Antivirus @ DESY

Allgemeine Informationen

Installation

Konfiguration

Update und Upgrade

Aufbau eines Viruses

- Installationsteil:
  - Installiert den Virus nach seinem Aufruf im Hauptspeicher
  - Ev. Test, ob bereits vorhanden
  - Kann Funktionen zur Selbsttarnung enthalten
- Reproduktionsteil:
  - Anweisungen zum Kopieren (Vermehrung)
- Payload (Schadensteil):
  - Muss nicht zwingend vorhanden sein
  - Viele Viren beschränken sich auf das Vervielfältigen und Ausbreiten (Verlangsamung des System, Belegung von Speicherplatz usw.)
  - Schadfunktionen: z.B. Formatieren der Festplatte

Typen von Computerviren - 1

- Systemviren (Bootviren)
  - Steht im Bootsektor von Disketten + Festplatten
  - z.B.: Parity Familie, Delwin
- Dateiviren
  - Verbreiten sich über die Infektion ausführbarer Dateien
  - Code kann am Anfang, Ende oder in unbenutzten Bereichen stehen
  - z.B. Pate
- Makroviren
  - Infizieren Dokumentdateien (Excel, Word)
  - Sind im ausführbaren Code (Makros) enthalten
  - Werden beim Öffnen eines infizierten Dokumentes aktiv
  - z.B. Klez, Marker, Magister, Elkern

Typen von Computerviren - 2

- Trojanische Pferde
  - Programme, die neben der gewünschten Funktion auch noch verborgene und unerwünschte Funktionen enthalten
  - Zusätzliche Funktionalität:
    - zerstörerisch
    - Ausspähen von Informationen
  - Sind nicht selbst reproduzierend, verteilen sich über Würmer
  - z.B.: Backdoor
- Hostile Agents (“feindselige Agenten”)
  - Bedrohung über das Internet
  - Ausführen von unerwünschten Applets auf lokalen PCs
  - Applets können z.B.
    - Daten ausspionieren
    - Daten löschen oder verändern
    - Viren installieren
  - z.B. JS-Seeker, Hantaner

Typen von Computerviren - 3

- Würmer
  - Breiten sich aus, indem sie sich selbst über Netze kopieren
  - Befallen das Netz als Gesamtheit
  - Sind nicht an ein Wirtsprogramm gebunden
  - Bewegen sich selbständig von Rechner zu Rechner, indem sie in den Speicher des Rechners eindringen, dort weitere Netzwerkadressen ermitteln und Kopien von sich selbst dahin schicken
  - Besonders gefährlich durch ihre hohe Ausbreitungsgeschwindigkeit
  - z.B. Lovesan, Bagle, Netsky, Mydoom, Funlove
- Hoaxes
  - Falsche Warnmeldungen über nicht wirklich existierende Viren
  - Verbreitung im Internet
  - Ziel: Panik unter Nutzern verursachen

Der Warhol Wurm - Theoretischer Superwurm I

- Ist der Ansatz für einen Superwurm
- Andy Warhol: “In the future, everybody will have 15 minutes of fame.”
- Nicholas C. Weaver (University of California) beschreibt, wie sich solch ein Wurm innerhalb von 15 Minuten im gesamten Internet ausbreiten könnte.
- Wurm muss sehr effizient neue Ziele finden, d.h. neue Ausbreitungsmechanismen sind notwendig.
- Suche nach neuen Zielen nennt man “Scannen”
- Wurm generiert ein IP-Adresse und verschickt eine Kopie von sich dorthin, vorherige Analyse des Zielsystem möglich (Dienst oder Schwachstelle)

Der Warhol Wurm - Theoretischer Superwurm II

- **3 Methoden des Scannens**:

1. Scannen nach Hitliste
   - Erstellen einer Hitliste von verwundbaren Systemen (10000 bis 50000 Einträge)
   - Je grösser die Hitliste, desto schneller die Infektion

2. Zufälliges Scannen (random scanning)
   - Zufällige Auswahl von IP Adressen (keine Überprüfung, ob Systeme infizierbar)
   - Guter Ausbreitungsmechanismus
   - Nachteile:
     - Systeme können mehrfach ausgewählt werden.
     - Keine Prüfung, ob Systeme bereits infiziert → Mehrfachinfektionen
     - Keine Garantie, dass der Wurm sich beendet, wenn alle verwundbaren Systeme infiziert sind (unkoordiniert + unkontrollierbar für den Wurmautor)

Der Warhol Wurm - Theoretischer Superwurm III

3. Permutiertes (Verteiltes) Scannen
   - Erkennbar, ob System schon infiziert
   - IP-Adressraum wird in Permutationen aufgeteilt
   - Jedem Wurm wird ein IP-Adressraum zugewiesen (Zufallsalgorithmus)
   - Jede Wurmkopie wählt einen zufälligen Startpunkt in der Permutation
   - Wird ein verwundbares System gefunden und infiziert, beginnt die dortige Wurmkopie ebenfalls mit dem permutierten Scannen.
   - Steht hinter einer IP kein verwundbares System oder hat der Wurm ein System infiziert, setzt er den Scan mit der nächsten Adresse fort.
   - Findet er ein infiziertes System, initialisiert er sich mit einem neuen Startpunkt
   - Vorteil:
     - IP Adressen werden nicht mehrfach gescannt → keine Mehrfachinfektionen
     - Nach einer bestimmten Anzahl von infizierten Systemen , Stopp des Scannens, weil dann alle Systeme der Permutation infiziert sind.

- Ungewiss, ob der Warhol Wurm, das in 15 Min. schaffen könnte → größere Anzahl schneller Netzwerkverbindungen notwendig, als derzeit verfügbar.

Phasen eines Superwurms

- Vorbereitungsphase
  - Sammeln von Informationen, wie z.B. Schwächen von Systemen oder das Erstellen der Hitliste
- Aktionsphase
  - Implementierung, Start und Ausbreitung
  - ev. Verwendung der Daten aus der Vorbereitungsphase
- Nachbereitungsphase
  - Autor kann mit dem Wurm durch Senden von Nachrichten in Verbindung bleiben
  - Ziel: Gezieltes Ausspionieren von Systemen oder Verbesserung des Wurmcodes

Viren mit Superwurm- Eigenschaften

- Code Red I
- Code Red II
- Nimda
- Lioten
- SQL Slammer/ Sapphire
  - Benutzt die Methode des zufälligen Scannens
  - Gehört zu den derzeit schnellsten Computerwürmern

Warum McAfee?

- 1993: Antivirenkit von GDATA (Zeuthen)
- Sophos (Hamburg) und andere Virenscanner
- 1997: VirusScan von Network Associates (Zeuthen)
- 2000: Total Virus Defense (HH und Zeuthen)
- Entscheidung für VirusScan (McAfee), weil
  - Gut managebar
  - Hohe Erkennungsrate
  - Einfach zu konfigurieren
  - Gute Lizenzbedingungen

Network Associates Active Virus Defense

Lizenzen: 2000 Knoten (für HH und ZN)

Beinhaltet: File Server Protection (Netshield)
Desktop protection (Alle Windows Systeme)
e-mail Schutz (Groupshield)
Internet Gateway Schutz (Webshield)
auch für Solaris und Linux
McAfee Prime support – 24 Stunden, 7 Tage/ Woche
Management tools

Total Virus Defense

3 Tools

1. **Auto Update Architect**
   - Schaut mehrmals täglich nach Updates auf dem McAfee Server
   - Unterstützt verteilte Repositories

2. **Installation Designer – VSE7.1**
   - Vorkonfiguration des Installationspaketes
   - neues .MSI file wird erzeugt

3. **ePolicy Orchestrator**
   - Management Tool
   - Überblick, Updates, Installation

Installierte Versionen

DESYNT

- VirusScan 4.03 (NT4)
- VirusScan 4.51 (WXP, W2K)
- VirusScan Enterprise V 7.1 (WXP, W2003)

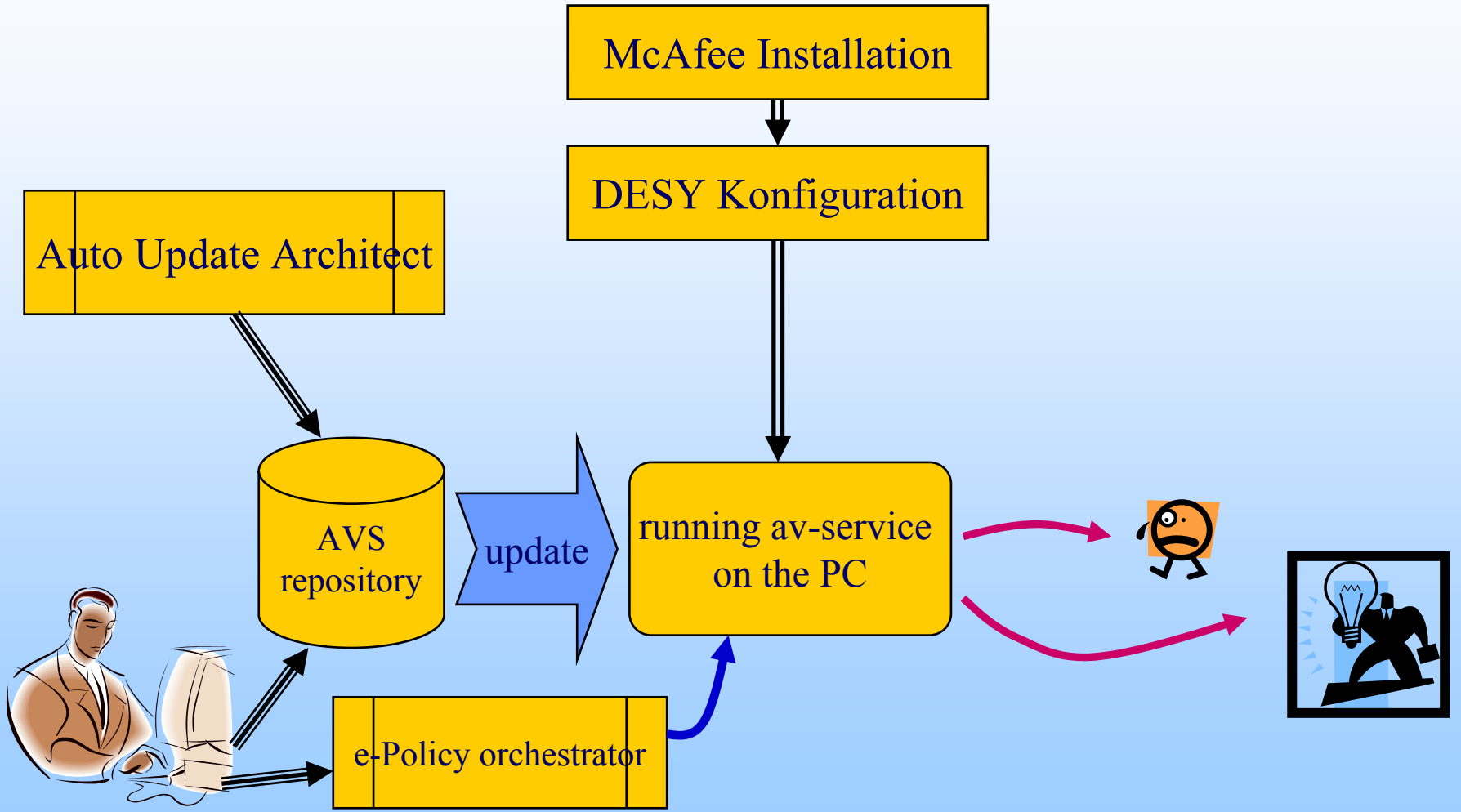
WIN

- VirusScan Enterprise V 7.1 (WXP, W2003)

Gründe für das Update

- Support für die Version 4.03 wird eingestellt
- Neue Scan Engine bringt Rechner zum Absturz
- Supportaufwand für 3 verschiedene Versionen zu hoch
- Version 4.51 schlecht managebar (Alert)
- Ziel: eine Version für alle unterstützten Windows Plattformen
- Version 7 läuft auf allen Windowssystemen (WS + Server)
- Installation Designer für Konfiguration
- Bessere Remote Konfiguration möglich

Overview Client Management



Installation - I

- DESYNT:
  - NetInstall Paket unter Tools (startet die native Installation)
  - Samba Server: \\desyntavsh\avs\systems\VirusScan71-EN
    bzw. \\desyntavsz\avs\systems\VirusScan71-EN
  - S:\products\avs\systems\VirusScan71-EN
- Win.desy.de:
  - RIS
  - WXP Installations-CD
  - Samba Server
  - \\adavsh\avs
- Workgroup
  - Samba Server

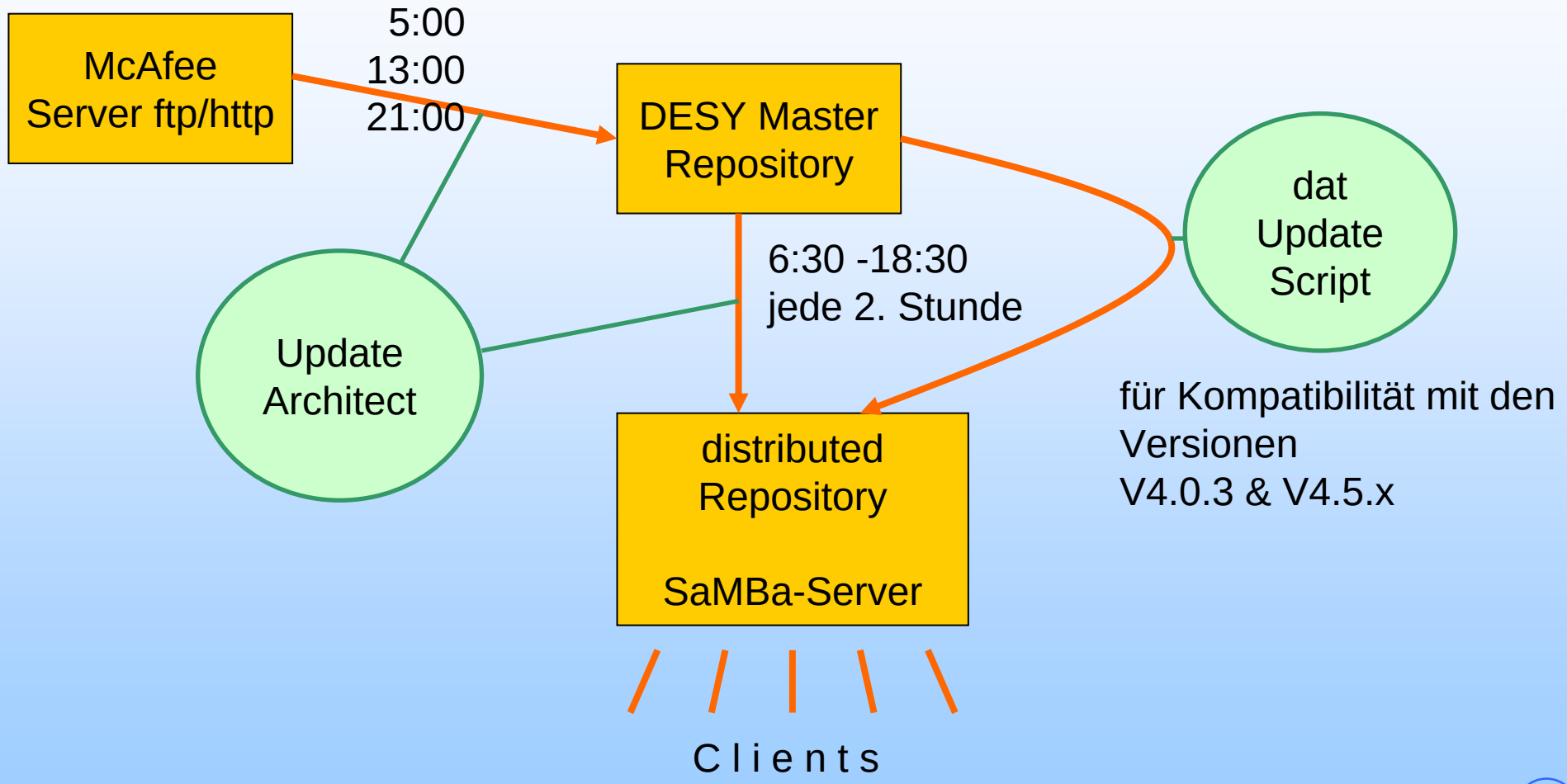
Installation - II

- Vorkonfiguriert mit Installation Designer
- stille Installation (wenn Reboot notwendig → Message)
- Installation ins Systemlaufwerk
- Alte Versionen von McAfee und andere Virenscanner werden automatisch deinstalliert während der Installation
- On Access Scanner wird nach der Installation gestartet
- 1. Update der Virensignaturen erfolgt unmittelbar nach der Installation (ausser RIS und CD)
- \\desyntavsh\avs Samba Server: Hamburg
- \\desyntavsz\avs Samba Server: Zeuthen
  - Vorteil: Leserechte für alle (DESYNT, WIN, keine Domain)

Konfiguration VSE 7.1

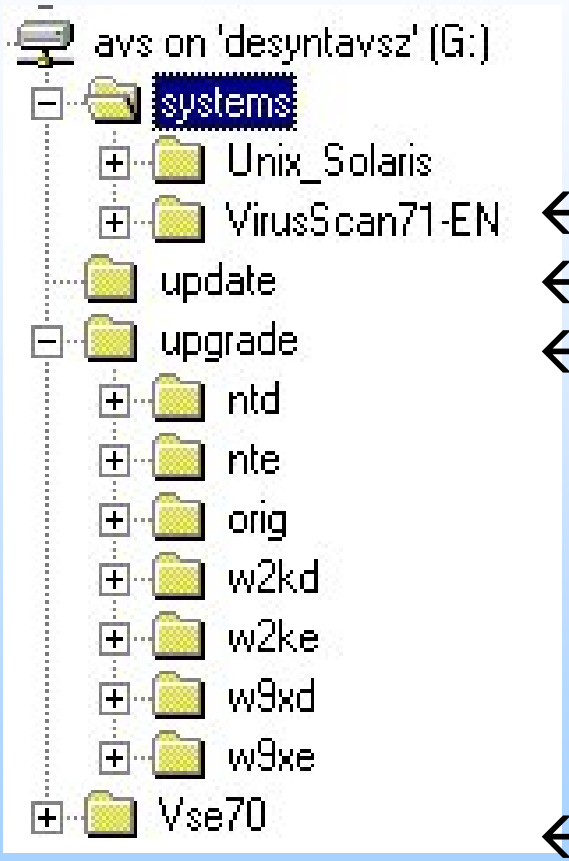
- **In Absprache mit den Sicherheitsbeauftragten**
- **allgemeine Einstellungen:**
  - Scannen bei Zugriff
  - Säubern des infizierten Files, anderenfalls löschen
  - Scannen von Netzlaufwerken + gepackten Files
  - Filescan: Defaultfiles + Macroviren
  - Suche nach unerwünschten Programmen (Adware, Dialer, Hackertools)
  - Ausschluss der NetInstall Server (nur Lesen)
- **Update Schedule**: täglich von DESYNTAVSH bzw. DESYNTAVSZ bzw. McAfee Server
- **Alerting:**
  - Popup Fenster auf dem PC
  - E-mail an avadmin@desy.de

Update Schedule



AVS repository

Auf den Samba Servern
erlaubt guest access
Lesezugriff für alle



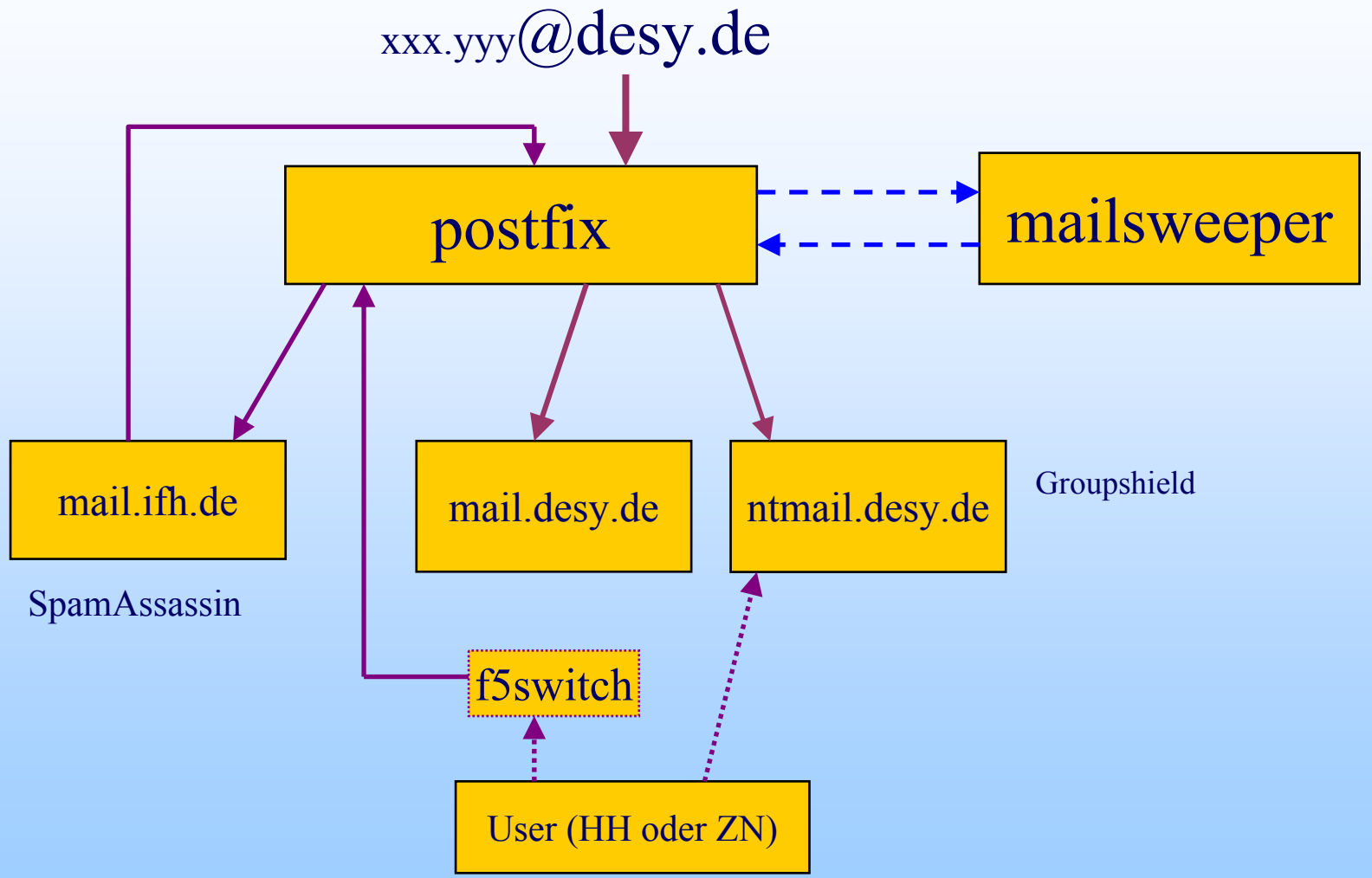
← Vorkonfiguriertes Installationspaket

← Enthält die aktuellen dat-xxxx.zip & update.ini

← Sprachabhängige SuperDAT's

← Enterprise repository (dat-xxxx.zip, sitelist.xml)

Mail + Virenscanner



Policies – Was ist wichtig?

- Flächendeckende Versorgung (Workstation + Server)
- Regelmäßige Updates der Virensignaturen (täglich + bei akuten Vorfällen sofort)
- Regeln für die Bearbeitung von Vorfällen
- Wer ist wofür zuständig? (Update, Virenvorfälle, Installationen)
- Kontrolle der PCs auf Aktualität + Installation
- Tool für Gruppenadministratoren unter s:\service\tools\avscan\ (Beschreibung + PerlScript)
  - Ausgabe von 4 Textfiles:
    - kein Virenscanner
    - nicht erreichbar
    - OK
    - Virenscanner mit Problemen

Hinweise zum Vermeiden von Infektionen

- Virenscanner nicht deaktivieren!
- Virensignaturen immer aktuell halten!
- Systemupdates installieren
- Suspekte E-Mails nicht öffnen, sondern gleich löschen!
- Dateianhänge an E-Mails nicht öffnen, wenn schon das Subjekt fraglich und unerwartet ist
- Vorsicht beim Download von Files aus dem Internet
- Nutzer sollte sich über den Schedule seines PCs informieren
- Ggf. Updates von Hand durchführen

Besonderheiten bei der Benutzung von Notebooks

- Virenscanner so konfigurieren, dass man auch unterwegs neue Signaturfiles installieren kann (z.B. NAI)
- Selbst auf die Installation neuer Signaturen achten, da automatischer Update nicht immer möglich
- Firewall Software aktivieren
- Vor dem Anschluss ans Netz: Stinger Diskette benutzen!
  - http://www-it.desy.de/systems/services/security/stinger.html.de
  - Stinger ist kostenfrei von Network Associates (McAfee)
  - Scannt und beseitigt eine Vielzahl von Würmern und Viren

FAQ's

- Wie wird gescannt?
  - Vergleich von Mustern (Patterns), die in den Signaturfiles enthalten sind, bevor ein File geöffnet wird
  - Beim Dateiexplorer schon beim Markieren
- Warum nicht 2 Virenscanner gleichzeitig?
  - Zugriff erfolgt auf niederer Schicht im BS
  - Die beiden Scanner würden sich gegenseitig behindern
- Warum ist das Scannen auf den Mailservern und Windowsservern nicht ausreichend?
  - Disketten, CDs
  - Notebooks
  - Problem: Serverperformance

Dokumentationen

- http://www-it.desy.de/support/services/software/virus_scanner/index.html.de
- http://www.desy.de/d4/intern/Virenwarnungen.html/
- http://www-it.desy.de/systems/services/security/stinger.html/
- http://agn-www.informatik.uni-hamburg.de/vtc/
- http://de.mcafee.com/
- http://www.symantec.com/region/de/
- http://www.bsi.bund.de/

Was ist zu tun ?

- Testen des ePolicy Orchestrator – Management Tool
- Zentrale Erfassung der Alarme