# Viren, Würmer und Trojaner

Andreas Marx
AV-Test GmbH

http://www.av-test.de

heise Security - Konferenz „E-Mail-Sicherheit“, Vortrag über „Viren, Würmer und Trojaner“

Telefon: +49 391 6075460, Fax: +49 391 6075469, http://www.av-test.de

# Inhalt

- Begriffe (II)
- Klassifikationsmöglichkeiten (I)

- Herausforderungen (V)
- Aktuelle Malware-Entwicklungen (V)
- Testergebnisse (VII)
- Gegenmaßnahmen (V)

# Begriffe (I)

- Malware = Oberbegriff (*Mal*icious Soft*ware*)
  - Per Intention schädliche Software
  - Umgangssprachlich oft mit „Viren“ gleichgesetzt
- Viren = infizieren Dateien (Wirte), etwa Programme oder Office-Dokumente
  - Heutzutage kaum noch verbreitet (< 2,5 Prozent)
- Würmer = verbreiten sich über Netzwerke und infizieren die Rechner des Verbundes

# Begriffe (II)

- Trojanische Pferde = Programm mit (meist versteckter) schädlicher Nebenfunktion
- Backdoor = Hintertürenprogramm
  - Angreifer kann alles, was der Benutzer auch kann
- Bot = Kombination aus Backdoor und Wurm, Kommunikation über IRC-Netzwerke (Internet Relay Chat)
- Adware, Spyware, Dialer…

# Klassifikationsmöglichkeiten (I)

- Nach „Lebensraum“:
  - Boot-, Datei-, Skript- und Makroviren
- Unterteilung nach Verbreitung:
  - Sehr weit verbreitete Viren = „ItW“- (In-the-Wild) oder WildList-Viren → http://www.wildlist.org
  - Wenig bis kaum verbreitete Viren = Zoo-Viren (sieht man nur in den „Viren-Zoos“ der Hersteller)
- Einordnung nach Schadensklassen:
  - Geringer Schaden, z.B. Bildschirmeffekte, Töne
  - Mittlerer Schaden, z.B. Löschen von Dateien
  - Hoher Schaden, z.B. Manipulation von Daten
  - Unermesslicher Schaden, z.B. Weitergabe vertraulicher Dokumente an die Konkurrenz

# Herausforderungen (I)

- Virenscanner heute:
  - Produkt zum Aufspüren von Viren per Signatursuche („Fingerabdrücke“ bekannter Schädlinge) und per Heuristik („typische Malwareeigenschaften“, Emulation  Sandbox)
  - Dateibasiert (einzelne Dateien auf dem Datenträger)
- „Virenscanner“ (genauer: Security Suiten) morgen:
  - Firewall als integraler Bestandteil, inkl. Filterung von Netzwerktraffic (Stichwort: Blaster, Sasser)
  - IPS = Intrusion Prevention (statt IDS = Intrusion Detection)
  - Erkennen von offenen (Windows-)Sicherheitslücken
  - Neue Filter: Anti-Spam, Anti-Spyware, Anti-Dialer …
  - Kurzum: Steigende Software- und Infrastruktur-Komplexität

# Herausforderungen (II)

- Reaktionsgeschwindigkeit bei Outbreaks (I)
  - Häufige Aktualisierung der Scannerdatenbanken wichtig
    - Vom Hersteller aus mehrmals pro Woche, besser mindestens einmal täglich und nach Bedarf auch öfter
    - Ca. 75 bis 100 neue Schädlinge pro Tag, davon schätzungsweise aber nur etwa 1 bis 2 Prozent kritisch

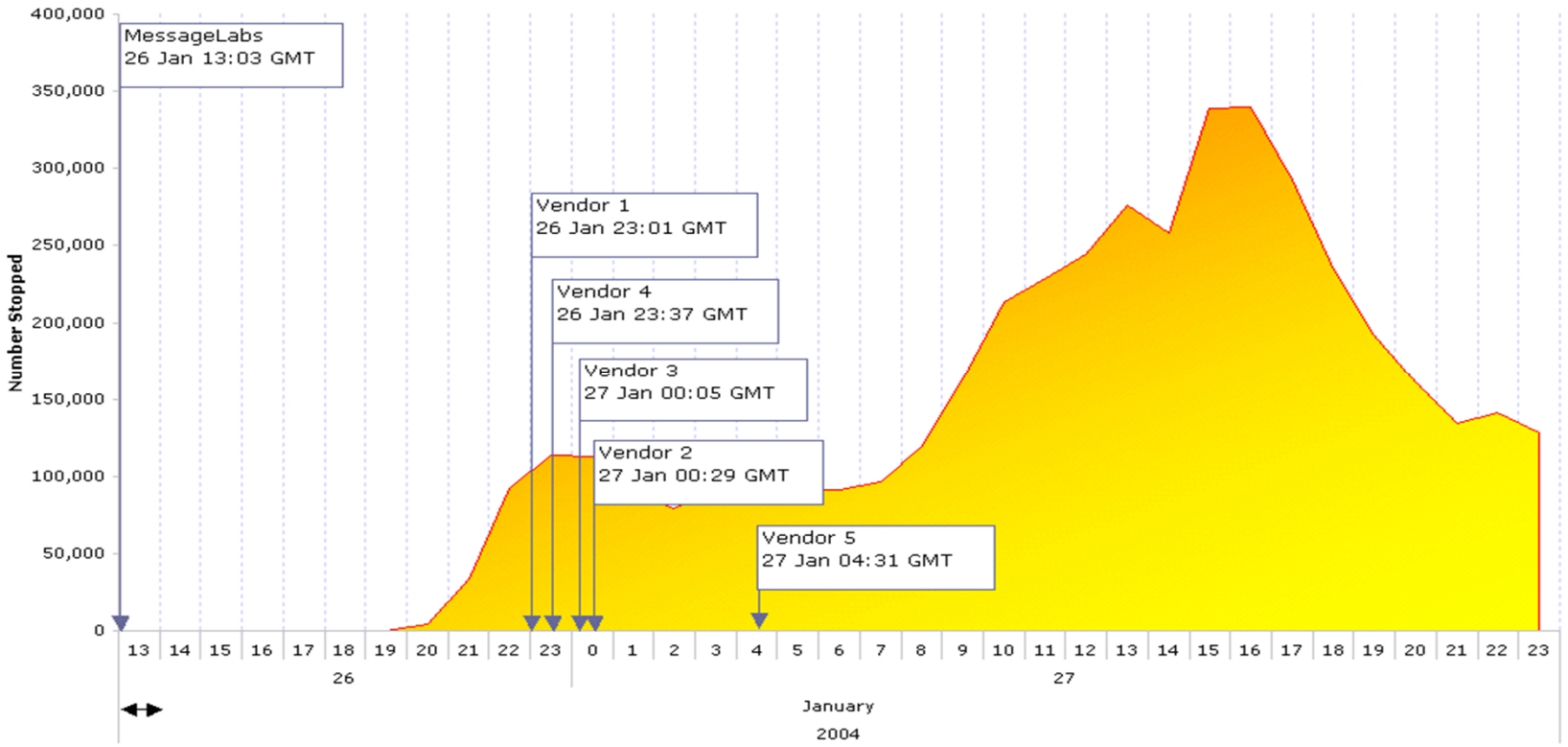
      → Jeden Tag gibt es mindestens eine echte, neue Bedrohung!
  - Hersteller: Definitionsupdates rechtzeitig bereitstellen…
    - Wichtig ist eine schnelle Reaktion, wenn was los ist und nicht, wenn es technisch (un-)möglich ist, Updates herauszugeben
    - Hersteller warten oft ab, wie sich ein neuer Wurm „entwickelt“ statt sofort zu handeln (Wichtig: Meldungen an AV-Hersteller!)

# Herausforderungen (III)

- Reaktionsgeschwindigkeit bei Outbreaks (II)
  - … und regelmäßig auf Updates prüfen und rechtzeitig automatisch einspielen lassen (vom Kunden)!
    - Priorität: Internet Gateway-Systeme (z.B. E-Mail-Schutz)
    - Komplette Verteilung im Rest des Unternehmens nach Bedarf
    - Achtung! Nebenwirkungen: Jedes Update ist Software-Patch!
- Durchschnittliche Outbreak-Reaktionszeit von AV-Herstellern im Jahr 2004 und im 1. Quartal 2005
  - Bei Würmern: ca. 8 bis 12 Stunden
  - Bei anderer Malware (z.B. Online Banking-Trojaner, die für Phishing genutzt wurden): Oft noch mehrere Tage
    → Daher ist Inhaltsfilterung unverzichtbar!

# Beispiel: Mydoom.A - Outbreak

**Datenquelle: © 2004 MessageLabs**



# Herausforderungen (V)

- Signaturdatenbanken von Virenscannern wachsen auf Grund der Malware-Flut ins Unermessliche
  - Es gibt heute ca. 125.000 verschiedene Schadprogramme (inklusiver vieler „Altlasten“ aus MS DOS-Zeiten)
  - Typisches Wachstumsbeispiel (Trend Micro):
    - August 2001: 4,0 MB
    - Januar 2004: 7,5 MB
    - Januar 2005: 11,8 MB
    - April 2005: 14,7 MB
  - 10 Jahre hat es gebraucht (1991 bis 2001), damit die Datenbank 4 MB groß wird, aber nur wenige Monate, bis sich ihre Größe mehr als verdoppelt und verdreifacht hat
  - Allein in den letzten 4 Monaten ganze 3 MB Wachstum

# Aktuelle Malware-Entwicklungen (I)

- Virenschreiber werden immer professioneller
  - Früher: Schlagzeilen in den Medien produzieren
  - Heute: Geld, Geld, Geld (organisierte Kriminalität)
    - Online-Banking (Phishing) und Spam am lukrativsten
- Integrierte Malware („All-Inclusive“-Prinzip)
  - Kombination von Viren, Würmern, Trojanischen Pferden, Backdoors, sowie Ad- und Spyware
  - Wenig Rechner infizieren, damit die Schadsoftware nicht so schnell auffällt und irgendwann nach einigen Kundenreports von AV-Software erkannt und eliminiert wird
  - „Seeding“ von weiterer Malware, Spam-Schleudern, Schutzgelderpressung per DDoS-Attacken

# Aktuelle Malware-Entwicklungen (II)

- Bot-Netzwerke (Spybot, SDBot, Agobot & Co.):
  - Quelltexte vieler Bots sind frei im Internet verfügbar
    - Anpassen, kompilieren, komprimieren und verschicken
  - Gestern: Zentralisierter Ansatz
    - Ein IRC-Server, der alle „Anmeldungen“ verwaltet
    - Killt man den Server, ist das Bot-Netzwerk „tot“
  - Aktuelle Erweiterungen:
    - Listen mit weiteren (Backup-)IRC-Servern
    - Verschlüsselte Kommunikation (AES-128 oder besser)
  - Morgen: Dezentralisierter (P2P-)Ansatz
    - Vergleich: Napster konnte man durch die Abschaltung des Zentralservers einfach vom Netz nehmen, aber bei eDonkey gibt es „kein Anfang und kein Ende“

# Aktuelle Malware-Entwicklungen (III)

- Pro Tag erscheinen mittlerweile ca. 75 bis 100 neue Malware-Programme und Varianten bekannter Schadsoftware
  - Hauptanteil: Kombinierte Angriffsmethoden (Bots)
  - Kaum noch „klassische“ Viren zu finden, die Dateien infizieren (zu kompliziert?)
- Häufiges Klassifikationsproblem: Malware, Ad-/ Spyware vs. legitime Software
  - EULA vs. „Potentiell unerwünschtes Objekt“
  - Klagen und gerichtliche einstweilige Verfügungen gegen AV-Hersteller wegen einer Erkennung

# Aktuelle Malware-Entwicklungen (IV)

- Malware-Schreiber „testen“ neue Varianten gegen AV-Software vor der Freisetzung
  - Selbst die beste Heuristik nützt oft nichts mehr
    - So lange modifizieren, bis nichts mehr erkannt wird
  - Wenn ein AV-Update erschienen ist, erscheint genauso schnell eine nicht erkennbare Version
    - Neue Varianten werden auf Vorrat produziert
- Trick mit „Malformed Mails“ (d.h. nicht RFC-konform)
  - Beispiel: Keine abschließende Anführungszeichen im Dateinamen, Scanner geht von deren Existenz aber aus und sieht .ex statt .exe
    - Mail-Scanner sieht keinen (kritischen) Anhang und prüft somit nicht
    - MS Exchange und Outlook reparieren die Mail aber, der Anhang wird sichtbar und die Schadsoftware wird erst auf dem Groupware-System oder dem Client gefunden

# Aktuelle Malware-Entwicklungen (V)

- Nur „Download-Link“ schicken, keine Mail-Anhänge
  - Rechner wird erst beim Besuch einer Webseite infiziert
    - Sicherheitslücken in gängigen Browsern sei Dank → Patches!

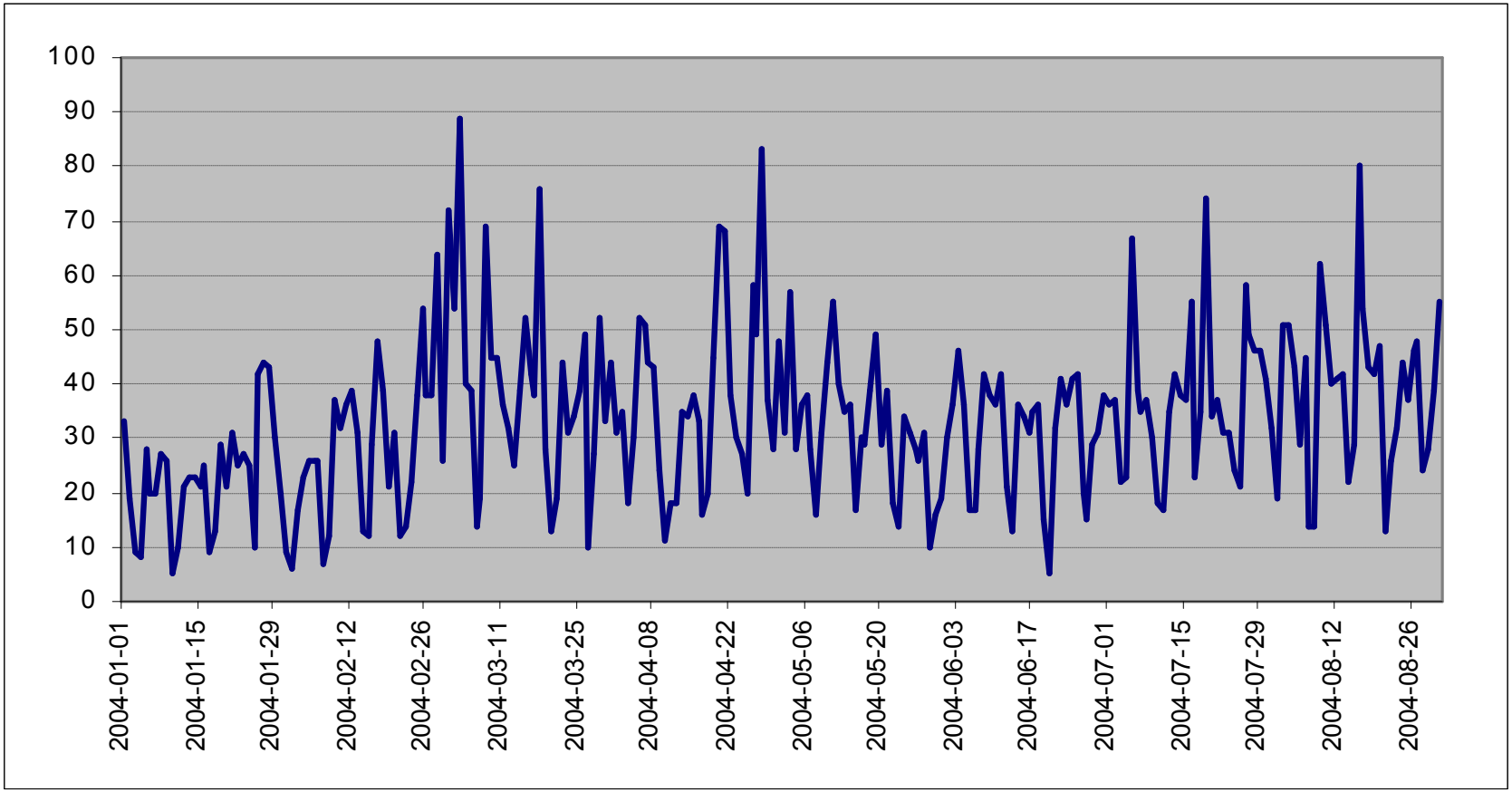
  → Links mit in die Filterung einbeziehen, http/ftp-Daten prüfen
- Deaktivieren von Sicherheitssoftware
  - Heimanwender meist mit Administrator-Rechten
    - Oft keine oder nicht alle Patches eingespielt
    - Schon gar kein Sicherheitsbewusstsein

      → Einfache „Beute“ für Malware
  - Beenden von Prozessen, Löschen von Dateien…
    - Erneute Installation von AV-Software unmöglich machen
  - „Selbstschutz“ der Malware vor Entfernung
    - Viele Startpunkte und „Backups“, schwer zu entfernen

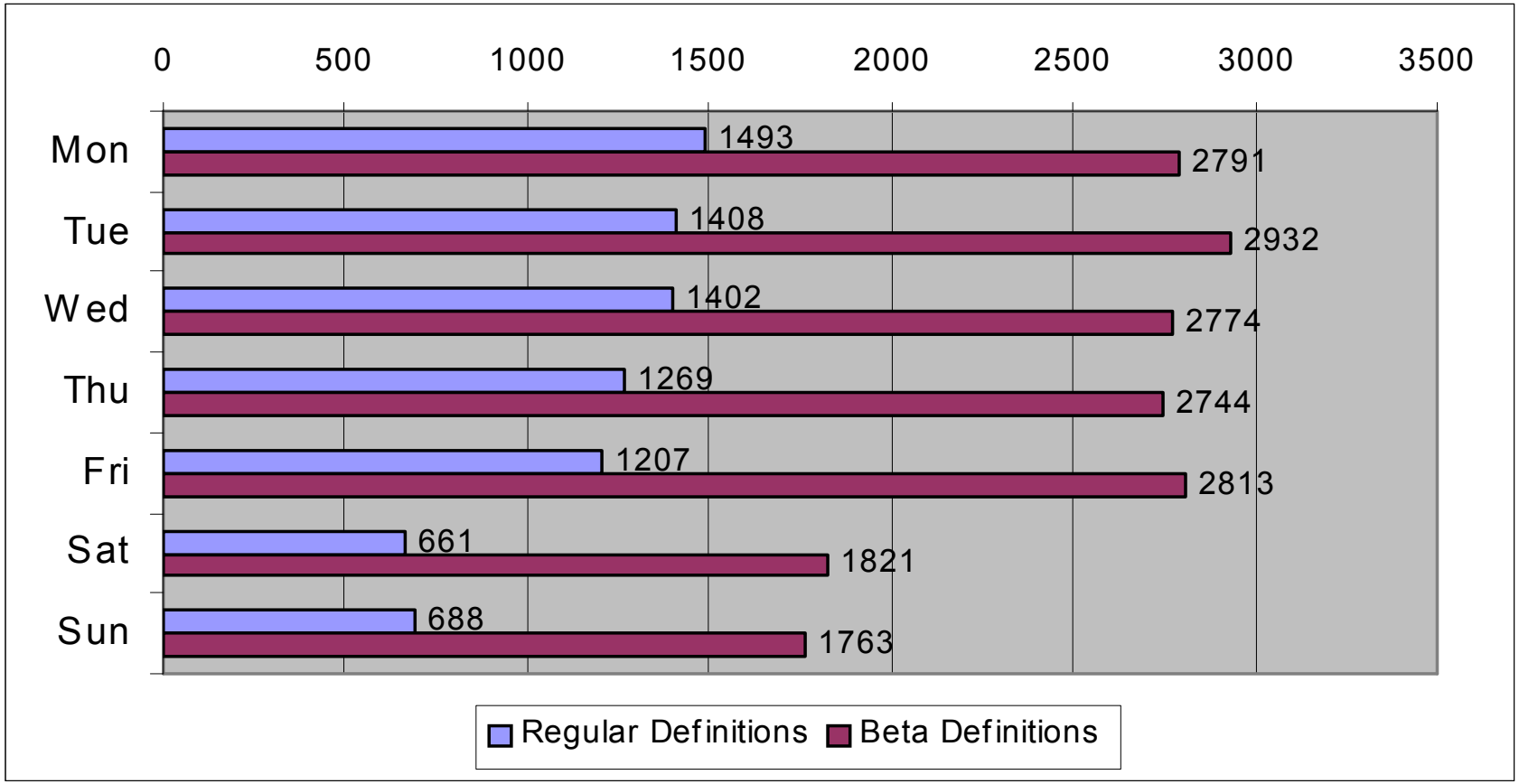
# Testergebnisse (I)

- Es folgen: Messergebnisse im Rahmen des Tests der Outbreak-Reaktionszeiten von AV-Produkten
- Updates von Virenscannern pro Quartal:
  - Q1 / 2004: 11.494 Dateien (35,4 GB)
  - Q2 / 2004: 15.761 Dateien (57,3 GB)
  - Q3 / 2004: 17.447 Dateien (63,9 GB)
  - Q4 / 2004: 17.103 Dateien (61,6 GB)
  - Q1 / 2005: 22.295 Dateien (77,8 GB)
  - Insgesamt: 84.100 Dateien (296 GB)

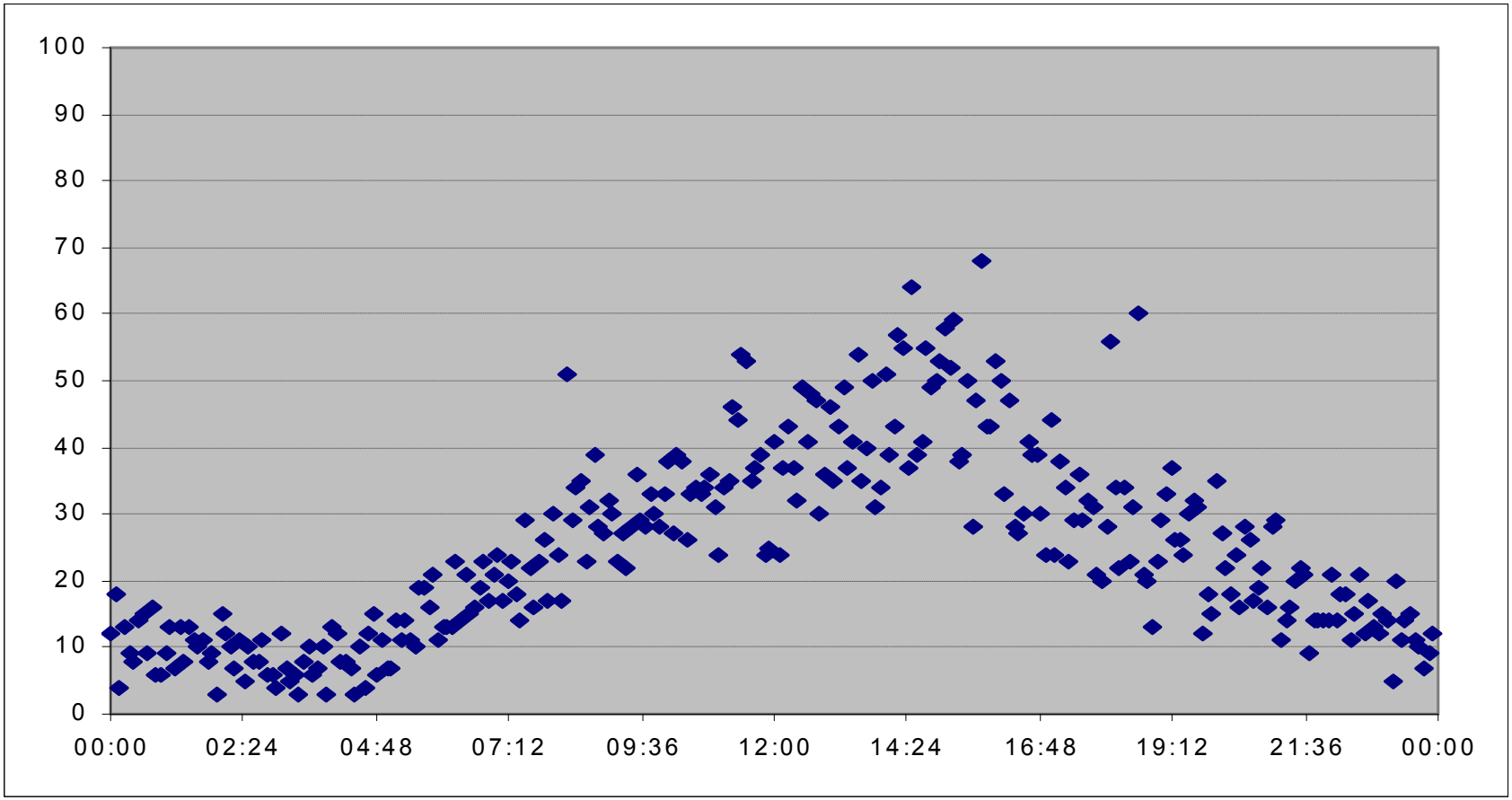
# TE (II) - Reguläre Updates pro Tag



# TE (III) - Updates pro Wochentag



# TE (IV) - Updates nach Tageszeit



# Testergebnisse (V)

- Reaktionszeiten: Letzter Sober-Ausbruch (I)
  - Heuristische Erkennung:
    - AntiVir Worm/Sober.gen
    - Dr. Web BACKDOOR.Trojan (probably)
    - eSafe Trojan/Worm (suspicious)
    - McAfee W32/Sober.gen@MM
    - QuickHeal Suspicious (warning)
  - Signaturerkennung (Auswahl):
    - ClamAV 2005-05-02 18:36 Worm.Sober.P
    - Kaspersky 2005-05-02 18:39 Email-Worm.Win32.Sober.p
    - F-Prot 2005-05-02 18:54 W32/Sober.O@mm (exact)
    - BitDefender 2005-05-02 19:19 Win32.Sober.O@mm
    - Sophos 2005-05-02 19:27 W32/Sober-N

# Testergebnisse (VI)

- Reaktionszeiten: Letzter Sober-Ausbruch (II)
  - Signaturerkennung (Fortsetzung):
    - Command 2005-05-02 20:07 W32/Sober.O@mm (exact)
    - Ikarus 2005-05-02 20:14 Email-Worm.Win32.Sober.P
    - VirusBuster 2005-05-02 20:44 I-Worm.Sober.Q
    - Panda 2005-05-02 20:49 W32/Sober.V.worm
    - eTrust (CA) 2005-05-02 21:54 Win32/Sober.53554!Worm
    - Norman 2005-05-02 22:46 Sober.O@mm
    - Trend Micro 2005-05-02 23:18 WORM_SOBER.S
    - AVG 2005-05-02 23:27 I-Worm/Sober.P
    - eTrust (VET) 2005-05-03 00:15 Win32.Sober.N
    - Symantec 2005-05-03 02:38 W32.Sober.O@mm
    - RAV 2005-05-04 08:52 Win32/Sober.Q@mm

# Testergebnisse (VII)

| Hersteller | Updates/Tag (Januar 2005) | Durchschnittliche Reaktionszeit (45 Outbreaks im Jahr 2004) |
|---|---|---|
| Kaspersky | 18.5 | < 4 Stunden |
| Sophos | 2.7 | < 8 Stunden |
| Bitdefender | 1.7 | < 4 Stunden |
| ClamAV | 1.5 | wenn erkannt, dann < 6 Stunden |
| AntiVir | 1.4 | < 6 Stunden |
| F-Secure | 1.4 | < 6 Stunden |
| Panda | 1.3 | < 6 Stunden |
| Trend Micro | 1.0 | < 10 Stunden |
| Norman | 0.5 | < 10 Stunden |
| McAfee | 0.2 | < 14 Stunden |
| Symantec | 0.2 | < 16 Stunden |

# Gegenmaßnahmen (I)

- **Alle** ein- und ausgehenden Daten müssen an Internet- **und** Intranet-Gateways gefiltert werden
  - Generell alle Mails auf Schädlinge prüfen (und nicht nur die)
    - Andere Infektionswege wie VPN oder USB nicht vergessen!
  - Einsatz mehrerer verschiedener AV-Engines sinnvoll, da andere Schwerpunkte, etwa bei Erkennungsraten (Viren und Exploits) und Reaktionszeiten bei Outbreaks
    - Fehlalarmen vorbeugen: Quarantäne statt Löschen!
  - Danach erst potentiell gefährliche Inhalte aussortieren
    - Wenn man schon vorher filtert, erhält man weniger brauchbare Statistiken („100 EXE-Dateien gefiltert“ vs. „50 Netskys, 39 Mydooms, 10 Bagles und eine unbekannte EXE-Datei“)
    - Benachrichtigungsoptionen besser nutzen

# Gegenmaßnahmen (II)

- Stichwort Inhaltsfilterung
  - Keine direkt ausführbaren Dateien per Mail empfangen oder verschicken (Blacklisting)
    - Alternativen nutzen: Web-Downloads, (s)ftp-Server
  - Nur erwünschte Dateien zulassen (Whitelisting)
    - Auch „reine“ Datendateien wie JPG, ANI, GIF, BMP oder MP3 können Schadcode enthalten und ihn durch Sicherheitslücken (meist Buffer Overflows) zur Ausführung bringen → Minimal-Prinzip!
    - Jede Abteilung hat spezifische Bedürfnisse (PR vs. HR)
    - Restrisko abschätzen und dokumentieren

# Gegenmaßnahmen (III)

- AV-Software auf allen Systemen einsetzen
  - Mail-Gateway: Laufend automatisch aktualisiert
    - Mindestens (!) ein Update-Check pro Stunde
  - Groupware-Systeme: Regelmäßig updaten
  - Client- und Server-Systeme: Nach Bedarf
    - Nicht jedes Update muss sofort unternehmensweit verteilt werden, besser vorher gründlich prüfen
    - Jedes AV-Update ist letztendlich ein Software-Patch
  - Welche Systeme sind nicht geschützt?
    - Bedrohungen und Risken einschätzen
- Ausblick: Cisco+Microsoft NAC/NAP

# Gegenmaßnahmen (IV)

- Und wenn doch mal was passiert…
  - Reinigungsfunktion der AV-Software nur als Mittel, den Infektionsherd schnell los zu werden ansehen (Anzahl der Neuinfektionen eindämmen)
  - Systeme generell neu aufsetzen (Imaging)
  - Denn: Keiner weiß, ob die Desinfektion wirklich komplett und erfolgreich war, sowie welche „Nebenwirkungen“ (etwa weitere Malware) der Schädling noch so mitgebracht hat
    - Beispiel: Wurm ist entfernt, Backdoor aber noch aktiv
  - Alle Service Packs und Patches einspielen, bevor der Rechner wieder ins Unternehmensnetzwerk darf

# Gegenmaßnahmen (V)

- Immer alle Ebenen in einem Schutzkonzept (IT-Sicherheitsstrategie) berücksichtigen:
  - TORP = Technisch, Organisatorisch, Rechtlich und Personell
  - In diesem Vortrag wurde nur der technische Aspekt entsprechend gewürdigt, d.h. 25 Prozent
  - Umgesetzt wird oft allein das technisch mögliche, die restlichen 75 Prozent werden oft vergessen
    - Technik: Es ist nur ein Schritt in die richtige Richtung
    - Mitarbeiter-Schulungen helfen! (Verständnis…)

# Gibt es Fragen?

- Gibt es Fragen?