Antivirenserver

Autor:	Marcel Hader, Thomas Refflinghaus
Lehrveranstaltung:	Netzwerksicherheit im 7. Semester, Angewandte Informatik
Termin:	Referat vom 26.01.2004
Ort:	Fachhochschule Gelsenkirchen
Schlagworte:	Symantec, Viren, Antivirenserver

© Thomas Refflinghaus, Marcel Hader, 2004

Antivirenserver

- Allgemeiner Überblick über Viren
- Deren Ausbreitung / Verbreitung
- Abhilfe / Gegenmaßnahmen

© Thomas Refflinghaus, Marcel Hader, 2004

Allgemeiner Überblick über Viren

Inhalt :

- Was sind Viren ?
- Arten von Viren
- Bekannte Viren und Auswirkungen
- Video
- Statistik der TopTen Viren

© Thomas Refflinghaus, Marcel Hader, 2004

Was sind Viren ?

- Aus der Biologie übernommene Bezeichnung für nicht selbständige Programmroutinen, die sich selbst reproduzieren und Manipulationen z. B. an der Betriebssystemsoftware oder anderen Programmen vornehmen.
- Computerviren sind immer Bestandteil eines ***Wirtsprogramms*** und arbeiten, wenn dieses ausgeführt wird.
- Durch Computerviren verursachte Schäden, sind insbesondere der Verlust oder die Verfälschung von Daten oder Programmen.

© Thomas Refflinghaus, Marcel Hader, 2004

Arten Von Viren

Mailwürmer	Viren	Makroviren	Trojaner
Selbstreproduzierende Programme	Selbstreproduzierende Programme	- - -	- - -
Infektion durch Schwachstellen in Mailprogrammen	Infektion durch Ausführen kompromittierter Executables	Infektion durch Ausführen kompromittierter Office-Dokumente	Infektion durch Ausführen kompromittierter Executables
Verbreitung via Mail	ggf. selbständige Verbreitung via Mail	ggf. selbständige Verbreitung via Mail	ggf. selbständige Verbreitung via Mail
Keine oder seltene Schadensfunktionen Eventuelle Dialer	Meistens mit Schadensfunktion	Oftmals mit Schadensfunktion	Öffnen von "Hintertüren" ins System Evtl. Keylogger

© Thomas Refflinghaus, Marcel Hader, 2004

Bekannte Viren und Auswirkungen

- Pakistani
- RTM
- Michelangelo
- ILOVEYOU
- W32/SQLSlammer

© Thomas Refflinghaus, Marcel Hader, 2004

Bekannte Viren und Auswirkungen 1/4

Pakistani

- erster MS-DOS-Virus von 1986
- Entwickelt von zwei Software - Händlern in Pakistan
- Die Händler verkauften billige Raubkopien von Originalsoftware .
- Sie legten jeder Softwarekopie den Virus bei, der den Zweck haben sollte, die Kunden an den Händler zu binden.
- Überraschenderweise verbreitete sich dieser Virus aber sogar bis in die USA.

© Thomas Refflinghaus, Marcel Hader, 2004

Bekannte Viren und Auswirkungen 2/4

Robert Morris alias RTM

- Wurm von November 1988 gehörte zu den effektivsten seiner Zeit.
- Bemerkenswert war die Verbreitung über vier verschiedene Mechanismen und seine falsch eingestellte Replikationsrate
- Über Schwachstellen in den Netzwerkprogrammen sendmail und finger sowie durch brute-force-Angriffe auf Passwörter verbreitete er sich innerhalb weniger Stunden über mehr als 2000 der rund 50.000 Unix-Systeme im damaligen Arpanet und legte sie mit tausenden von Prozessen lahm.
- Es war ein außer Kontrolle geratenes Experiment des Studenten, dessen Vater damals als wissenschaftlicher Leiter des NCSC (National Center for Supercomputing) tätig war

© Thomas Refflinghaus, Marcel Hader, 2004

Bekannte Viren und Auswirkungen 3/4

Michelangelo

- Boot-Virus aus den frühen 90'er Jahren.
- Überschreibt auf der Festplatte die ersten 17 Sektoren in jeder Spur , Köpfe 0 bis 4 und macht somit die erste Partition unbrauchbar. Auf 360 KB-Disketten zerstört er die ersten 17 Sektoren jeder Spur.
- Auch wenn Michelangelo heutzutage als ausgestorben gelten darf, so gab es dennoch in den letzten Jahren noch zwei Mailwürmer, die ihn als Payload (Mechanismen zu Ihrer Verbreitung) mit sich führten.
- Der Name wurde ihm von seinem Entdecker gegeben, der bemerkte, dass das Auslösedatum mit dem Geburtstag von Michelangelo, 6. März (1475), übereinstimmt.

© Thomas Refflinghaus, Marcel Hader, 2004

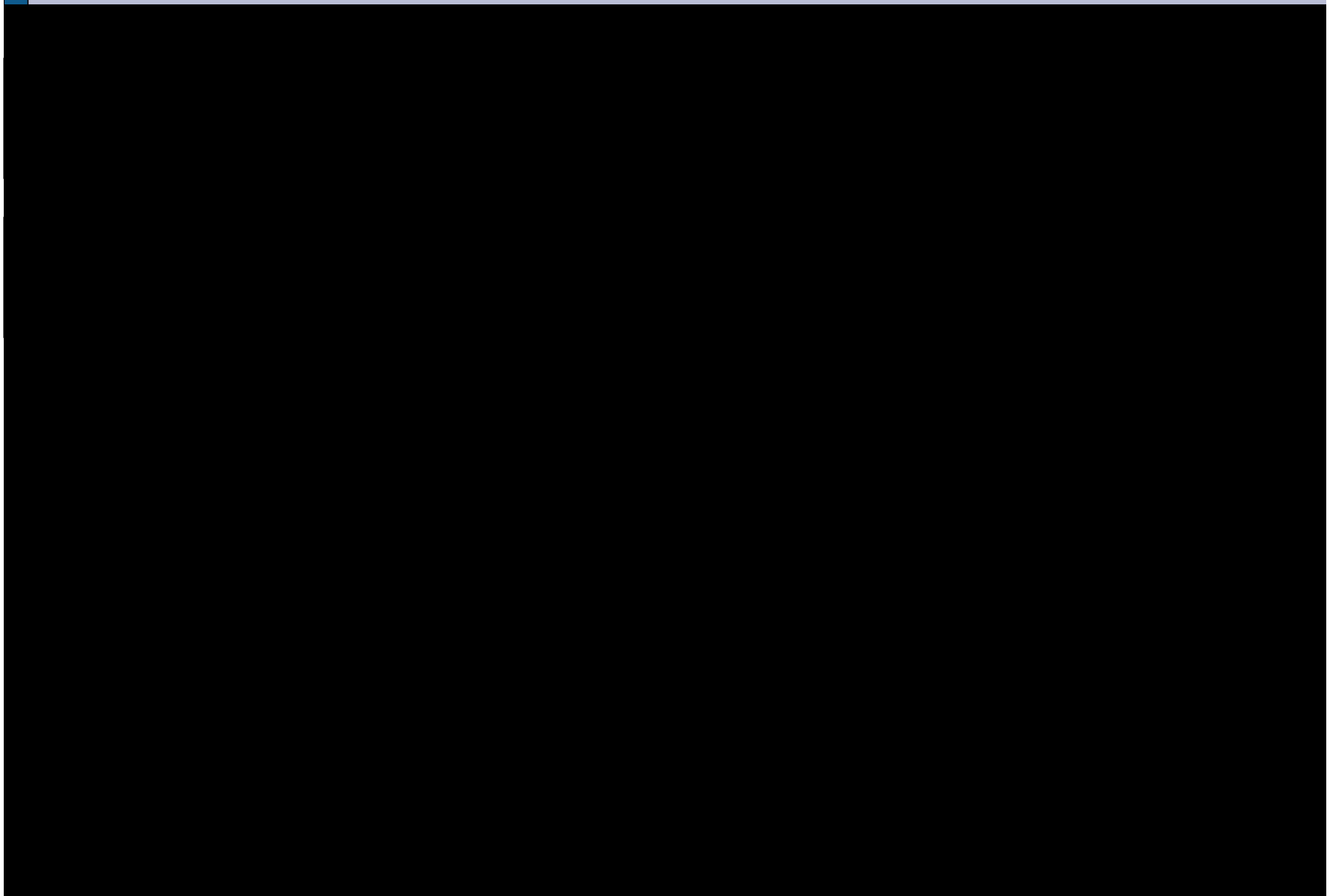
Bekannte Viren und Auswirkungen 4/4

ILOVEYOU 

- Massmailwurm vom 4.Mai 2000 der als Liebesbrief getarnt war
- Angriff auf die Mailserver zahlreicher Großunternehmen wie Verlage und Banken, sowie Behörden und Regierungen und legte sie zeitweilig lahm.
- Der bekanntere Name ILOVEYOU rührt vom Betreff der Mails her, über deren Anhang sich der Wurm verbreitete.
- Angriffsfläche war das Windows Scripting Host (WSH).
- Diese wurde von Microsoft bei Privatnutzer-Installation defaultmässig mit installiert .

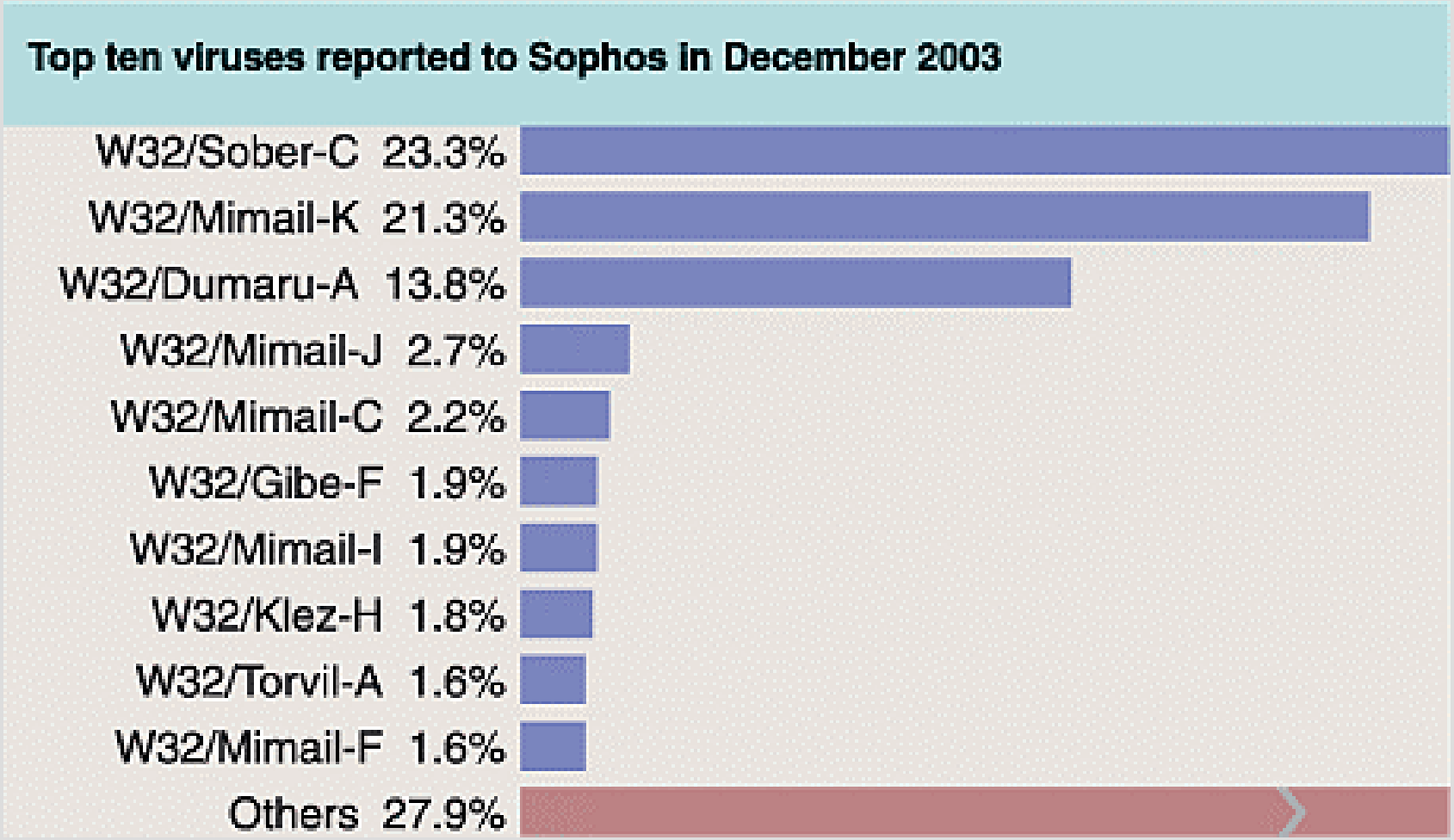
© Thomas Refflinghaus, Marcel Hader, 2004

Pro7 Video vom 07.01.04



Statistik der TopTen Viren 1/2

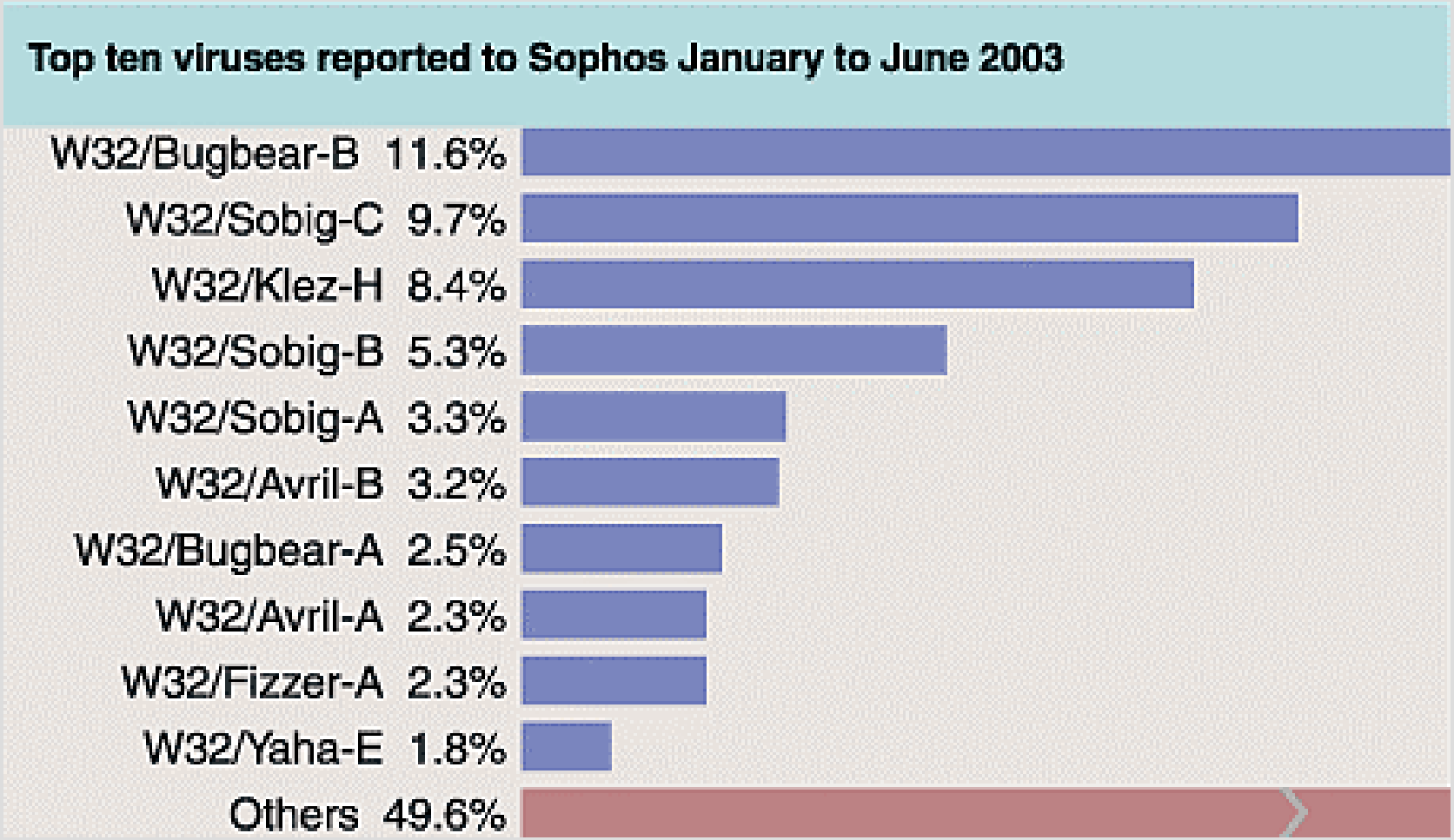
Top Ten Dezember 2003



© Thomas Refflinghaus, Marcel Hader, 2004

Statistik der TopTen Viren 2/2

Top Ten Januar bis Juni 2003

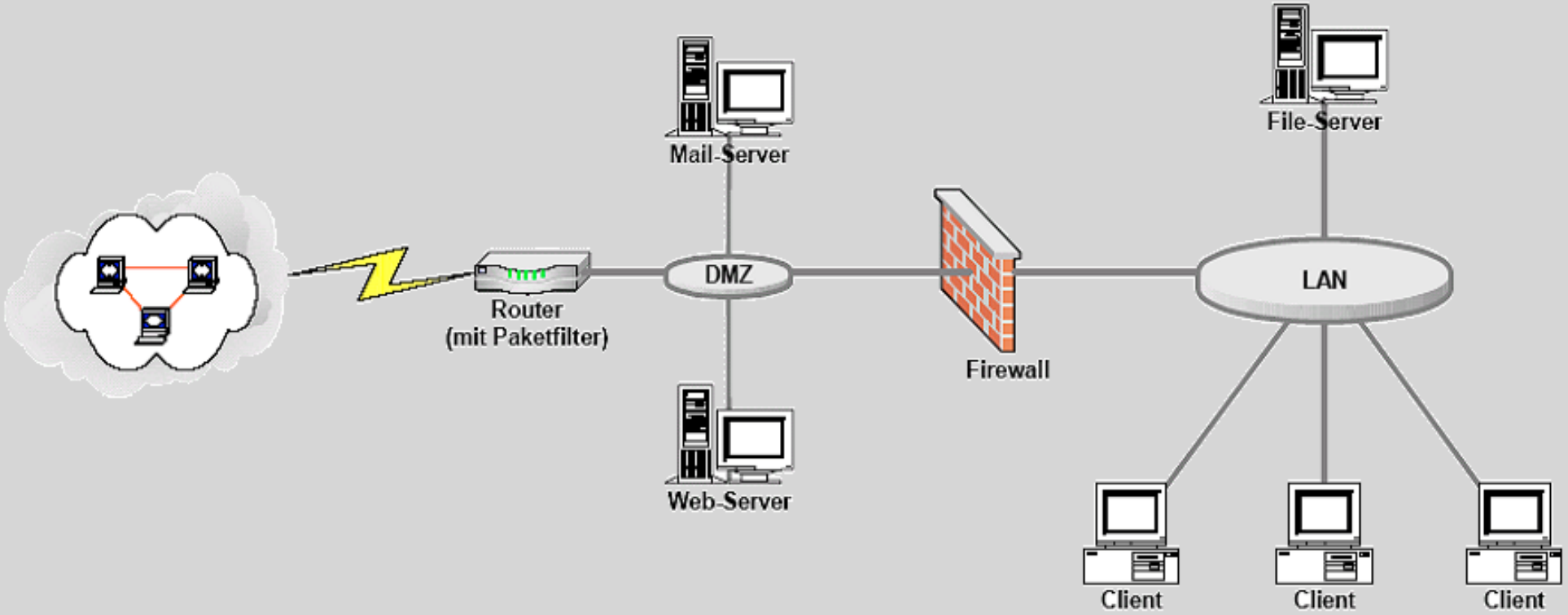


© Thomas Refflinghaus, Marcel Hader, 2004

Ausbreitung /Verbreitung

- Mailwürmer
- Viren
- Trojaner

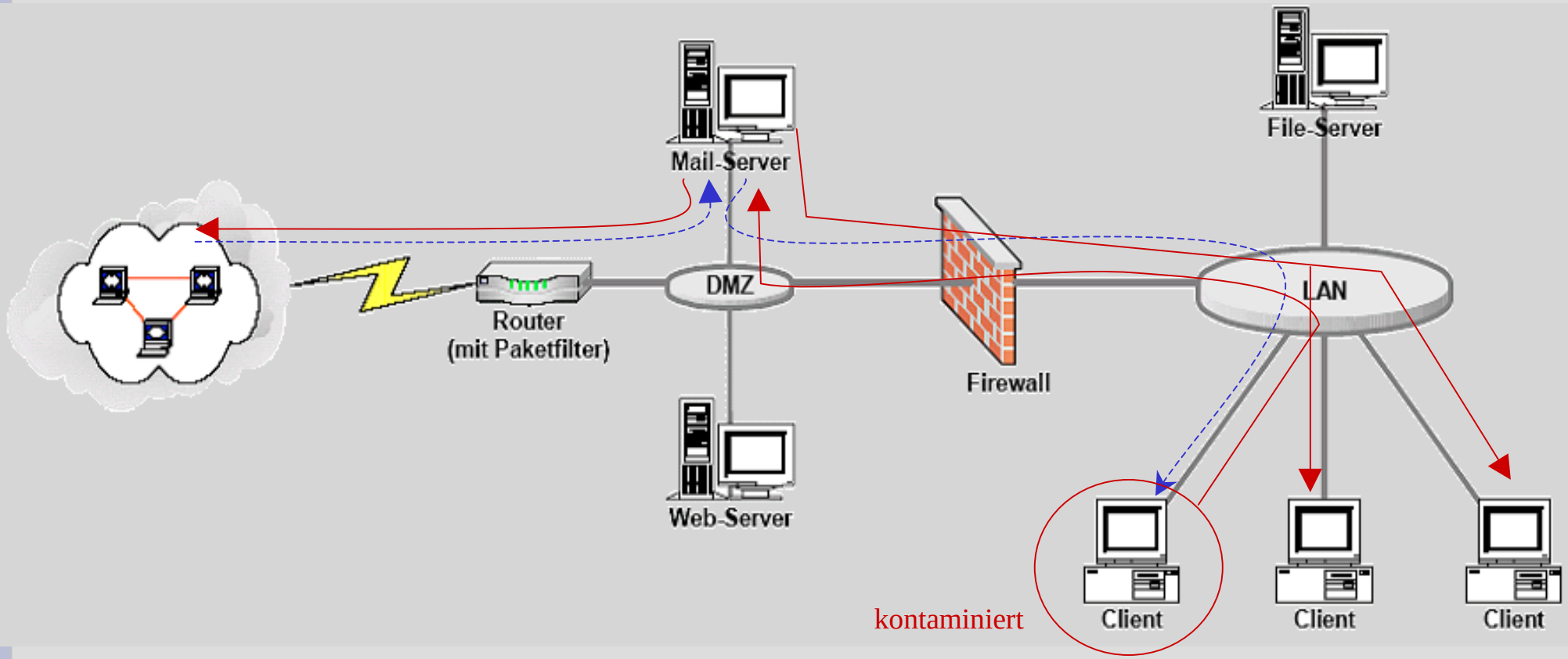
In einer Netzwerkstruktur (kleines/mittelständiges Unternehmen)



© Thomas Refflinghaus, Marcel Hader, 2004

Ausbreitung /Verbreitung 1/3

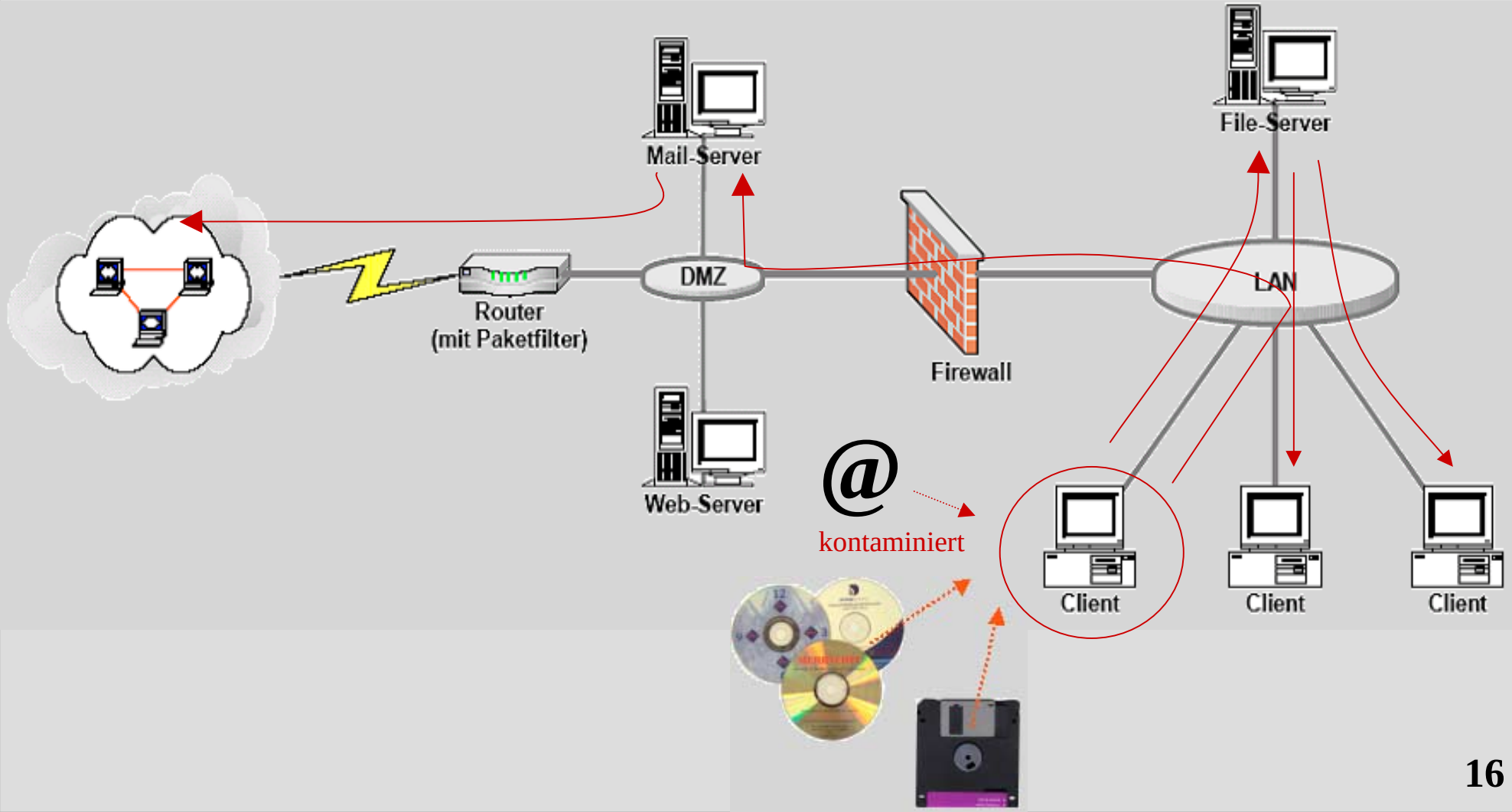
Mailwürmer



© Thomas Refflinghaus, Marcel Hader, 2004

Ausbreitung /Verbreitung 2/3

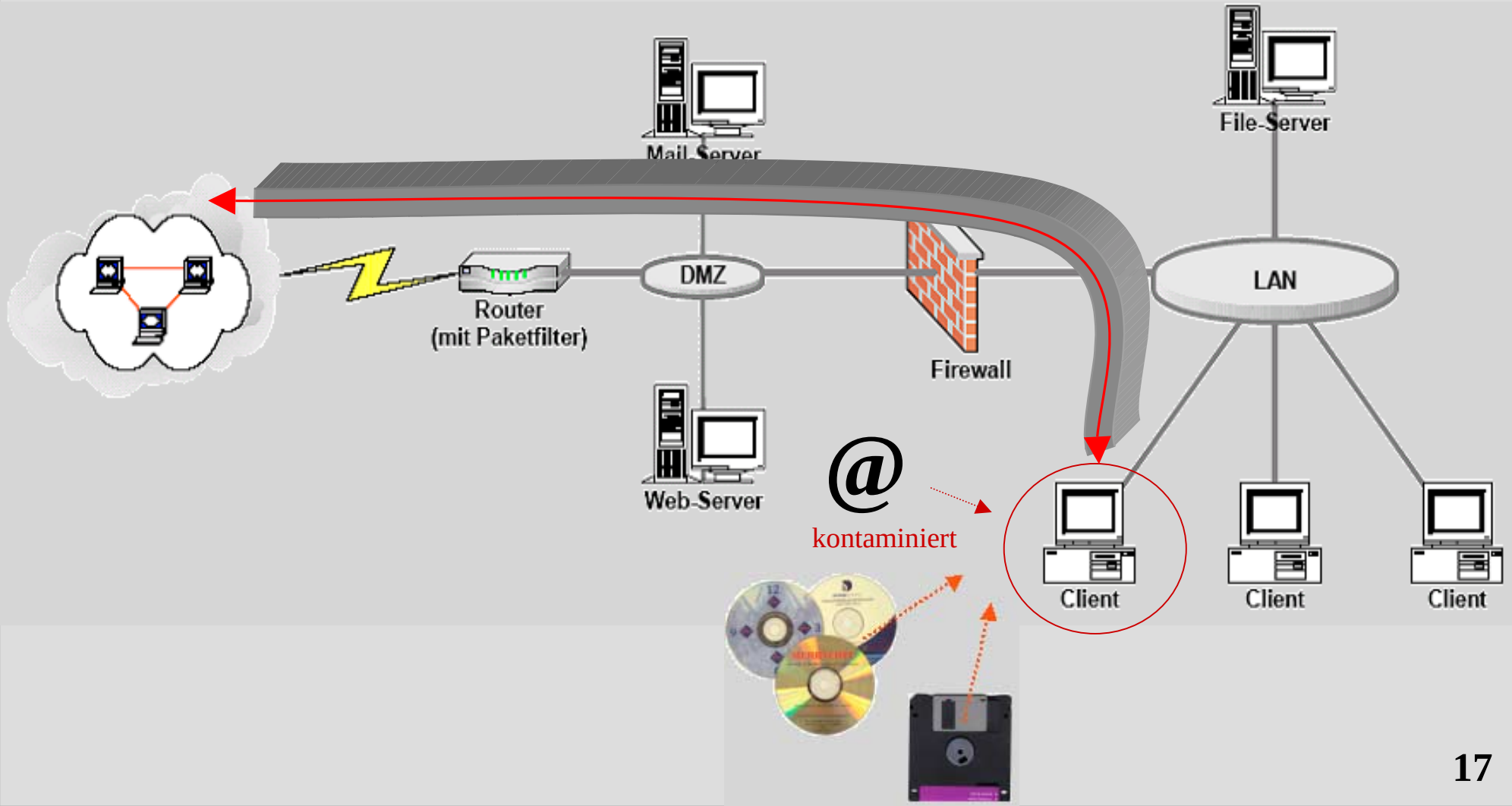
Viren



© Thomas Refflinghaus, Marcel Hader, 2004

Ausbreitung /Verbreitung 3/3

Trojaner



© Thomas Refflinghaus, Marcel Hader, 2004

Abhilfe / Gegenmaßnahmen

Abhilfe und Gegenmaßnahmen erklärt anhand eines Symantec Norton Antivirenservers

- Ausführliche Erläuterung von Komponenten
- Virenerkennungsverfahren
- Signaturen
- Firewall- und Gatewayvirenscanner
- Quellennachweis

© Thomas Refflinghaus, Marcel Hader, 2004

Komponenten 1/7

Servergruppen

- Eine Servergruppe dient als Behälter für Server und Clients, die dieselben Kommunikationskanäle verwenden.
- Auf allen Mitglieder dieser Gruppe ist es z.B. möglich eine Virenentfernung zu starten oder sie zu Konfigurieren.

© Thomas Refflinghaus, Marcel Hader, 2004

Komponenten 2/7

Primärserver

- Der Primärserver ist für die Konfigurationsfunktionen in der Servergruppe zuständig
- kann auch für die Aktualisierung der Virusdefinitionsdateien verantwortlich sein
- Der Primärserver gibt die Aufgabe an alle anderen Server der Servergruppe weiter

© Thomas Refflinghaus, Marcel Hader, 2004

Komponenten 3/7

Sekundärserver

- Server, die keine Primärserver sind, werden als „Sekundärserver“ bezeichnet
- Sie rufen Informationen vom Primärserver ab und nutzen sie gemeinsam mit den Clients

© Thomas Refflinghaus, Marcel Hader, 2004

Komponenten 4/7

Master-Primärserver

- Ein Master-Primärserver ist ein Primärserver, von dem andere Primärserver LiveUpdate-Informationen, z.B. Virusdefinitionsdateien und Produktaktualisierungen, abrufen.
- Wenn ein Master-Primärserver einrichtet wird, heißt das, dass nur ein Server auf die Website von Symantec zugreift, um neue Virusdefinitionsdateien herunterzuladen

© Thomas Refflinghaus, Marcel Hader, 2004

Komponenten 5/7

System Center

- ermöglicht Ihnen die Konfiguration aller Server- und vieler Client-Schutzoptionen für Windows-Clients.
- nur eine Installation erforderlich
- könnte aber auf beliebig vielen Computern installieren werden.

© Thomas Refflinghaus, Marcel Hader, 2004

Komponenten 6/7

Alert Management System

- Das Alert Management System (AMS²) ist ein Warnsystem, das bei Virenereignissen Warnungen erzeugt
- über Pager, E-Mail, SNMP - Traps oder andere Wege sendet

© Thomas Refflinghaus, Marcel Hader, 2004

Komponenten 7/7

Quarantine

- Infizierte Elemente, die mit den aktuellen Virusdefinitionen nicht repariert werden können, werden auf den infizierten Client vom Virenscanner isoliert
- Diese Elemente werden danach zum zentralen Isolationsbereich weitergeleitet
- Von Central Quarantine aus werden die infizierten Dateien zur Analyse an das Symantec AntiVirus Research Center (SARC) gesendet
- Durch das verwenden dieses Dienstes sollte berücksichtigt werden, dass schnell sehr viel Netzlast anfallen kann

© Thomas Refflinghaus, Marcel Hader, 2004

Virenerkennungsverfahren 1/4

Heuristisches Verfahren

- Mit heuristische Verfahren ist gemeint, ohne auf einen bereits bekannten Scan-Code zurückzugreifen, ein Virus zu erkennen.
- Ganze Datei zu scannen wäre recht aufwändig
- Deshalb wir nur der Anfang und das Ende einer Datei gescannt, wo sich der Virencode meistens befindet.
- Dabei wird nach klassischen Funktionsaufrufen der Viren, etwa den Zugriff auf einen Datenträger überprüft.

© Thomas Refflinghaus, Marcel Hader, 2004

Virenerkennungsverfahren 2/4

Statische Verfahren

- Das Antivirenprogramm greift auf Signaturen zurück, in der Bytefolgen gespeichert sind, die virentypische Aktionen ausführen
- Das Antivirenprogramm ist ebenfalls auf vorgespeicherte Codesequenzen angewiesen
- Aktionen, die einen Virus zwar identifizieren würden, die der Virus aber durch nicht gespeicherte Befehlssequenzen aktiviert, bleiben verborgen

© Thomas Refflinghaus, Marcel Hader, 2004

Virenerkennungsverfahren 3/4

Dynamische Verfahren

- Das dynamische heuristische Verfahren lässt das zu prüfende Programm einfach laufen, ohne Rücksicht auf Verluste
- Vor dem Programmstart erzeugt das Antivirenprogramm einen virtuellen Computer im Computer
- Das Programm hat aber keinen Zugriff auf den Datenbestand
- Die Folge des Schreibens, im virtuellen Bereich, gibt sehr genaue Auskunft darüber, ob es sich um einen Virenbefall handelt oder nicht.

© Thomas Refflinghaus, Marcel Hader, 2004

Virenerkennungsverfahren 4/4

Bloodhound-Technologie

- wartet nicht darauf, dass sich ein Virus durch einen Aufruf zu erkennen gibt
- sondern versucht durch intelligente Verfahren einen Virus zu aktivieren
- Mit diesen Verfahren schafft es Norton Antivirus, unbekannte Viren mit einer **Sicherheit von bis zu 90%** zu erkennen (laut Symantec)

© Thomas Refflinghaus, Marcel Hader, 2004

Signaturen 1/9

Was sind Signaturen?

- beinhalten unschädliche Codeteile oder Virusdefinitionen für bekannte Viren
- Jeder Client und Server hat seine eigene Virusdefinitionsdatei

© Thomas Refflinghaus, Marcel Hader, 2004

Signaturen 2/9

Aktualisierungsverfahren

- Transportverfahren
- LiveUpdate
- Intelligent Updater

© Thomas Refflinghaus, Marcel Hader, 2004

Signaturen 3/9

Transportverfahren

- Durch dieses Verfahrens können die Verteilung der aktualisierten Virusdefinitionen auf allen Servern und Clients in Ihrem Netzwerk automatisieren werden

- Es sollte lediglich ein Computer in einem Netzwerk so konfiguriert werden, dass er die neueste Virusdefinitionsdatei von der Symantec abruft

© Thomas Refflinghaus, Marcel Hader, 2004

Signaturen 4/9

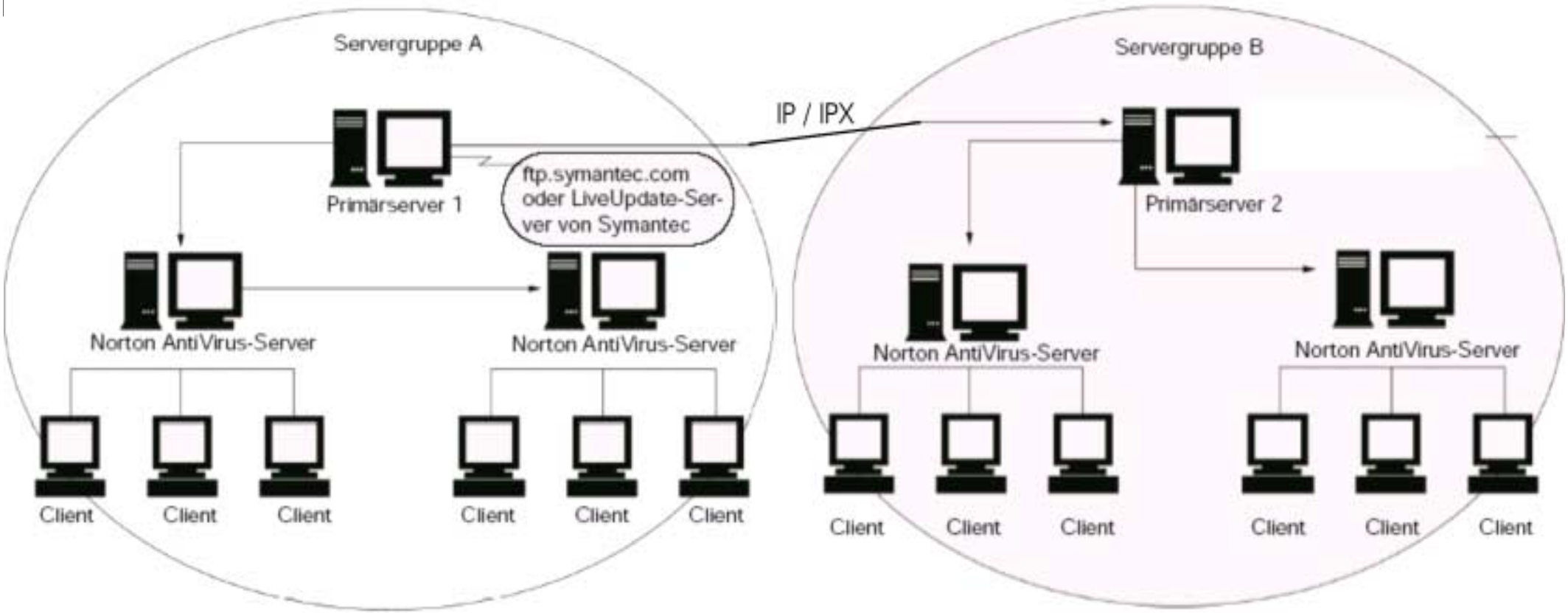
Live Update

- Der Hauptvorteil von LiveUpdate liegt in der geringen Größe der Microdefs- Datei
- Microdefs: Nur der Teil der Datei, der neue Daten enthält
- Jeder Client kann eine direkt Verbindung mit dem Symantec Live-Updateserver herstellen
- Oder zu einem intern Updateserver
- Nachteil: Hohe Netzlast
- Vorteil: für Mobile Benutzter die nicht immer zu einen intern Updateserver in Verbindung stehen

© Thomas Refflinghaus, Marcel Hader, 2004

Signaturen 5/9

Beispiel



Signaturen 6/9

Intelligent Updater

- Sind selbstextrahierende, ausführbare Dateien.
- Aktualisierung wird vom Benutzer jedes Mal selber ausgeführt.
- Für Clients interessant die nicht ans Internet oder Netzwerk angeschlossen werden können

© Thomas Refflinghaus, Marcel Hader, 2004

Signaturen 7/9

Verifizierung von Signaturen

- Virensignaturdateien können mit Hilfe des MD5 Hashalgorithmus überprüft werden

© Thomas Refflinghaus, Marcel Hader, 2004

Siganturen 8/9

http://www.symantec.de/avcenter/download/md5-hash.txt

AC6C558C7296645954F82917CD30C19A 20040116-006-i32-3.zip

C:\WINDOWS\system32\cmd.exe

```
C:\AOL 8.0\download\Virenserver\Signaturen\MD5>md5 20040116-006-i32-3.zip
AC6C558C7296645954F82917CD30C19A  20040116-006-i32-3.zip

C:\AOL 8.0\download\Virenserver\Signaturen\MD5>_
```

© Thomas Refflinghaus, Marcel Hader, 2004

Signaturen 9/9

Symantec AntiVirus Research Center (SARC)

- Infizierte Dateien die mit aktuellen Virusdefinitionen nicht repariert werden können werden über die Central Quarantine aus zur Analyse an das Symantec AntiVirus Research Center (SARC) gesendet.
- automatische Analyse der eingeschickten infizierten Dateien
- Die Virusdefinitionen, die zur Entfernung der Viren benötigt werden, können ohne menschliche Hilfe erstellt werden.

© Thomas Refflinghaus, Marcel Hader, 2004

Firewall- und Gatewayvirenscanner 1/3

zwei Arten:

- Virenscanner direkt auf der Firewall
- Und/oder auf einem Gateway

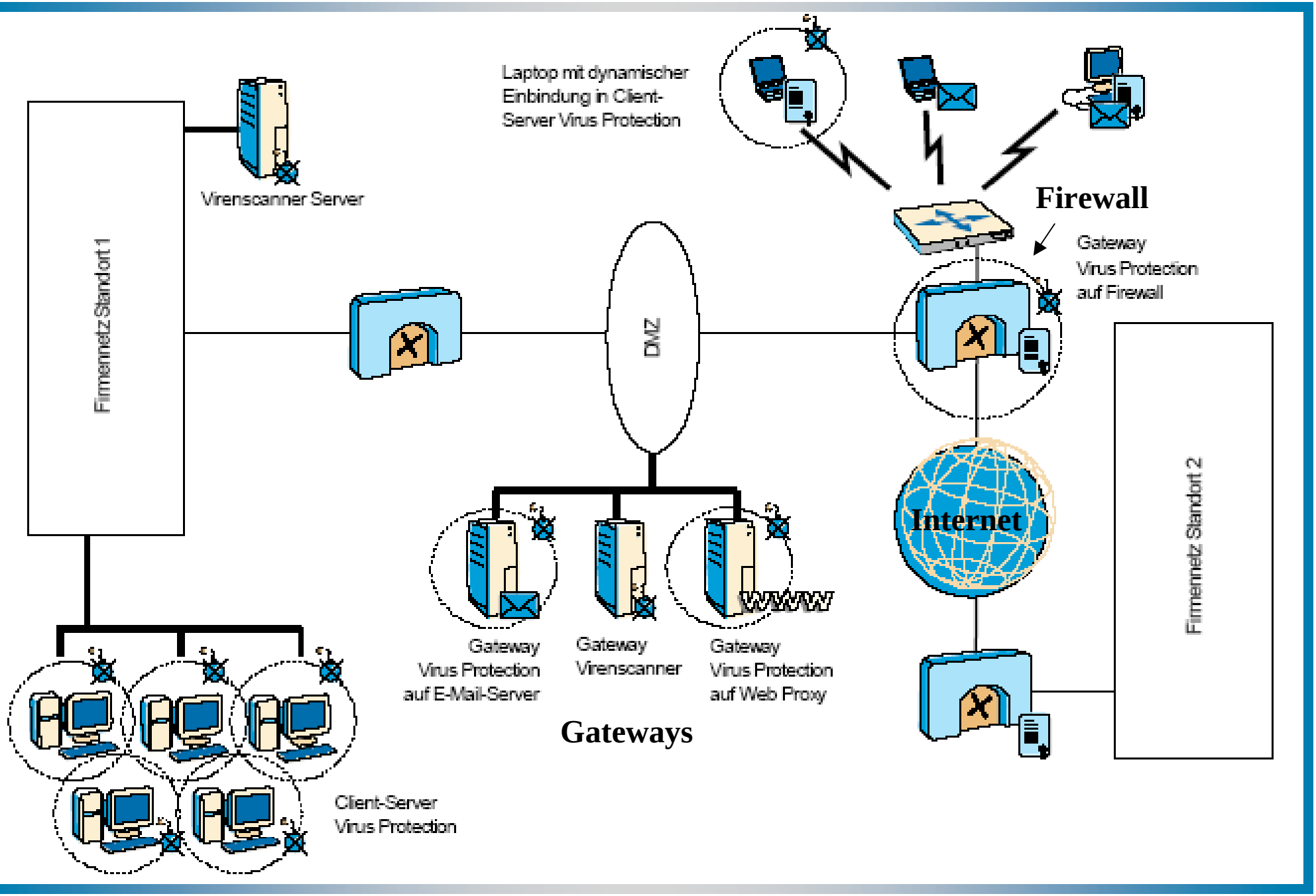
© Thomas Refflinghaus, Marcel Hader, 2004

Firewall- und Gatewayvirenscanner 2/3

- Durch diese Art von Scannern werden infizierte E-Mails isoliert bevor sie den Anwender erreichen und sich der Virus verbreitet
- Viruse könne auch über Protokolle wie HTTP und FTP in Unternehmen gelangen
- Eingehenden Datenströme von einer Firewall oder einem Proxyserver werden auf einen Virenscanner zur Prüfung umgeleitet und es wird so sichergestellt, dass den Anwender nur bereinigte Daten erreichen

© Thomas Refflinghaus, Marcel Hader, 2004

Firewall- und Gatewayvirenscanner 3/3



© Thomas Refflinghaus, Marcel Hader, 2004

Quellennachweis

Internetseiten:

www.symantec.com

www.symantec.de

www.sophos.de

http://www.bsi.de/av/virbro/kap1/kap1_1.htm

Bücher:

Symantec, Norton AntiVirus Corporate Edtion Update-Handbuch, (Version 7.6), Irland 2000

Symantec, Norton AntiVirus Corporate Edtion Implementierungshandbuch, (Version 7.5), United Stats of America 2000

Symantec, Symantec System Center Implementierungshandbuch, (Version 4.0 & 4.5), Irland 2000

© Thomas Refflinghaus, Marcel Hader, 2004

Antivirenserver

Haben Sie noch Fragen?

The End.

© Thomas Refflinghaus, Marcel Hader, 2004