

Viren - Wie sicher ist Mobile Commerce?



Patrick Heinen
Systems Engineer
Symantec (Deutschland) GmbH

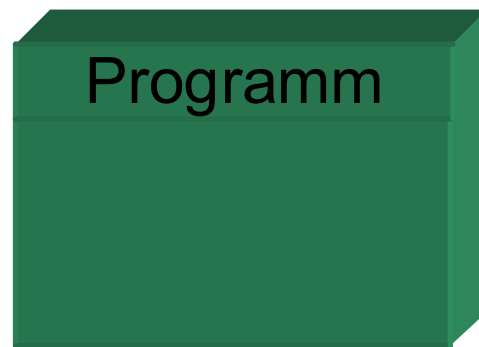
Inhalt

- Viren, Würmer und Trojaner
 - Definition
 - Funktion
 - Typen
 - Geschichte
- Virensclannern - Abwehrmechanismen
 - Anforderungen
 - Komponenten
 - Funktionen
 - Komponenten im Backend

Virus – Definition und Aufbau

Definition:

*Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt.
(Definition nach BSI Virenbroschüre)*



Original



Infiziert

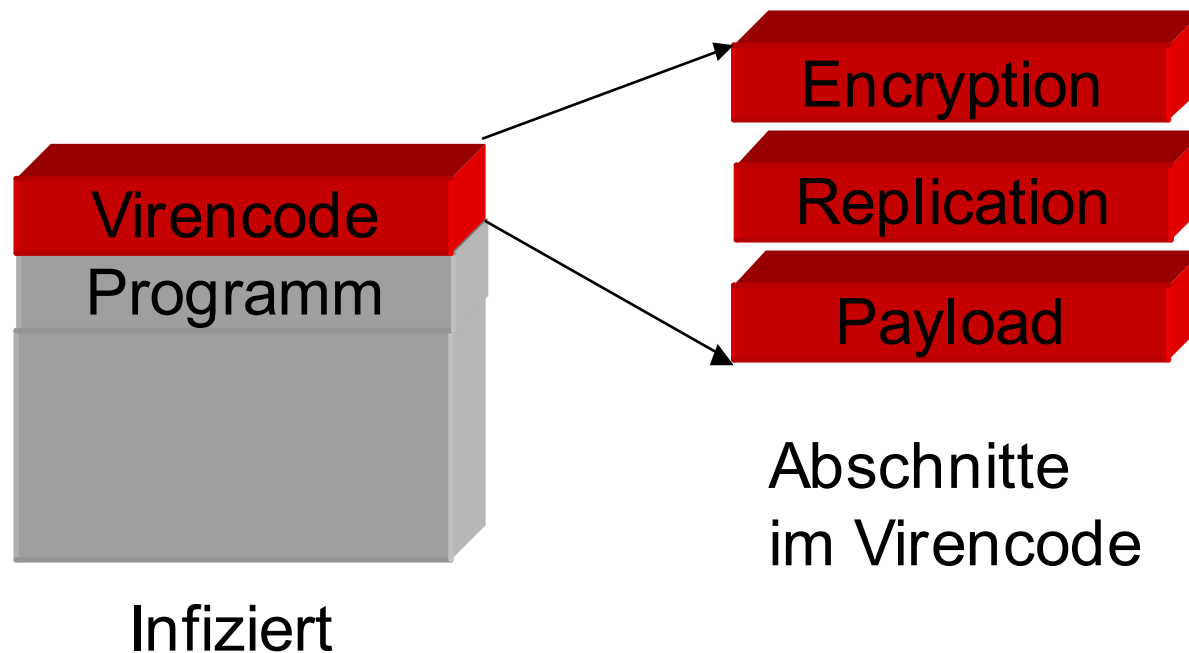
Funktionen des Virencodes

- Der Virencode ist nicht selbständig – d.h. er kopiert sich an bestehende Programme an (Befall, **Reproduktion**)
- In vielen Fällen dienen Viren dazu, **Schaden** anzurichten. In diesem Fall enthält der Virencode entsprechende Kommandos, um z.B. Daten zu löschen oder zu verändern.
- Die Abschnitte zur Reproduktion und zum Schaden sind oftmals an **Bedingungen** geknüpft. So wird i.d.R. eine bereits befallene Datei nicht erneut befallen. Ein Schaden wird evtl. nur an bestimmten Tagen angerichtet.
- Da die reine Reproduktion schon zu Veränderungen an Programmdateien führen, ist eine Befall oft leicht zu entdecken. Um diese Änderungen vor dem Anwender zu verstecken kommen z.T. Mechanismen zur **Tarnung** zum Einsatz.

Tarnen und Täuschen

- **Verschlüsselung**

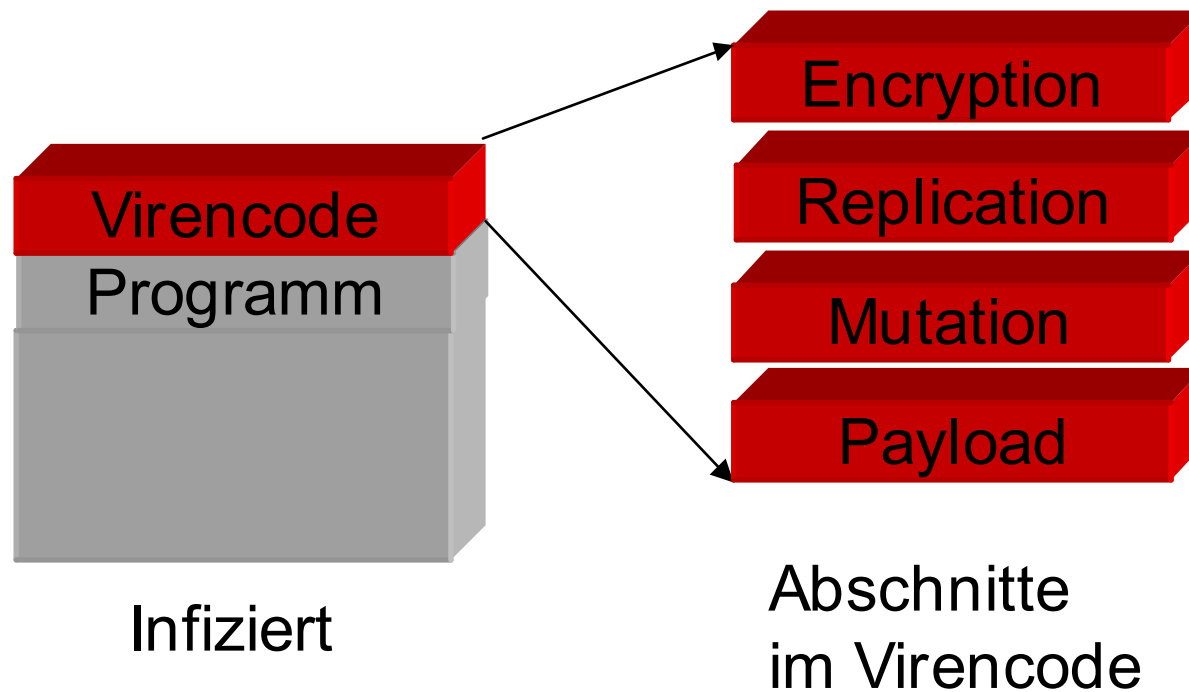
Um sich vor einem Virens Scanner zu verstecken, verschlüsselt sich der Virus (mit wechselnden Schlüsseln), so dass er in Form der ausführbaren Datei nicht erkannt werden kann.



Tarnen und Täuschen

- **Polymorphe Viren**

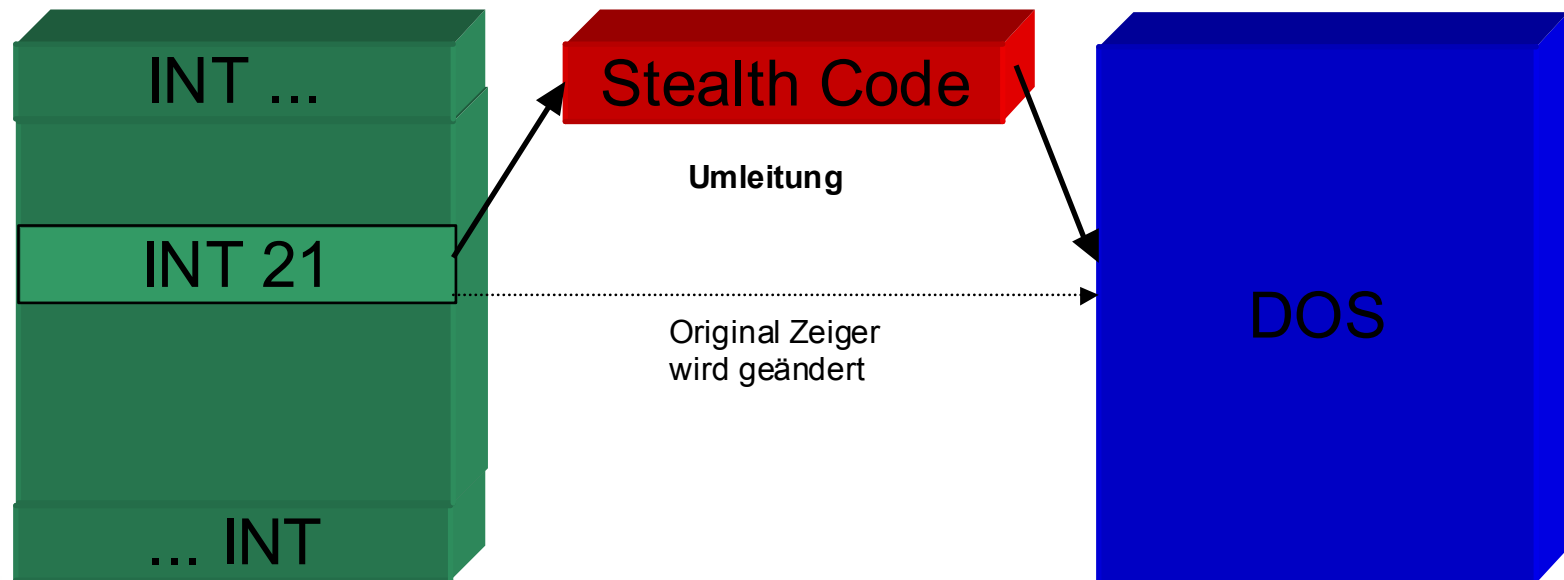
Als Weiterentwicklung zur „einfachen“ Verschlüsselung wird der Programmcode zur Verschlüsselung bei jeder Infektion verändert (Mutation).



Tarnen und Täuschen

- **Stealth Viren**

Der Virus verändert vom Betriebssystem zur Verfügung gestellte Routinen (z.B. INT 21 unter DOS) und verändert diese, so dass der Originalzustand der befallenen Dateien vorgetäuscht werden kann.

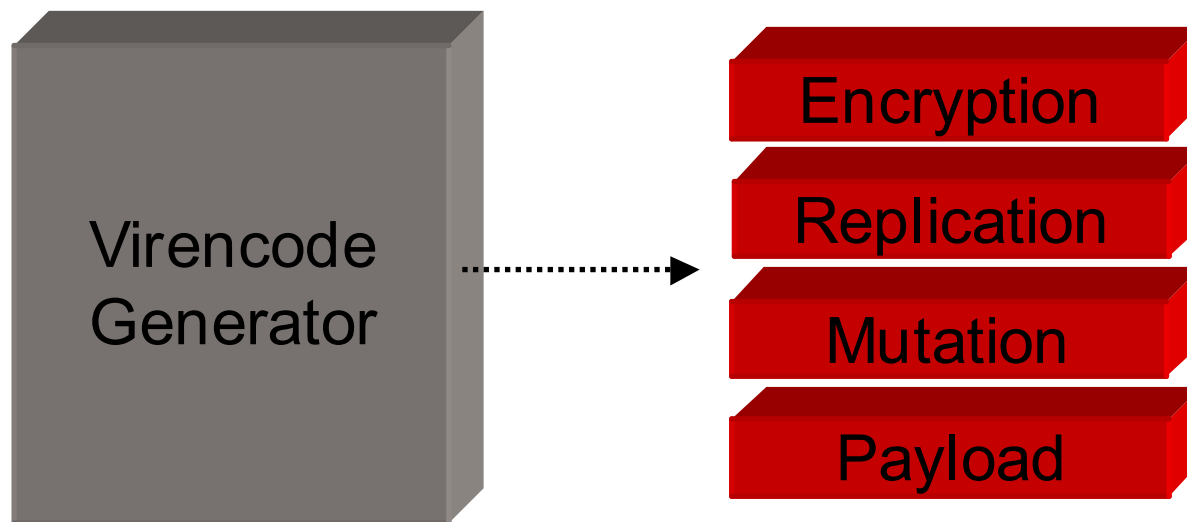


IRQ Table

Tarnen und Täuschen

- **Mutationen – Varianten**

Veränderungen müssen nicht notwendig durch den Virencode selber durchgeführt werden. Auch über externe Programme kann der Code derart verändert werden, dass er die gleiche Aufgabe erfüllt, aber ein anderes Erscheinungsbild besitzt.



Typen von Viren

- **Boot-Virus:**
Zum Start eines Betriebssystems wird i.d.R. Programmcode verwendet, der im sogenannten Bootsektor einer Festplatte, bzw. einer Diskette abgelegt ist. Befällt ein Virus diesen Bereich kann er bereits zum Start des Systems aktiv werden.
- **Datei-Virus:**
Diese Art des Computer-Virus kopiert sich an eine bestehende ausführbare Datei (Programm) an. Hier wird z.B. der Virencode ausgeführt, bevor er die Kontrolle an das befallene Programm übergibt.
- Denkbar ist eine Reproduktion bzw. ein Schaden, die/der nur zur Laufzeit des Virencodes geschieht, also während des Aufrufs des befallenen Programms.
- Alternativ kann sich der Virus als Teil Betriebssystem, oder als abgesetzter Prozess einbinden.

Makro-Viren

- Mit dem Aufkommen von immer komfortableren Office-Anwendungen wurden zunehmend auch immer leistungsfähigere Makrosprachen implementiert.
- Heute lassen sich fast alle komplexeren Anwendungen unter Microsoft Windows mit Hilfe von VBA (Visual Basic for Applications) steuern.
- In den Anwendungen können oftmals Routinen hinterlegt werden, die beim Öffnen einer Datei aktiv werden.
- Somit ist es möglich die Reproduktion und auch Schadensfunktionen in einer höheren Programmier- oder Scriptsprache zu schreiben und Nicht-Programmdateien zu befallen, die einer anderen Anwendung als Laufzeitumgebung bedürfen.

Würmer

- Würmer können sich wie Viren vermehren. Dabei verbreiten sie sich aber nicht von Datei zu Datei, sondern von Rechner zu Rechner, und infizieren das System.
- Würmer duplizieren sich selbst (beispielweise per E-Mail) auf die einzelnen Computer im Netzwerk. Da hierfür keine Interaktion mit dem Benutzer erforderlich ist, können sich Würmer sehr viel schneller verbreiten, als Computerviren.



Trojanische Pferde

- Trojaner werden in der Regel durch das Herunterladen von Programmen eingeschleppt, die harmlos oder interessant erscheinen oder Versprechungen machen. Wird das Programm heruntergeladen und ausgeführt, beginnt der schädliche Code sein Werk.
- Der Unterschied zwischen Viren und Trojanischen Pferden besteht darin, dass Trojanische Pferde sich nicht vermehren oder von sich aus weiterverbreiten. Sie können nur absichtlich per E-Mail oder Datenträger übertragen oder direkt auf den PC heruntergeladen werden.

Aufstieg ...

- Computer benötigen zum Betrieb ein Betriebssystem (OS). Viren sind i.d.R. für ein bestimmtes OS geschrieben und nur auf diesem lauffähig.
- Computerviren folgen der am meisten verbreiteten Technologie, um eine möglichst große Verbreitung erreichen zu können.
- Die zunehmende Vernetzung von Computern und PDAs erleichtert den Viren die Verbreitung mit Hilfe der Netze (lokale Netze und später Internet).

... und Fall von Viren

- Der 6. April 1992 (Windows 3.1) führte dazu, dass viele DOS basierte Viren nicht mehr funktionierten.
- Ab Ende 1995 erscheinen die ersten Makro-Viren für Microsoft Office.
- In 1996 nimmt die Verbreitung von Bootsektor-Viren deutlich ab, was auf die zunehmende Einführung von Windows 95 und Windows NT zurückzuführen ist.

Aber:

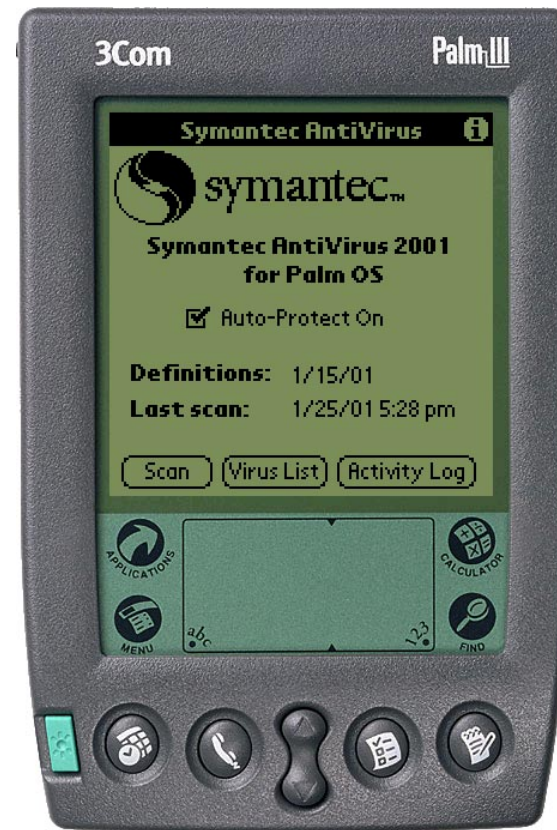
- Dafür entstehen nun die ersten Viren für die Windows Plattform.
- Viren für neue Betriebssysteme und Geräte tauchen mit einer zunehmenden Verbreitung auf (Linux, Palm).

Ausgangsbasis heute

- Es sind über 50.000 bösartige Programme bekannt.
- 250 – 350 davon befinden sich aktiv im Umlauf (in the Wild).
- Macro und Script basierte Malware ist am häufigsten.
- Viren für 32 Bit Plattformen und OS sind vorhanden.
- Malware, die in der Lage ist bestehende Netzwerkstrukturen zu nutzen, ist am gefährlichsten.
- Fast alle Firmennetze haben Anschluß an das Internet. Zumindest eMail ist fast in allen Fällen am Arbeitsplatz vorhanden.

Und die Zukunft ?

- Die Vernetzung nimmt nicht ab – neue Technologien, wie z.B. Bluetooth und UTMS, werden dazu beitragen, dass sich Viren und andere Malware noch schneller verbreiten können.



Ausbreitungsgeschwindigkeit

- Durch verbesserte Netzwerkstrukturen haben auch Viren und Malware bessere Transportwege zur Verfügung.
- Viren werden immer komplexer, intelligenter und nutzen bestehende Netze zu ihrem Vorteil.
- Eine zunehmende Standardisierung kann auch Viren helfen sich besser und immer schneller zu verbreiten.

Medium	Floppy Disk	LAN	Internet	Wireless
Transport Speed	1	10x	100x	1000x

Palm Breach: Ruhestörung unter Palms

- Personal Digital Assistants sind genau wie herkömmliche Computerplattformen nicht vor Viren gefreit.
- Im Jahre 2003 werden ca. 18,9 Mio. Einheiten im Umlauf sein
- Palm OS verwendet kein herkömmliches Dateisystem, sondern ist für das Zusammenspiel mit Primärgeräten wie einem PC optimiert worden.
- Das Palm OS ist datenbankbasiert. Die Einträge werden direkt im Speicher abgelegt, und nicht im Gegensatz zum PC, nur dort zwischengespeichert.

Palm Breach: Infektionswege

- Jede Methode, mit der ausführbarer Code auf das Palm Gerät gebracht wird, stellt zugleich eine Eintrittsmöglichkeit für schädlichen Code dar.
- HotSync ist die grundlegende Methode, Anwendungen auf den Palm zu transferieren
- IrDa (Infrared Data Associations)

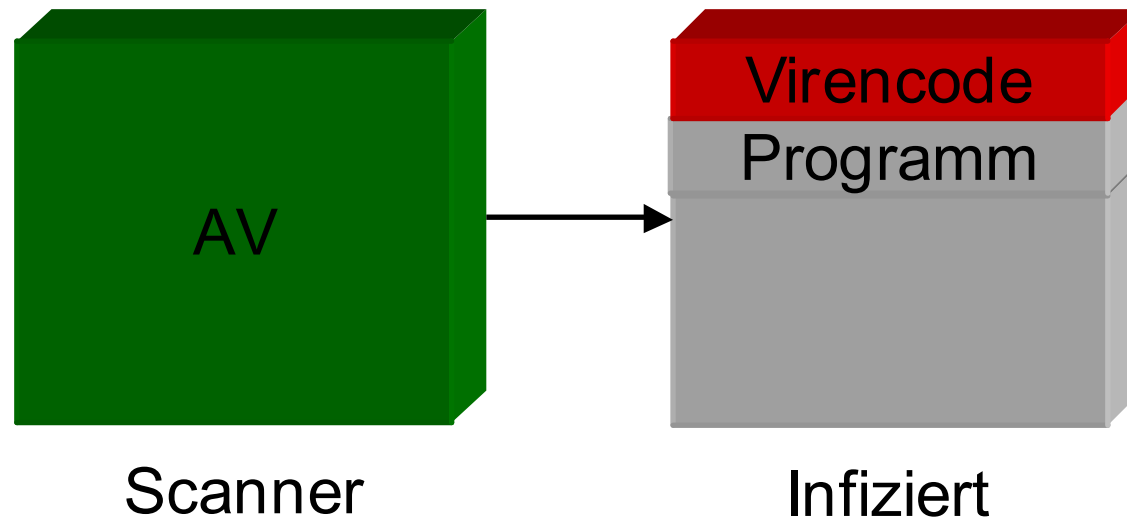
Übertragung von Daten möglich, ohne dass der Benutzer etwas davon merkt.

- Netzwerkzugang

Neuere PDA's bieten Zugang über ein in- oder externes Modem. Damit ist ein eingeschränkter Zugang zum Internet möglich.

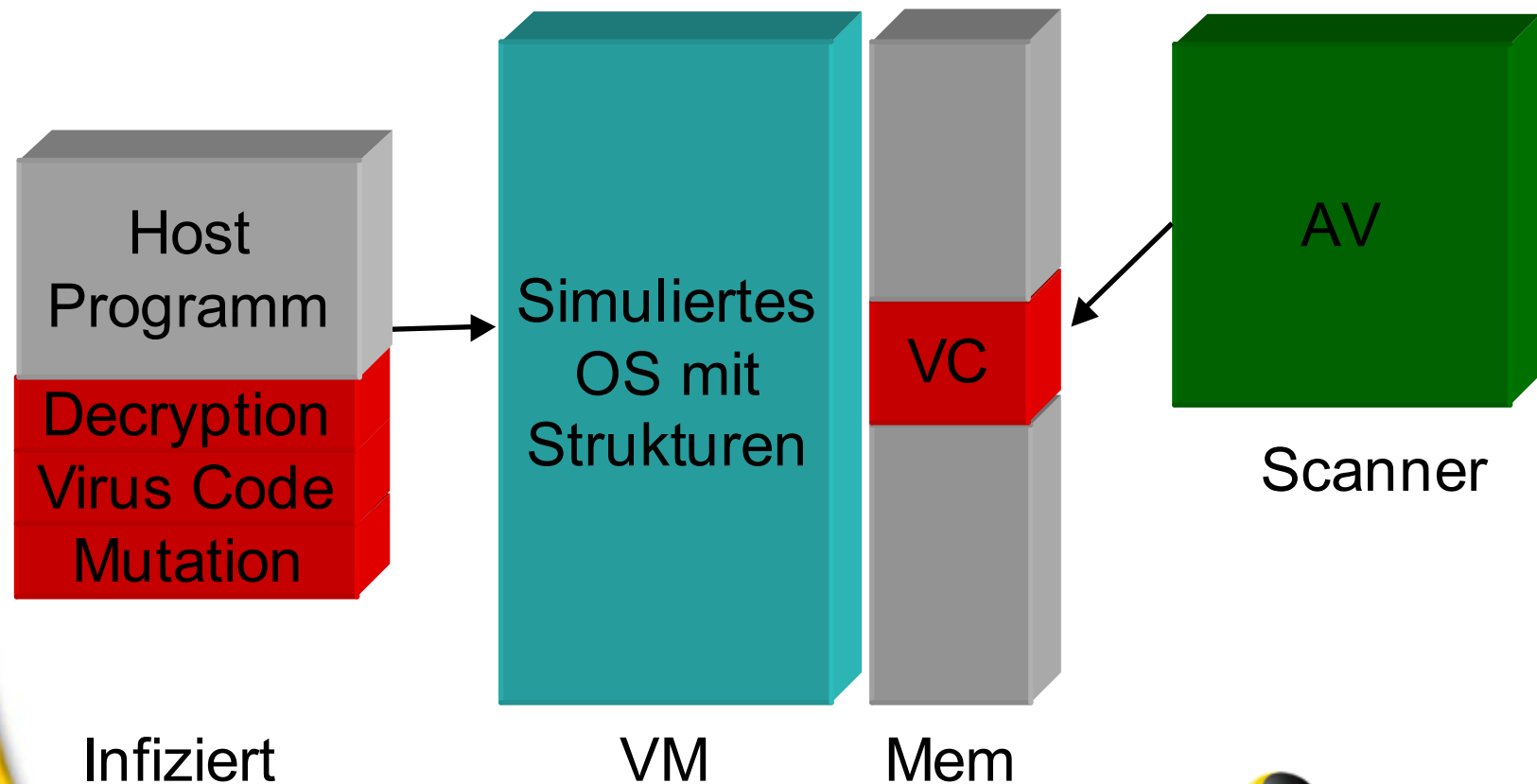
Erkennung

Ohne Verschlüsselung ist die Erkennung einfach mit Hilfe eines Pattern-Matching beim Scannen einer Datei möglich (ID, Fingerprint).



Erkennung II

Durch Verschlüsselung wird der Scan aufwendiger und belastet durch eine virtuelle Maschine den Prozessor.



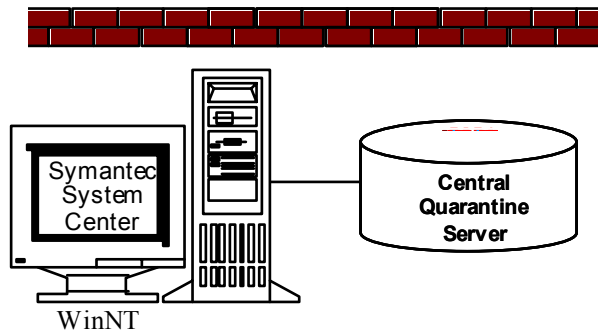
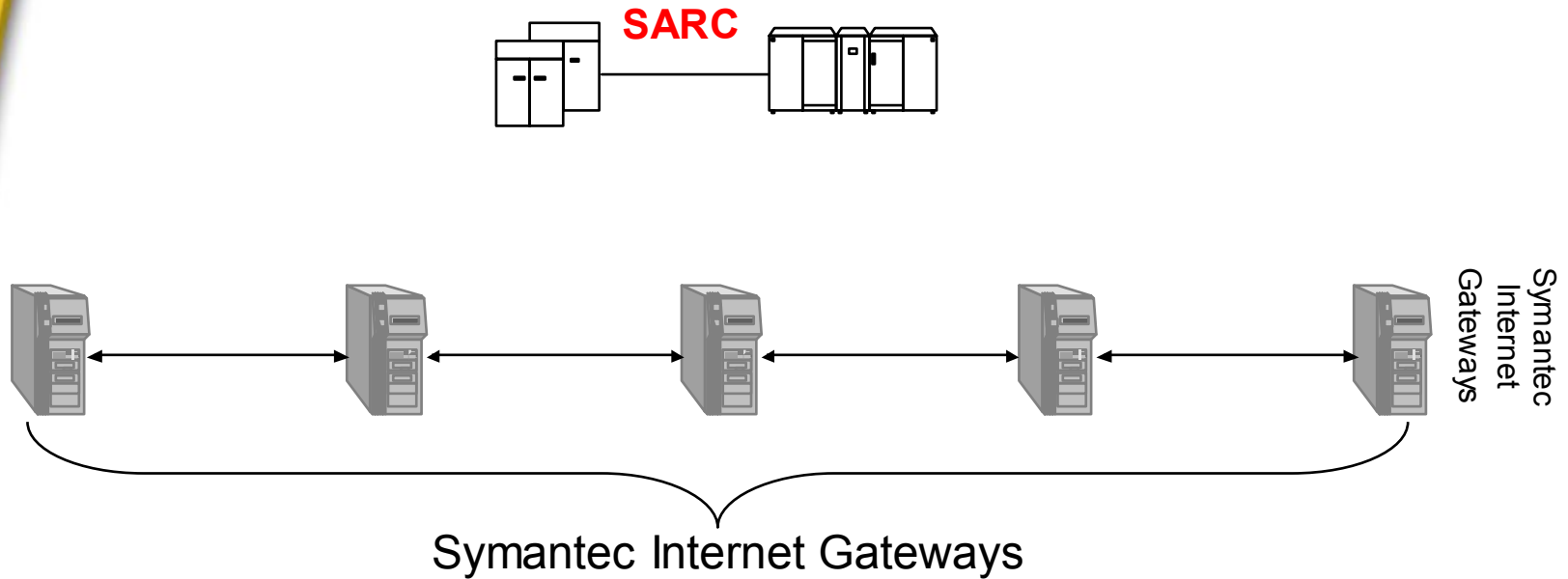
Ein nicht erkennbarer Virus?

Der nicht erkennbare Virus ist ein solcher, der nicht in einer akzeptablen Zeitspanne gescannt werden kann bei erträglicher CPU Belastung ohne dabei unverhältnismäßig viele “False Positives” zu generieren.

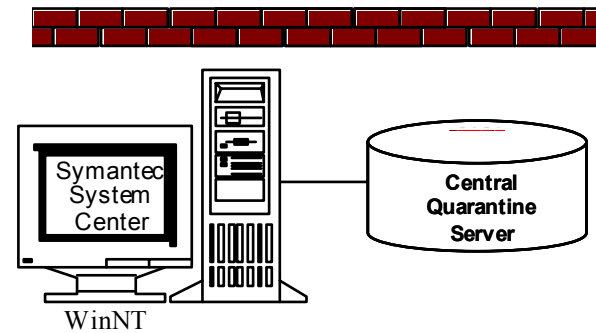
Merkmale:

- Metamorphisch
- Zufälliger Einstiegspunkt aus Host-Programm
- Zufällige Anordnung des Viren Codes im Host-Programm

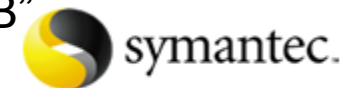
Mechanismen im Backend



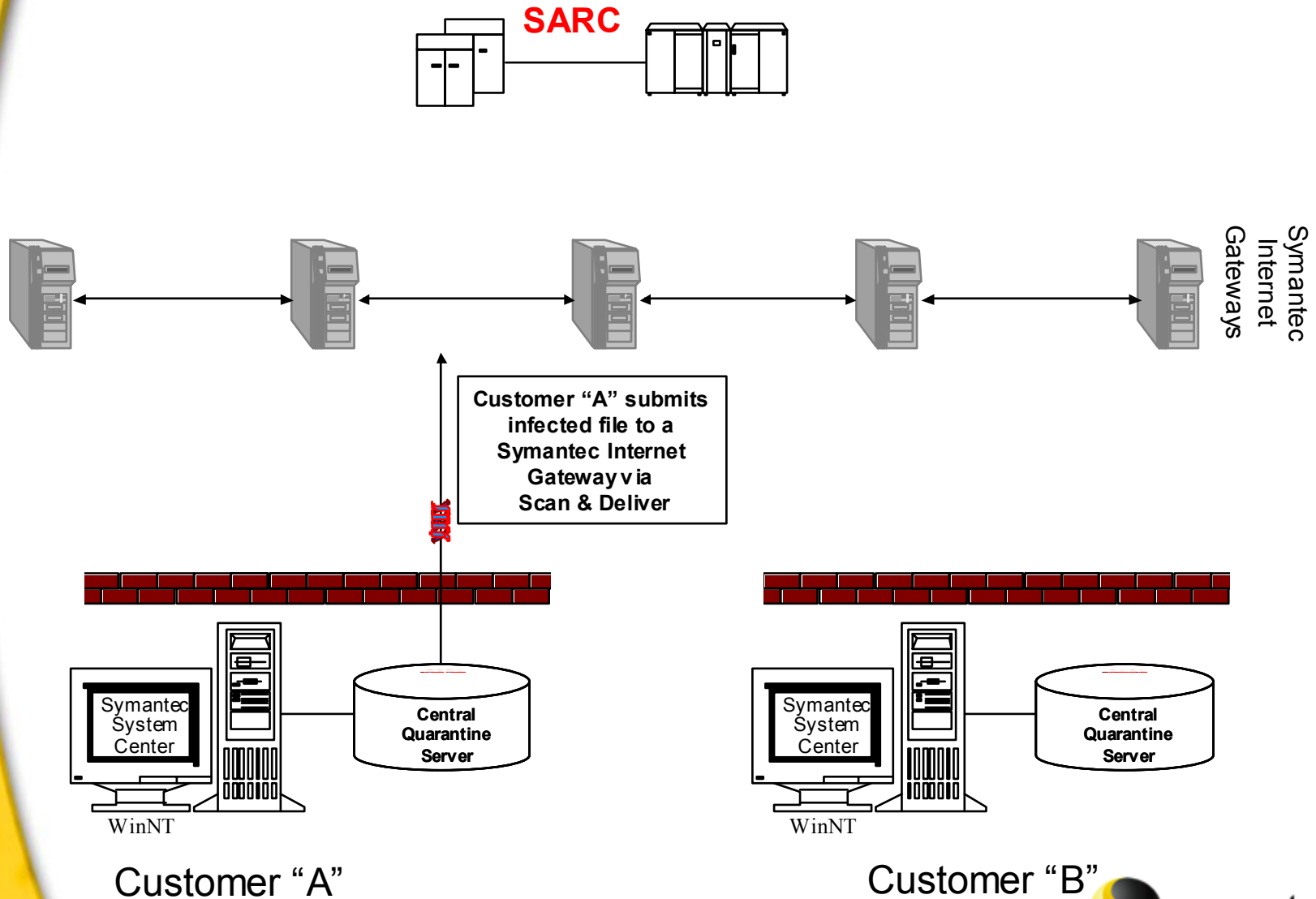
Customer "A"



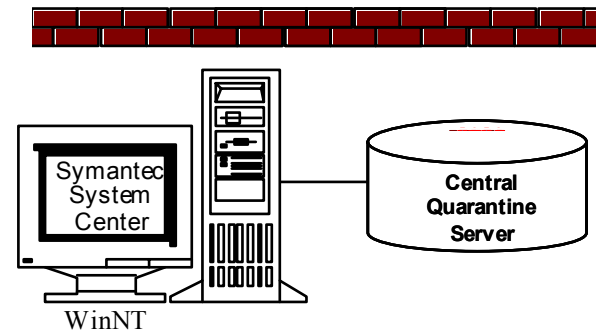
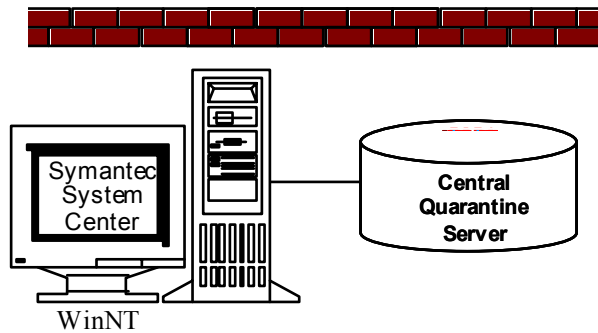
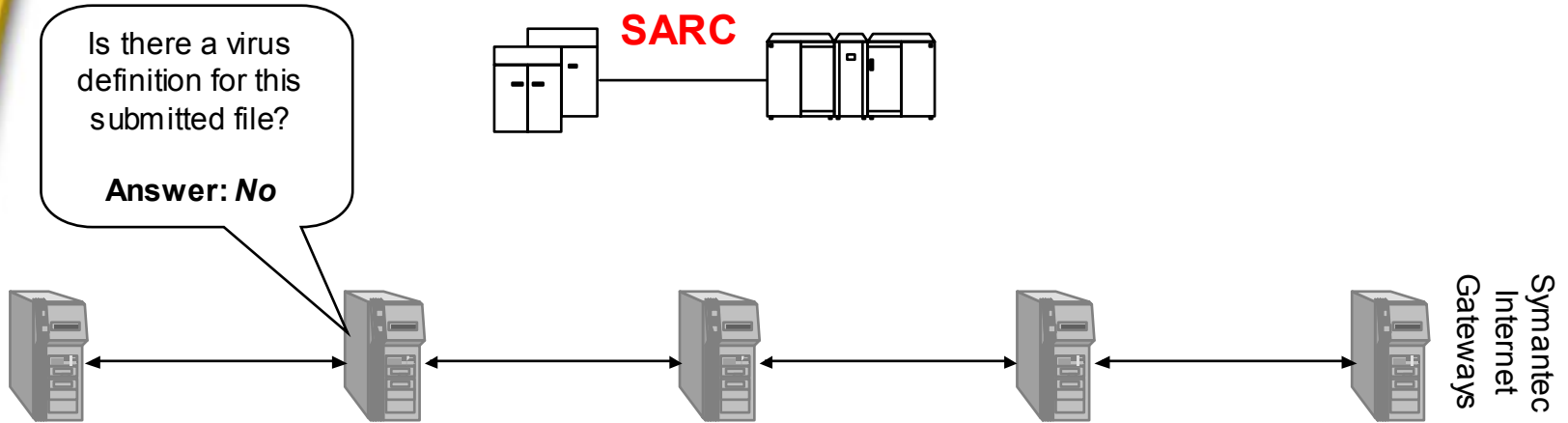
Customer "B"



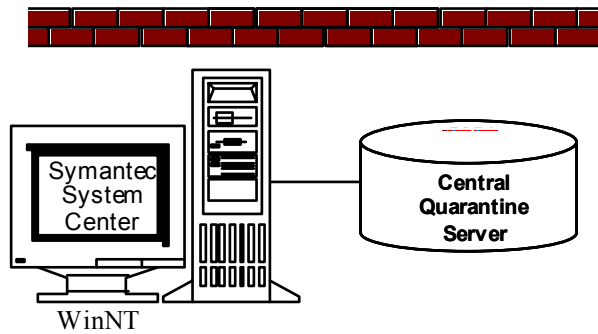
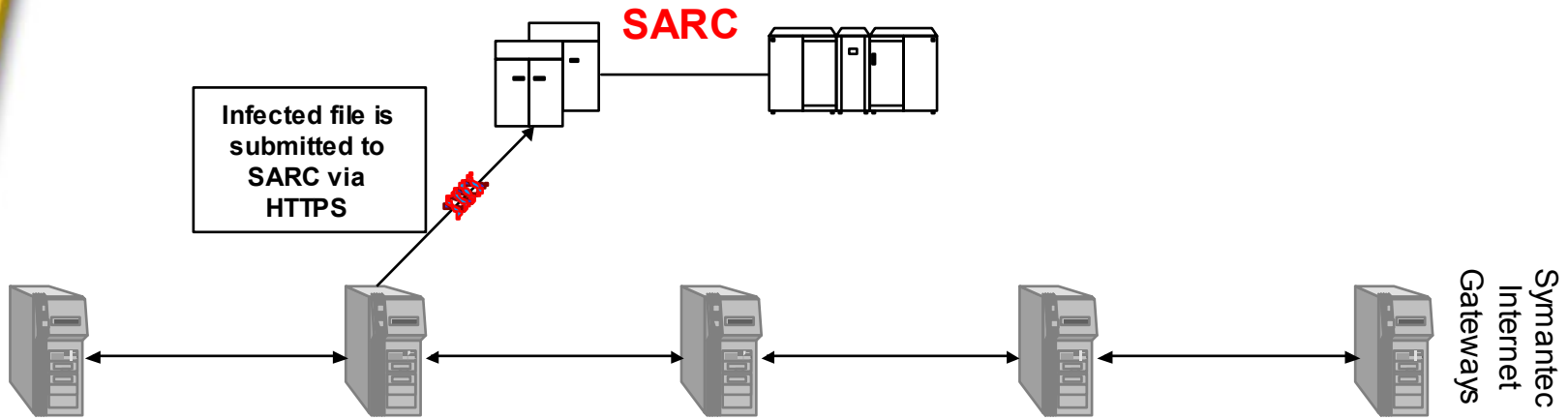
Mechanismen im Backend



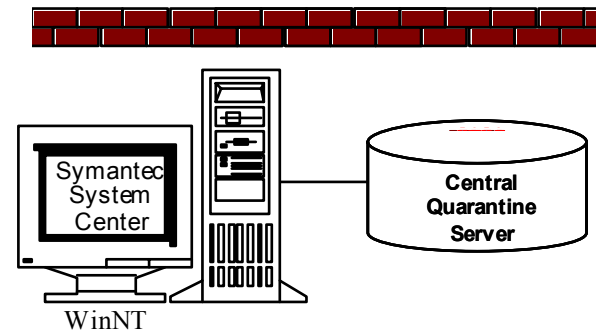
Mechanismen im Backend



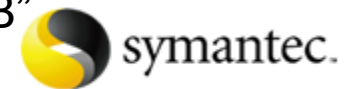
Mechanismen im Backend



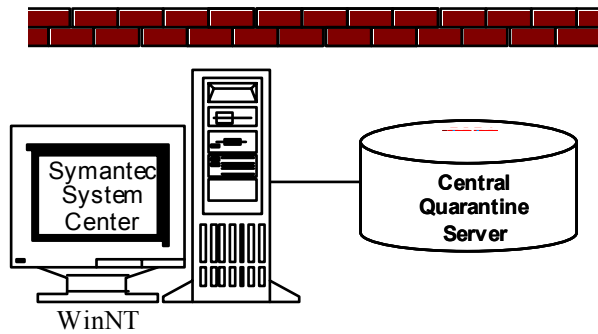
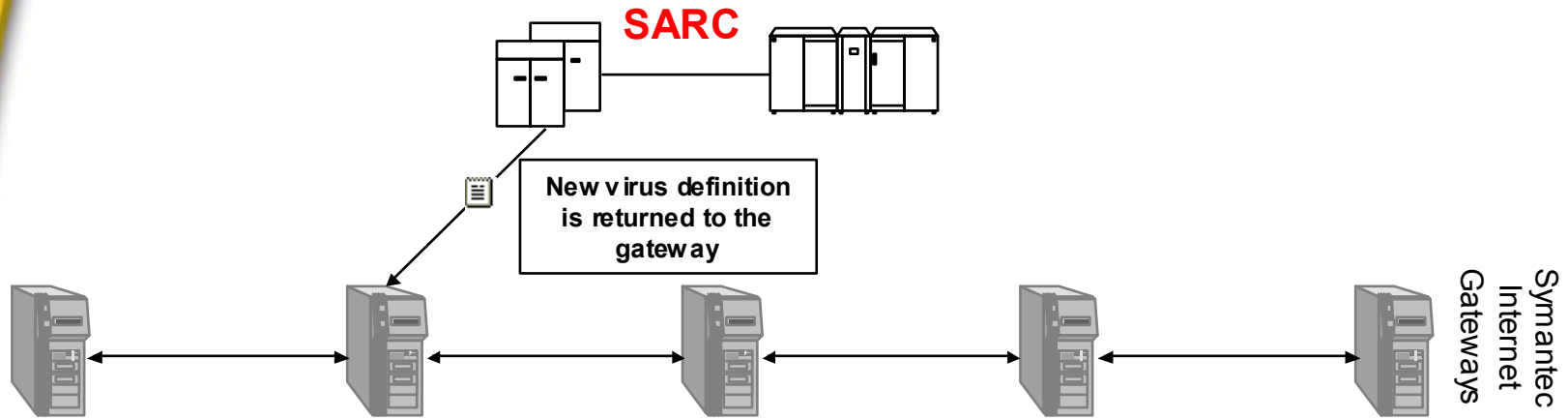
Customer "A"



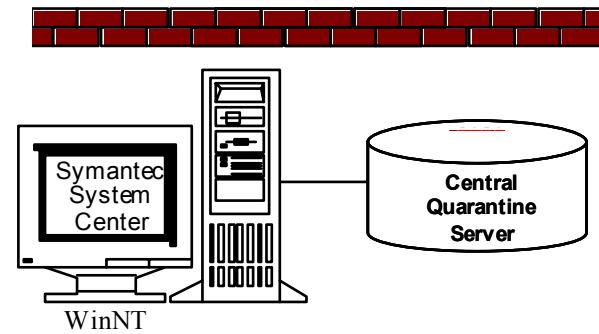
Customer "B"



Mechanismen im Backend

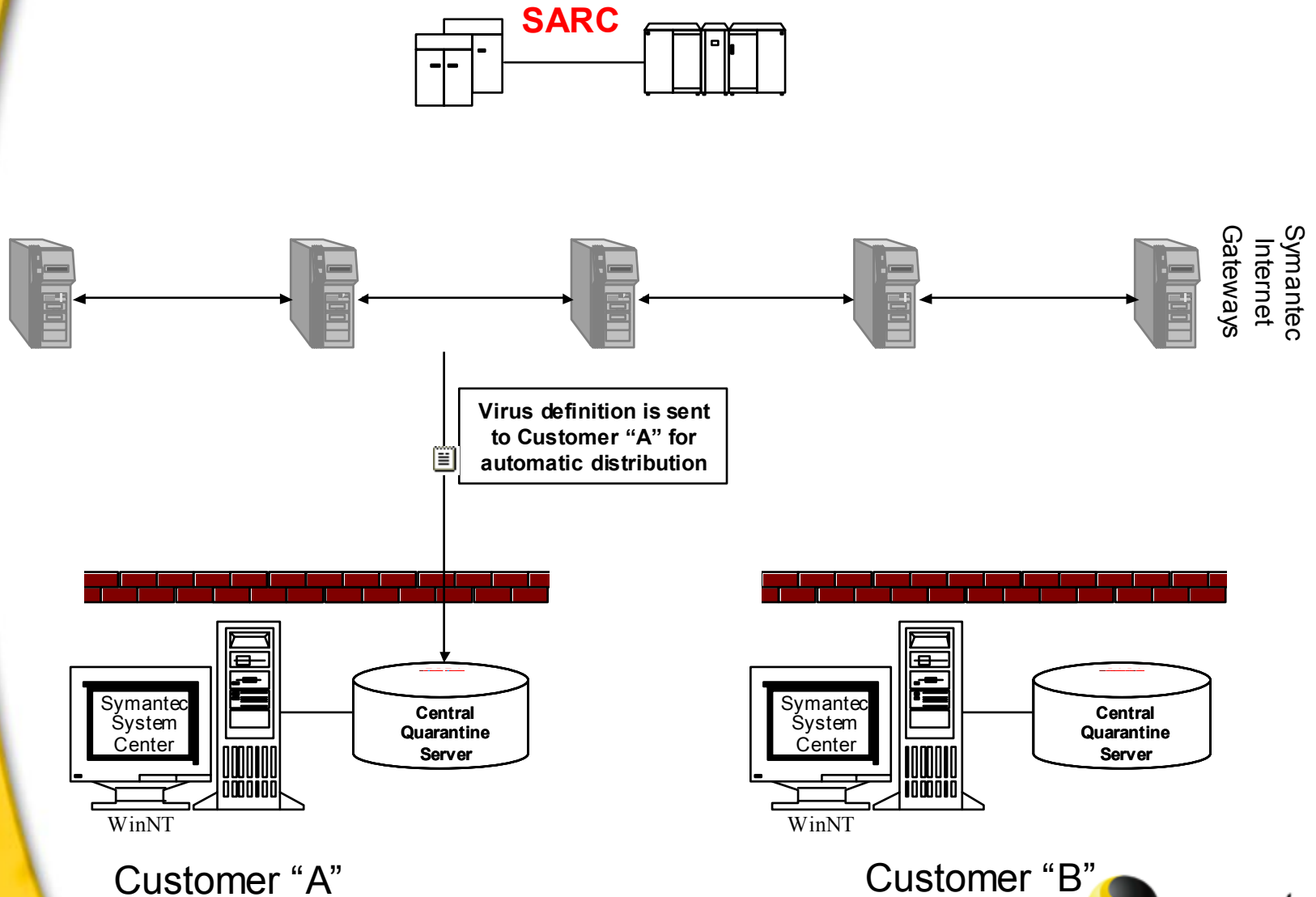


Customer "A"

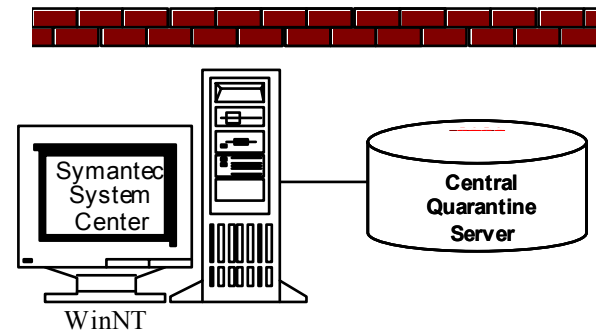
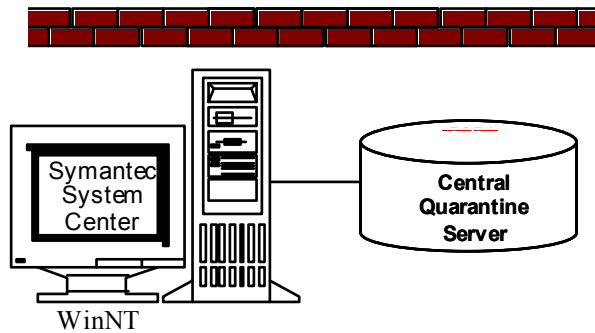
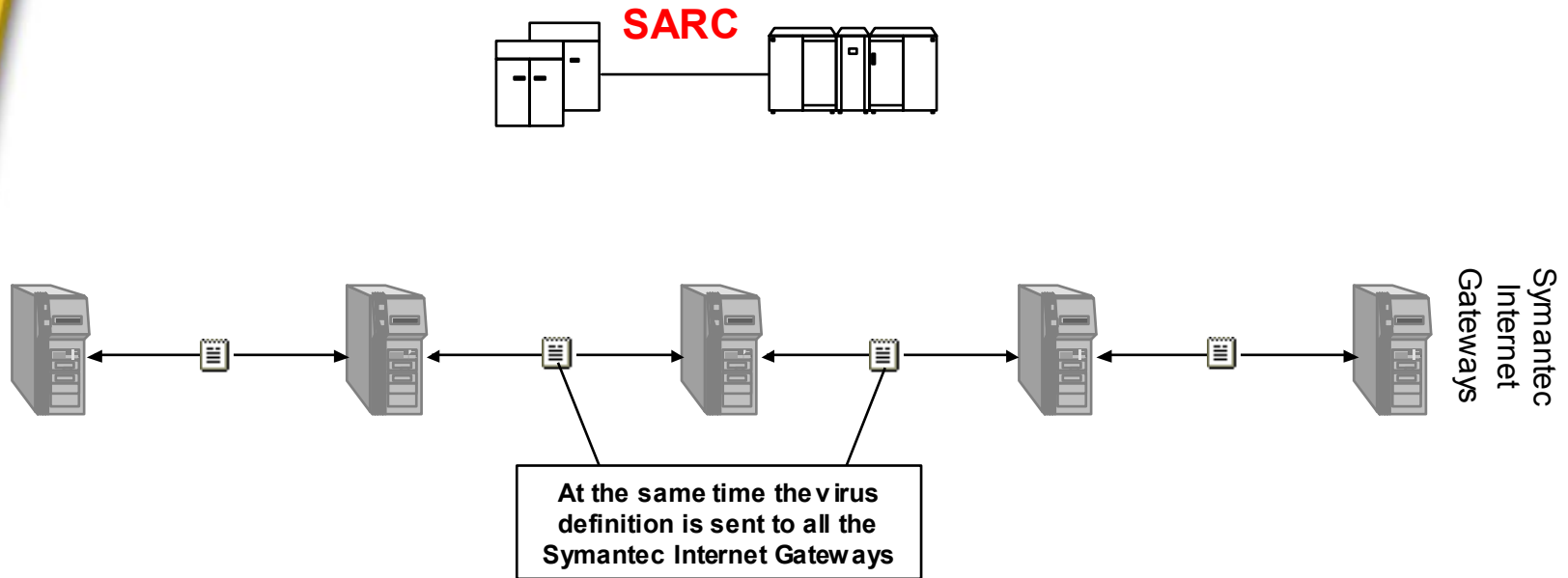


Customer "B"  symantec.

Mechanismen im Backend

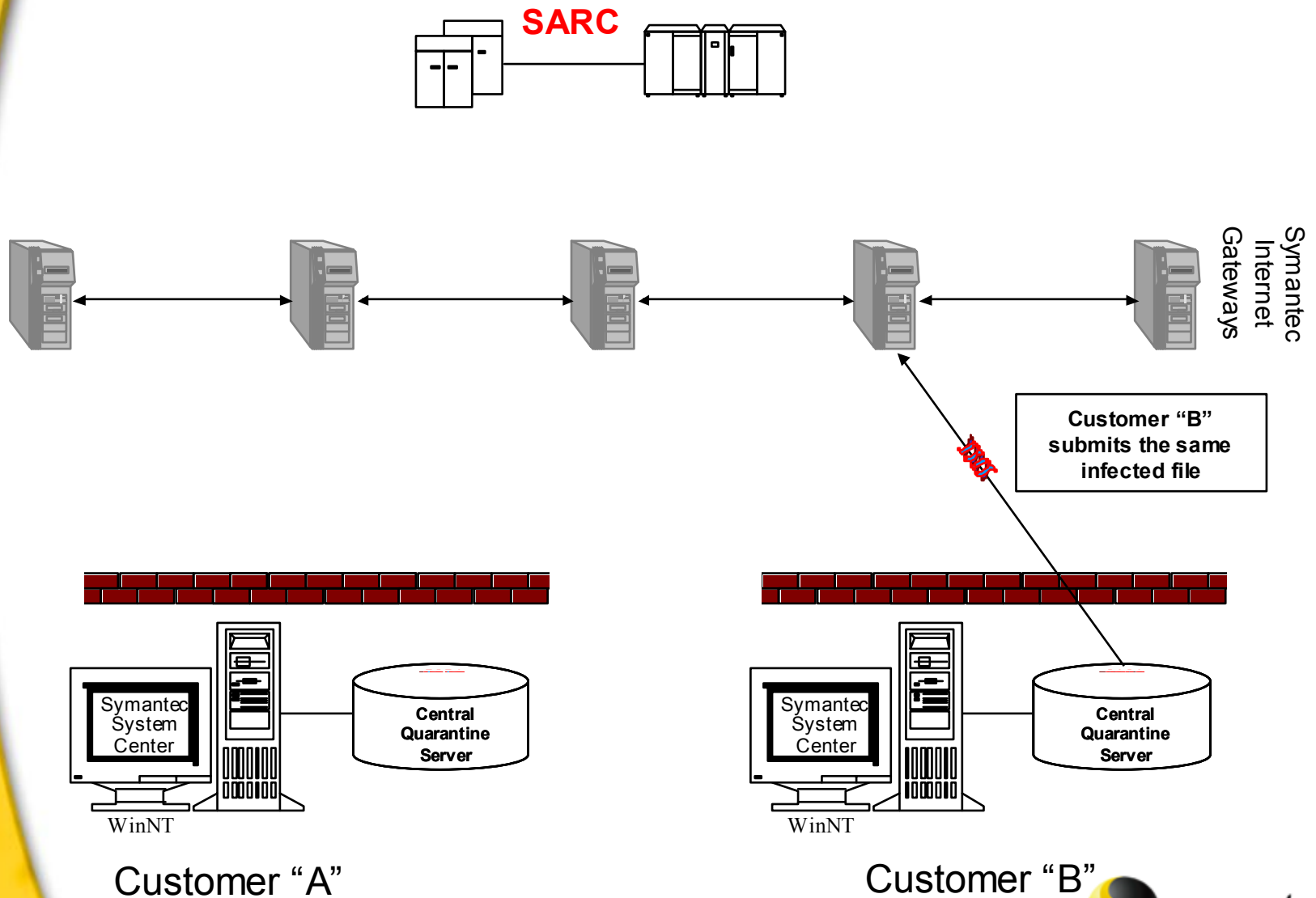


Mechanismen im Backend

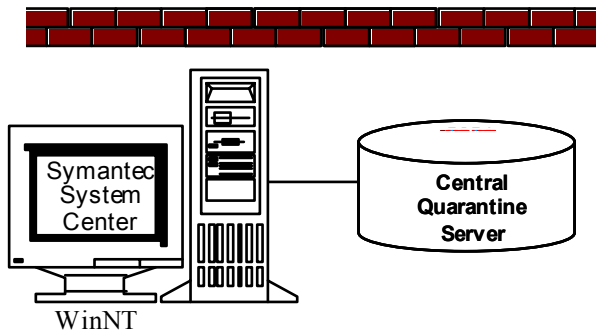
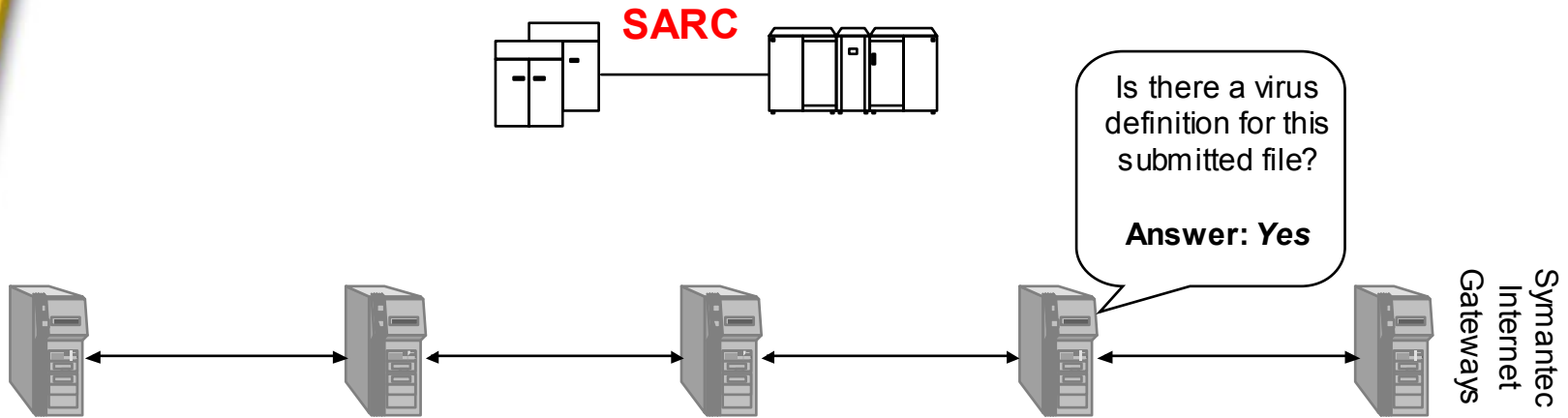


Customer "B"  symantec.

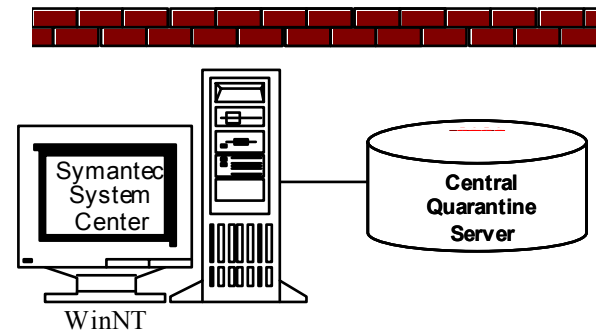
Mechanismen im Backend



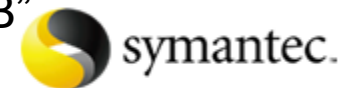
Mechanismen im Backend



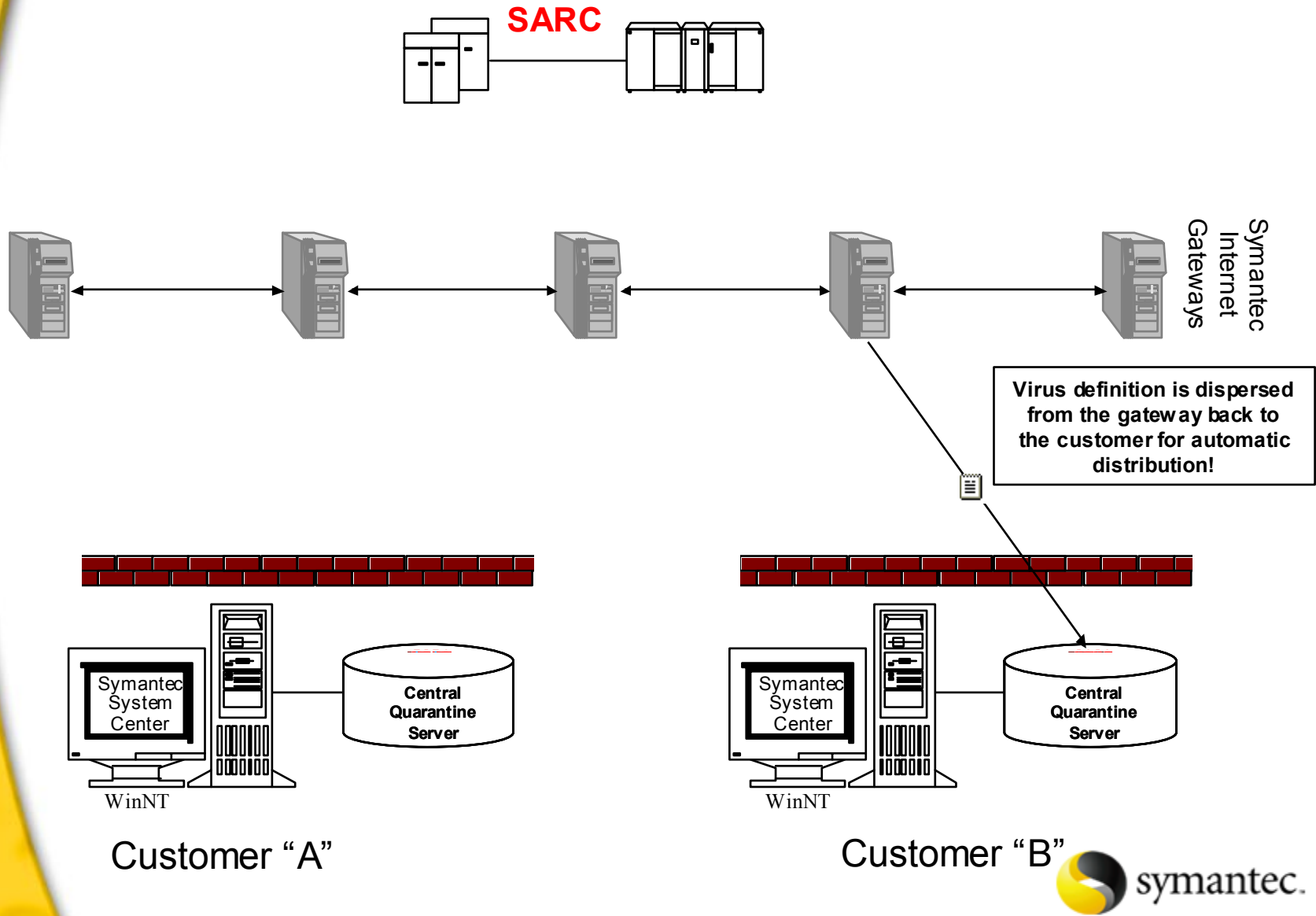
Customer "A"



Customer "B"



Mechanismen im Backend



Antivirus ist nicht genug

- Zunächst ist es unerlässlich eine Sicherheitsrichtlinie zu definieren.
- Zum Schutz gegen Hacker, Cracker, Scriptkids ist eine Firewall notwendig (Unternehmen, wie privater Anwender). Gleichzeitig wird hier ein Schutz gegen diverse Trojanische Pferde aufgebaut.
- Netzwerke sind „lebende“ Gebilde. Eine einmalige Aufnahme des Zustandes reicht nicht. Bestehende Sicherheitsrichtlinien sind regelmäßig zu überarbeiten.

Und noch einmal:

- Eine Virens Scanner kann nur wirksam sein, wenn die Definitionen und die Scanengine aktuell sind.

