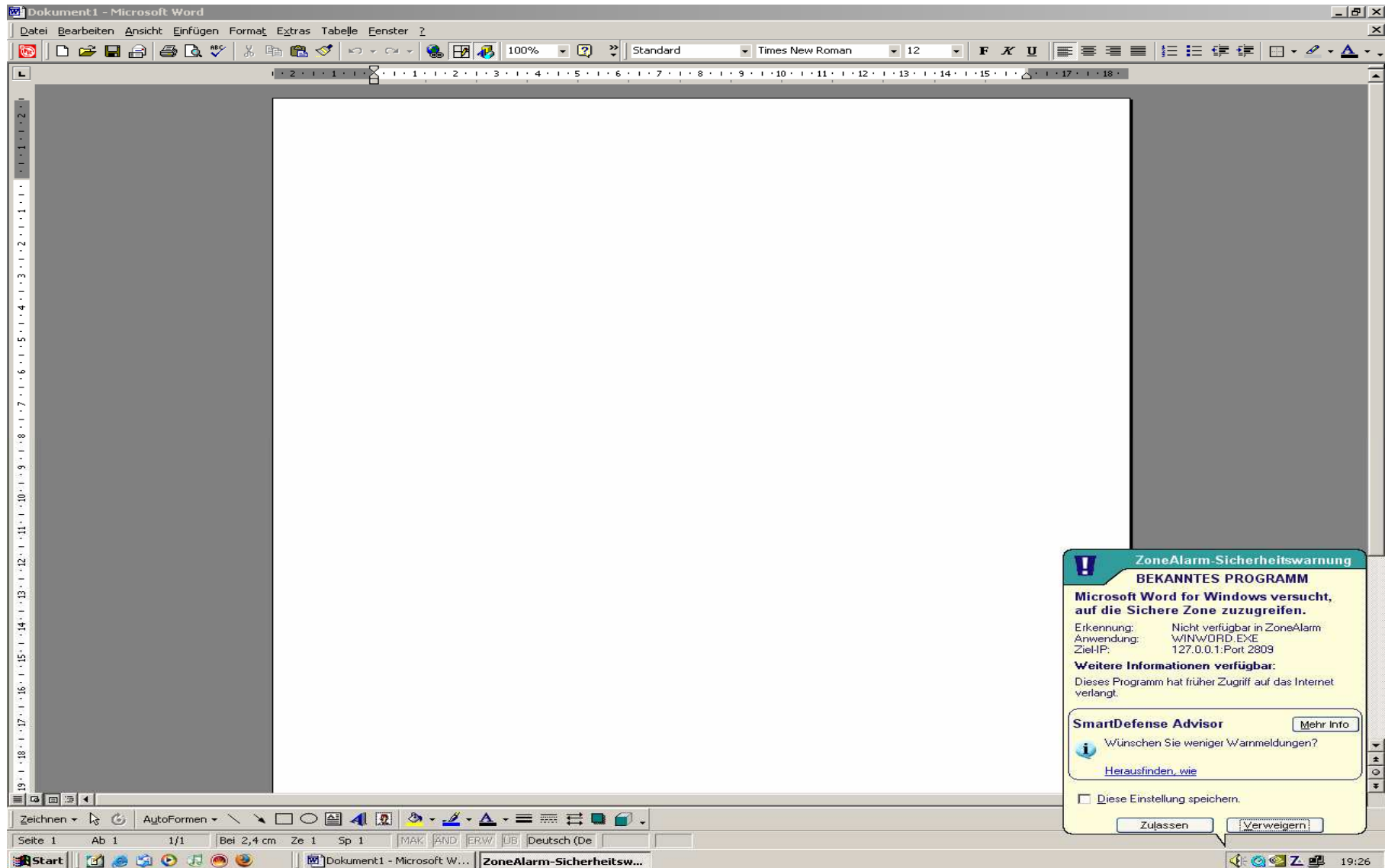
# Wie funktioniert eine Desktop Personal Firewall (DPF)?



## Welche weiteren Funktionen bietet eine DPF ?

- Lernmodus; durch Interaktion mit dem Benutzer können Regeln für den Paketfilter und Anwendungsfiler festgelegt werden (Dialogfenster)
- Content Filter; überprüfen & filtern Inhalte von Datenpaketen (JavaScript, HTML, Email-Anhänge)

# Interaktion mit Benutzer



## Welche weiteren Funktionen bietet eine DPF ?

- Einbruchserkennungs- und Abwehrsysteme
  - Intrusion Detection System (IDS)
  - Intrusion Prevention System (IPS)

Versuch durch Schadsoftware DPF zu umgehen, z.B. über Vertrauenswürdiges Programm (Browser) Verbindung herstellen

## Welche weiteren Funktionen bietet eine DPF ?

- Logfile; Protokollierung des Vorgehens des Paketfilters, so können Fehler bei der Netzwerkkonfiguration erkannt werden
- Automatische Updates

## Welche Sicherheitsmaßnahmen sollten zusätzlich zu einer DPF getroffen werden?

- Viren- und Spywarescanner
- regelmäßige Datensicherung
- Software Updates um Sicherheitslücken zu schließen
- Sichere Konfiguration von Webbrowser, Email-Programmen und Betriebssystemen

## Welche Personal Firewall Software gibt es?

- Windows Firewall; Bestandteil in XP und Vista
- ZoneAlarm; kostenlose und kommerzielle Version im Netz verfügbar
- Norton Personal Firewall; inkl. Antivirenpr.
- Norman Personal Firewall

# Anti-Virus-Software

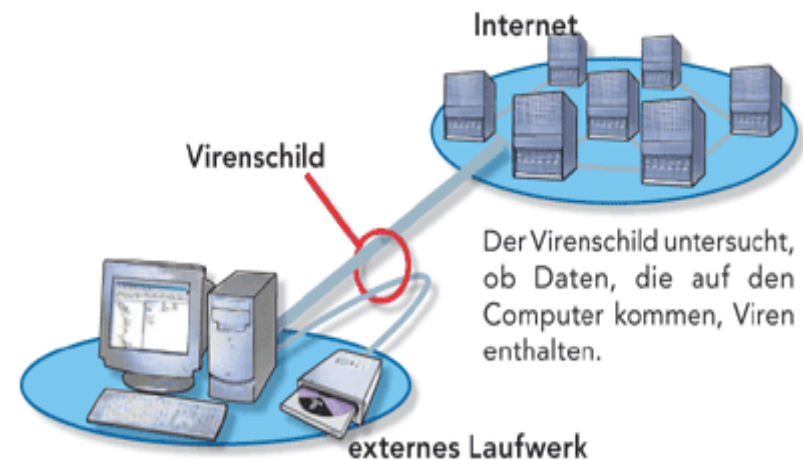


## Was ist eine Anti-Virus-Software?

- Eine Software die Eindringlinge wie Viren und Würmer (Malware) aufspürt und beseitigt.
- Warum braucht man sie?
- Weil ein Windows XP PC bei ungeschütztem Internetverkehr nach ca. 4 Minuten mit einem Virus oder ähnlichem infiziert ist.

# Woraus besteht Anti-Virus-Software?

- Virenbibliothek
  - Enthält Merkmale der Viren
- Virens Scanner
  - untersucht Festplatten und Daten
- Virenschild (Scanengine)
  - Überwacht alle Daten die neu auf den PC kommen



## Welche Anti-Virus-Software gibt es?

- Echtzeitscanner
  - arbeitet im Hintergrund als Zugriffsscanner
- Manuelle Scanner
  - wird automatisch von Hand gestartet
- Online Virens Scanner
  - Nur zum Reinigen, kein präventiver Schutz

# Wie funktioniert Anti-Virus-Software?

- **Reaktiv:**
  - Erkennung von Schädlingen wenn dem Programm eine Signatur vorliegt
- **Proaktiv:**
  - Erkennen von Viren auch ohne entsprechende Signatur mit Hilfe der Heuristik
- **Heuristik:**
  - Suchen nach allgemeinen Merkmalen der Viren

## Was leistet eine Anti-Virus-Software?

- Aufspüren, blockieren und beseitigen der folgenden Schädlinge:
  - Viren
  - Trojaner
  - Würmer
  - Backdoor (wartet auf Anweisung von außen)
  - Spyware (Spionageprogramme)

## Was leistet eine Anti-Virus-Software?

- Adware (Werbeprogramme)
- Dialer (Wählprogramme)
- Rootkits

(verdächtige Prozesse, Veränderung der Registry)

- Keylogger (Tastaturspione)
- Spam

## Zusammenfassung

- Was muss eine gute Anti-Viren-Software leisten?
  - Proaktiver Schutz durch Heuristik und permanenten Überwachung aller Prozesse
  - Berücksichtigung von Komprimierungsprogrammen
  - Berücksichtigung aller bekannten Schadprogramme
  - Leistungsfähiger Scanengine
  - Regelmäßige und automatische Updates

# Fazit

Maximaler Schutz durch Firewall und Virens Scanner

