Aktuelles in der IT-Sicherheit

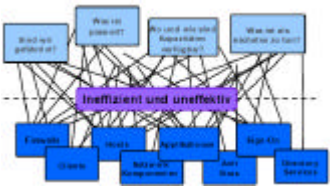
Dr. G. Weck, INFODAS GmbH, Köln
Rheinlandtreffen 7./8.11.2006
Schloß Birlinghoven

Inhalt

- Bericht vom DECUS-Symposium 2006
  - Vorträge: Sicherheitsmanagement, Technik, Jura
- Aus den GI-Arbeitskreisen
  - Präsidiumsarbeitskreis Datenschutz und IT-Sicherheit
  - Arbeitskreise Lehre
- Aktuelle Hacking-Tendenzen
  - Statistiken
    - Sicherheitslücken / Verwundbarkeiten
    - Angriffsspektrum / Schadensverteilung
    - Denial-of-Service Angriffe und Bot-Netze
    - Phishing und Schadsoftware
  - Aktuelle Tendenzen

Vorträge zum Sicherheitsmanagement

- BSI Grundschutz / ISO 27001 / ITIL
  - unterschiedliche Standards wachsen zusammen
  - ISO 27001-Zertifizierung nach IT-Grundschutz
    - international anerkannte Zertifikate
    - ... dennoch aussagekräftig!
  - BS 7799 geht in internationalem Standard auf
  - Security Information Management als zentrales Thema aller Standards
- IT-Sicherheit nicht-technisch
  - Motivation / Schulung / Ausbildung
- Information Lifecycle Management
  - Ordnung im Chaos?
  - Nutzen der Log-Auswertung
  - Security Policy



Juristische Aspekte der IT-Sicherheit

- Mit Datenschutz Geld verdienen
  - Anforderung zur Bereitstellung eines Verfahrensverzeichnisses, wenn kein bDsb vorhanden ist
  - fehlende Compliance kann zu Abmahnungen führen
- Software Escrow
  - Quellcode-Hinterlegung bei vertrauenswürdigem Dritten
  - notwendige Ergänzung des Risikomanagements
- Sarbanes-Oxley, Basel II und und IT-Sicherheitsmanagement
  - Basel II: Bestimmung und Verwaltung des operationellen Risikos
  - Sarbanes-Oxley :
    - Management ist voll verantwortlich und schuldfähig
    - Management muss sicherstellen, dass die Informationen rechtzeitig und insgesamt unverfälscht bereitgestellt werden können.

Vorträge zur technischen Sicherheit

- Von RFID zur Biometrie
- Honeywall
- Aspekte vertrauenswürdiger Systeme
  - Trusted Computing – Lösungen und Perspektiven
  - Hochsicherheits-Gateway
  - Sichere Benutzerauthentifizierung
- Anwendungssicherheit
  - Web Application Security
  - Enterprise E-Mail Security
  - Sicherheit IP-Telefonie
  - Gateway Security
  - Personal Firewall
- Sicherheit(slücken) durch Verschlüsselung
  - Sicherheitslücke SSL-Traffic
  - Unterschiede SSL VPNs zu HOBs Remote Desktop VPN
- Computer-Viren aktuell

GI-Präsidiumsarbeitskreis Datenschutz und IT-Sicherheit

- Datenweitergabe der Biometrie-Daten des Personalausweises an „Interessierte Dritte“
  - Überlegungen des BMI zur Finanzierung der neuen Pässe und Personalausweise
  - Stellungnahme / Pressemitteilung des GI-PAk
  - Presseecho (Spiegel Online, Deutschlandfunk ...)
  - Drohungen des BMI mit Strafverfolgung
  - Weisung des Bundeskanzleramtes am das BMI, „die Überlegungen sofort einzustellen“
- Workshop Biometrie in Kooperation war mit dem Bundesbeauftragten für den Datenschutz geplant
  - wegen Abstimmungsproblemen vom BfD allein durchgeführt

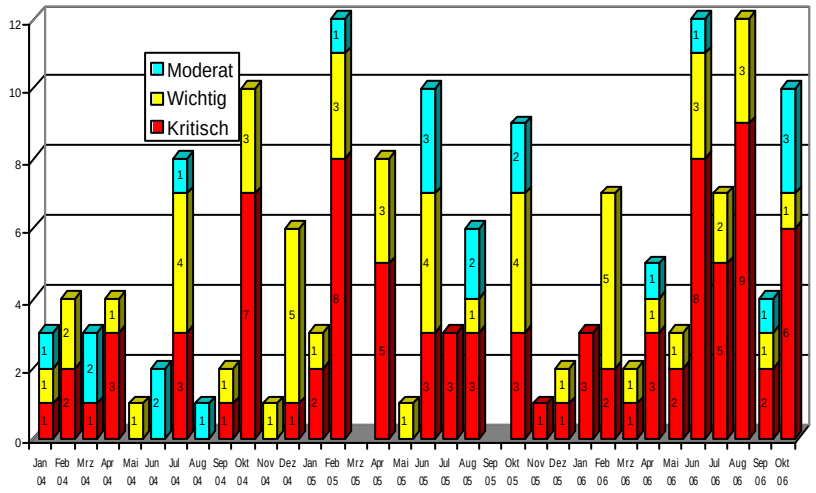
GI-Präsidiumsarbeitskreis Datenschutz und IT-Sicherheit

- Grundsatzpapier zur Identifizierung und Überwachung („Bonner Memorandum“)
  - Diskussion grundsätzlicher Risiken und Schwachstellen
  - Forderung nach Bewertung der Technik in breiter gesellschaftlicher Diskussion
- Stellung nahme zur Nutzung von iTANs beim Home-Banking
  - zusätzlicher Aufwand ohne wirklichen Nutzen
  - iTANs können fast so gut zum Phishing verwendet werden wie normale TANs
  - Banken nicht bereit, geringe Sicherheit zuzugeben

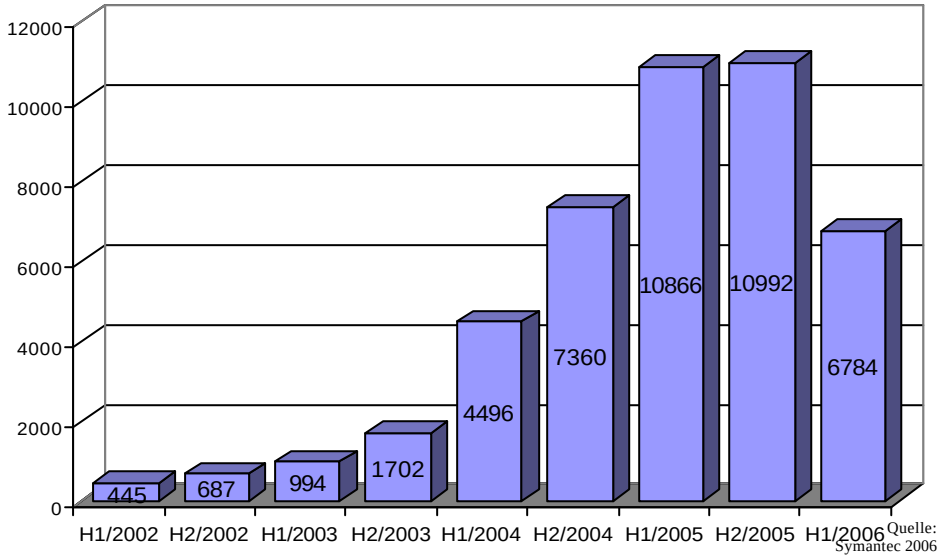
GI-Arbeitskreis Lehre

- Empfehlung zur Verankerung des Themen-bereichs IT-Sicherheit in der Lehre
  - im universitären Bereich / an Fachhochschulen
    - Hauptstudium (Bachelor / Master)
    - als Ergänzung in Nebenfächern
  - im schulischen Bereich (Gymnasien, Berufsbildung)
- Empfehlung für die Schulen übernommen
- Empfehlungen für die Hochschulen unpräzise
  - Befindlichkeiten von Hochschullehrern
  - Furcht, die Themen nicht abdecken zu können

Microsoft Sicherheitslücken seit 2004

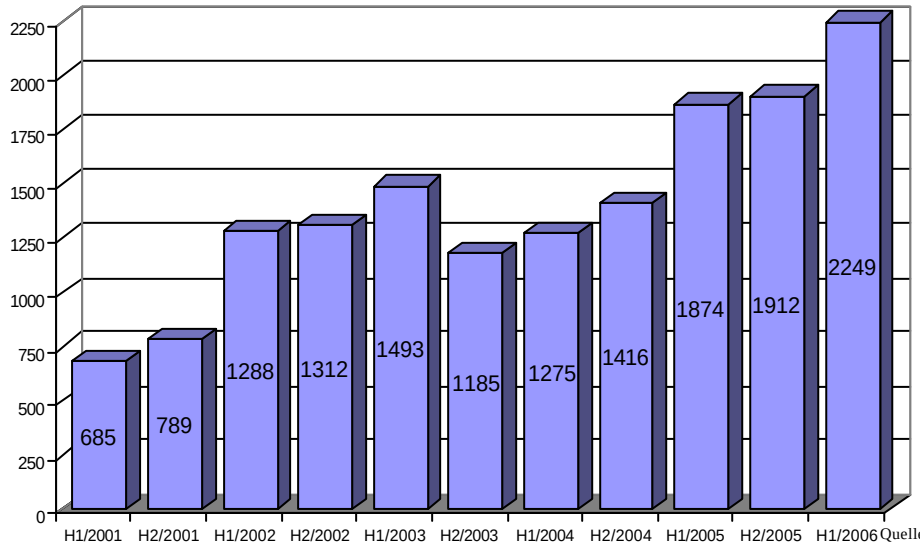


Anzahl Win32-Viren und -Würmer



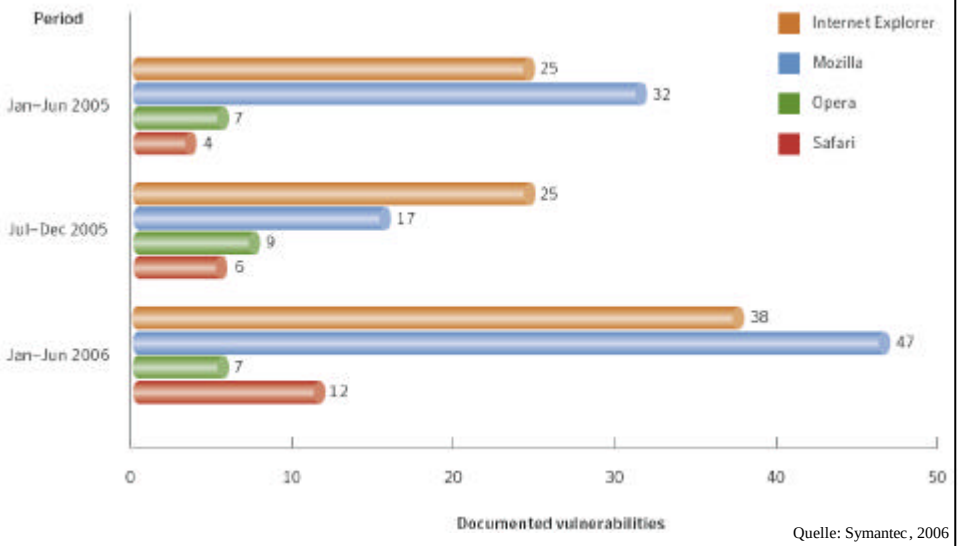
Quelle: Symantec 2006

Anzahl Verwundbarkeiten



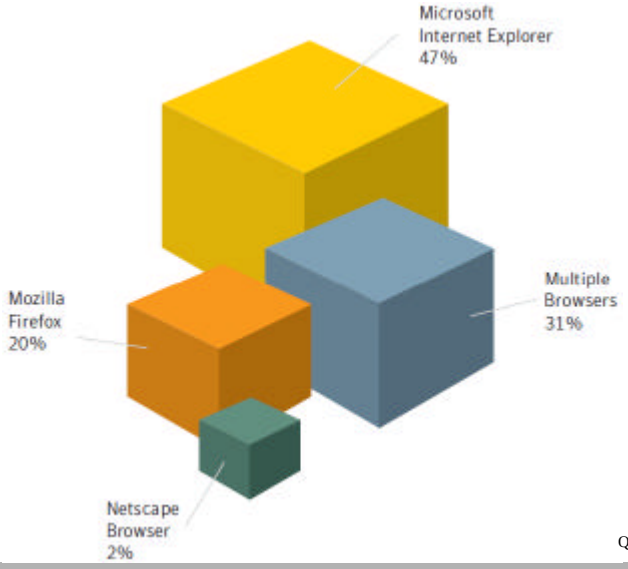
Quelle: Symantec 2006

Sicherheitslücken in Browsern



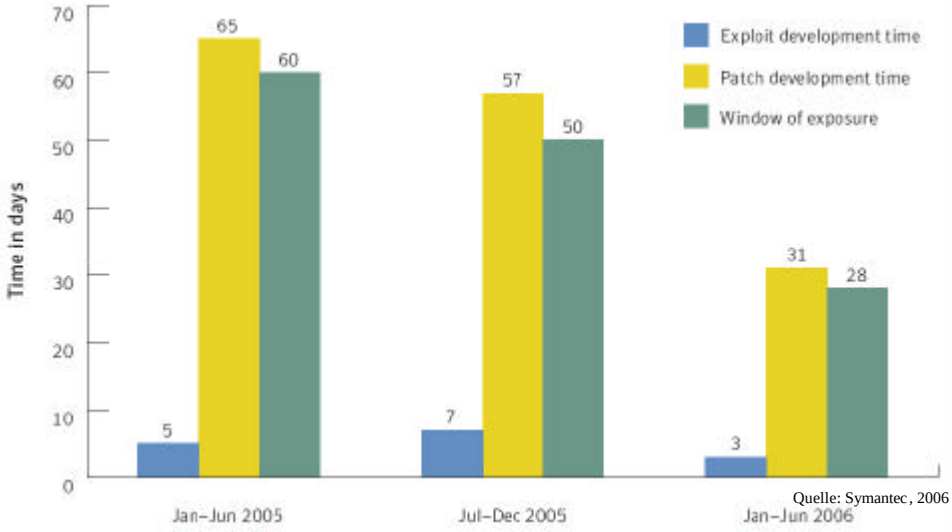
Quelle: Symantec, 2006

Angriffe auf Browser



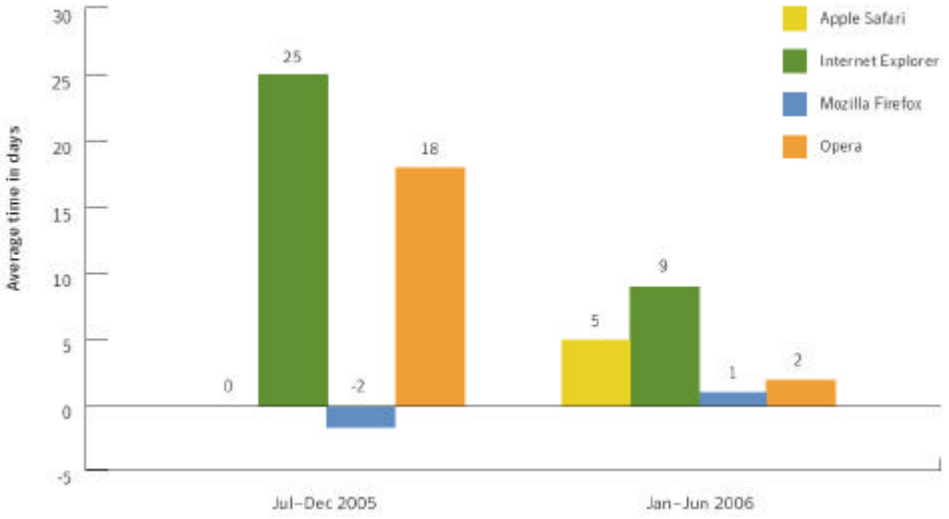
Quelle: Symantec, 2006

Zeitfenster für Angriffe



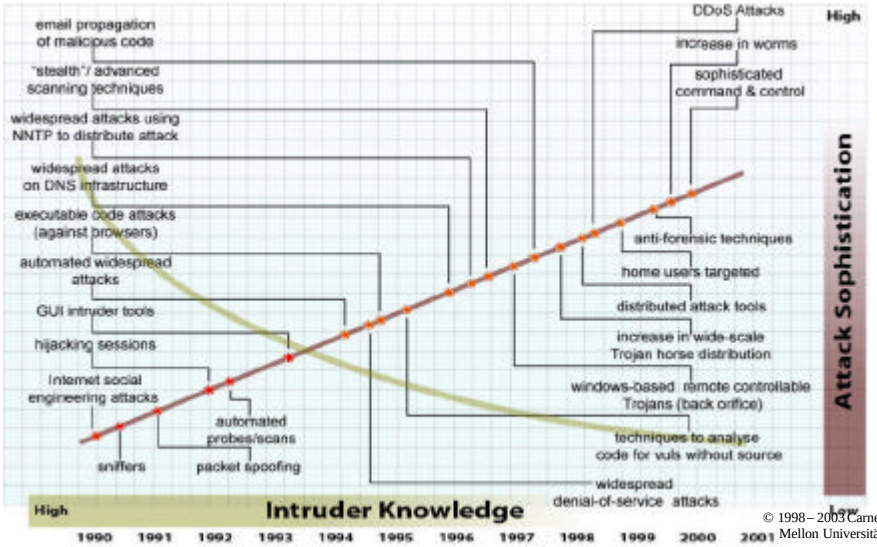
Quelle: Symantec, 2006

Zeitfenster für Browser-Angriffe

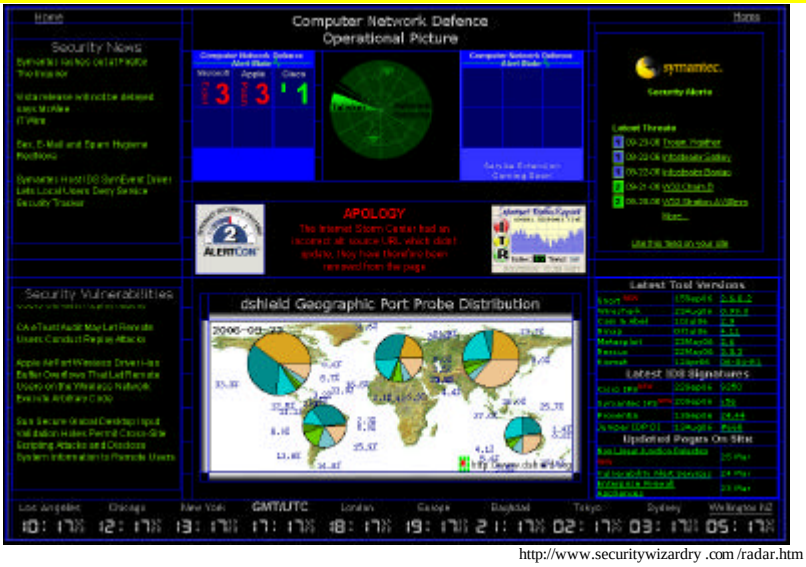


Quelle: Symantec, 2006

Hacking wird immer einfacher!

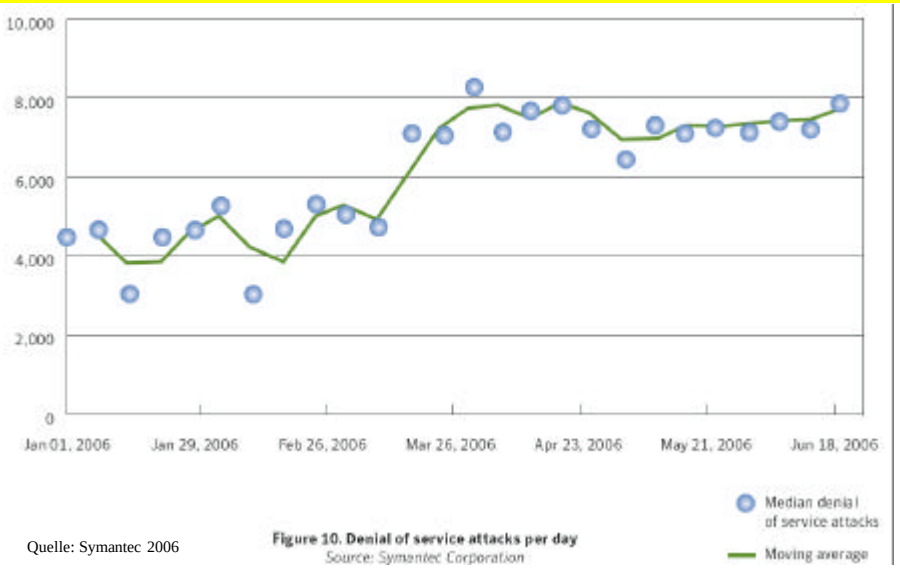


Talisker Internet Sicherheit



http://www.securitywizardry .com /radar.htm

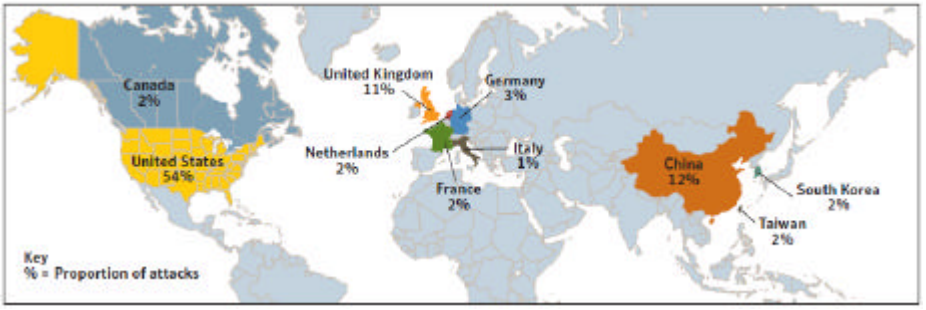
Denial-of-Service Angriffe



Quelle: Symantec 2006

Figure 10. Denial of service attacks per day
Source: Symantec Corporation

Weltweite Verteilung der Denial-of-Service Opfer

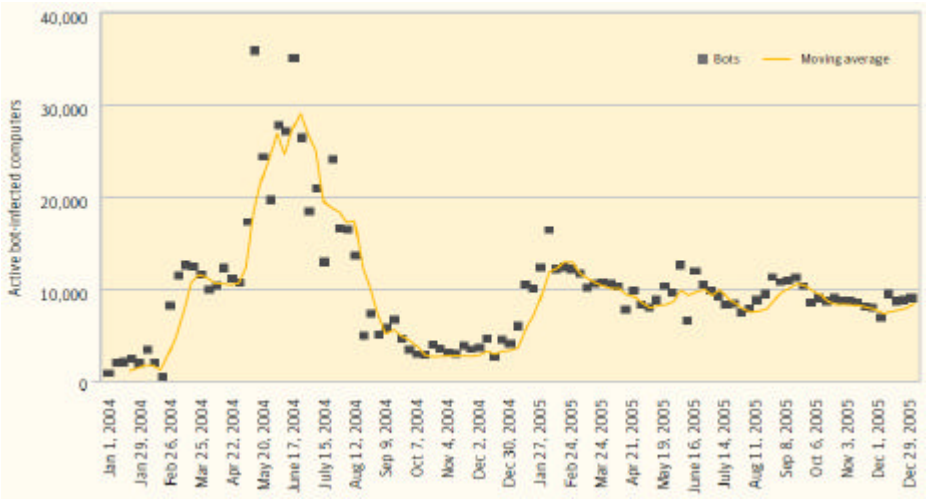


Quelle: Symantec, 2006

Entwicklung von Bot-Netzen

- Fernsteuerung gekaperter Rechner über Backdoor-Funktion
  - Installation durch Virus / Wurm / Sicherheitslücke
  - Kommandoübernahme über IRC / Web / Mail
  - Nachladen neuer Funktionalität
- Vielzahl von Schadensfunktionen
  - Angriffe auf Drittrechner
  - Ausspähen lokaler Daten
  - Lokale Manipulationen
  - Spam-Schleuder

Anzahl und Größe von Bot-Netzen



Quelle: Symantec 2006

Aktive Bot-Netze

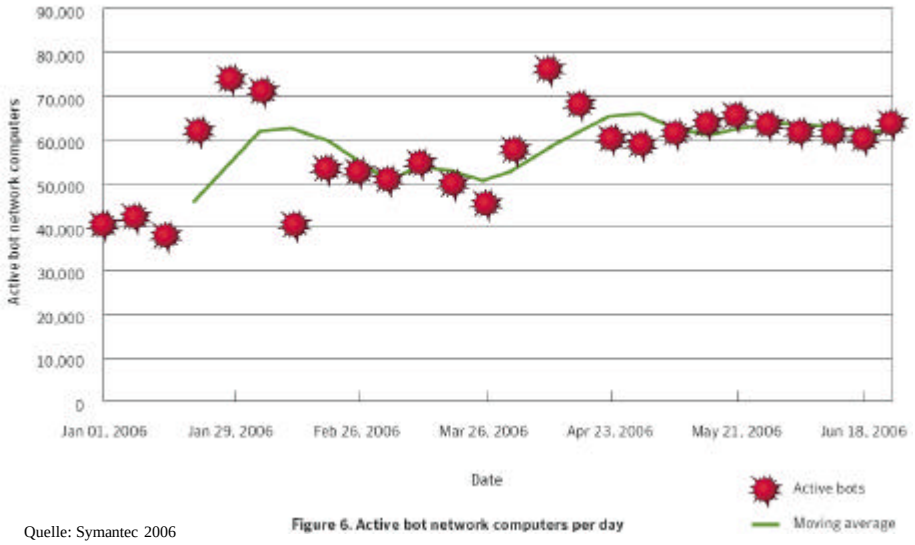
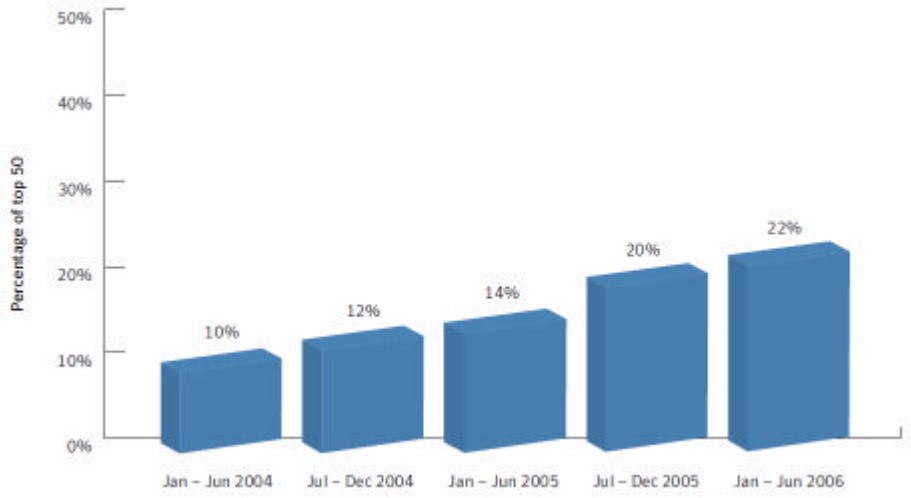


Figure 6. Active bot network computers per day

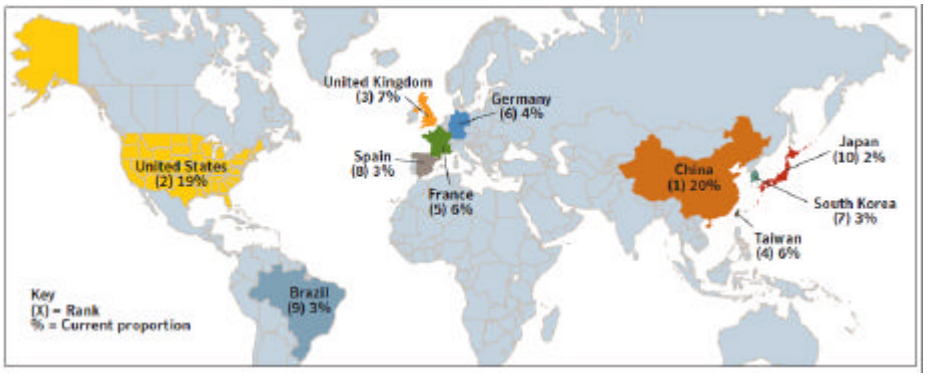
Quelle: Symantec 2006

Anteil der Bot-Infektionen an der Schadsoftware



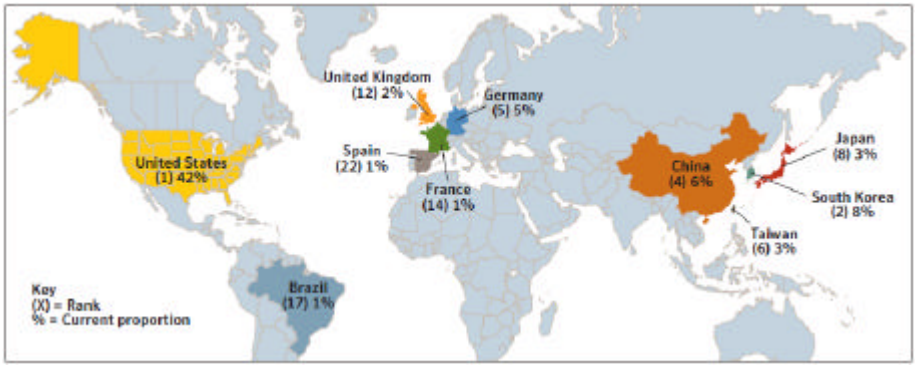
Quelle: Symantec 2006

Weltweite Verteilung Bot-infizierter Computer



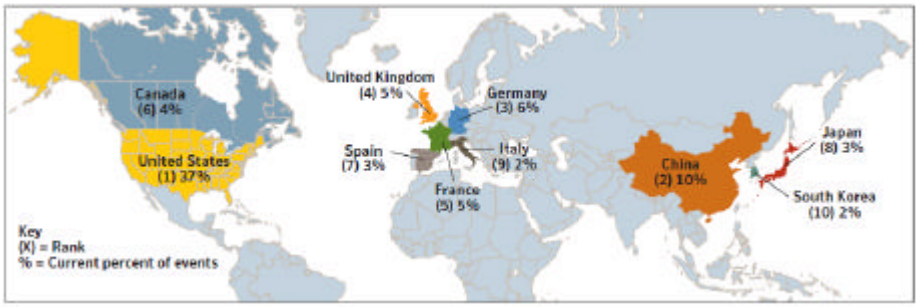
Quelle: Symantec 2006

Weltweite Verteilung der steuernden Systeme von Bot-Netzen



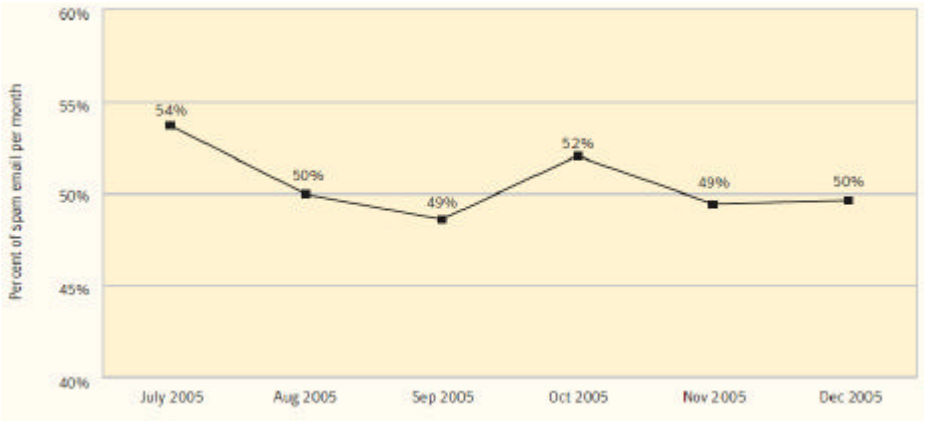
Quelle: Symantec 2006

Weltweite Verteilung der Angriffsquellen



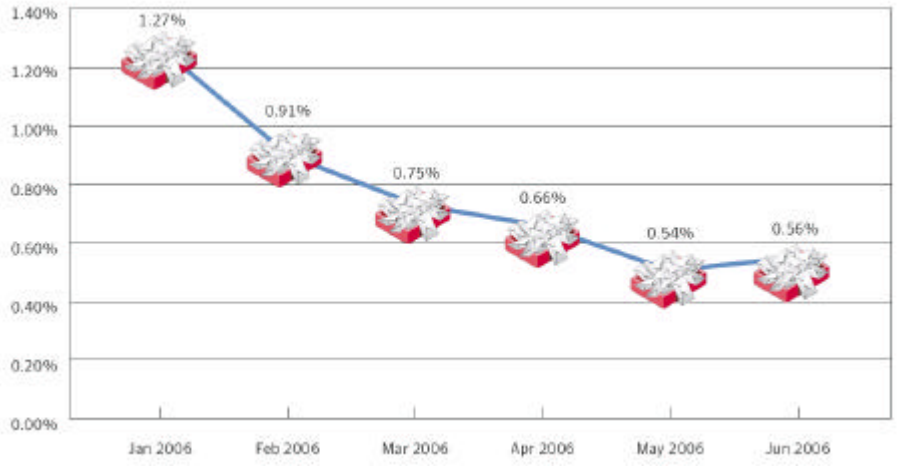
Quelle: Symantec 2006

Spam-Anteil am E-Mail-Aufkommen



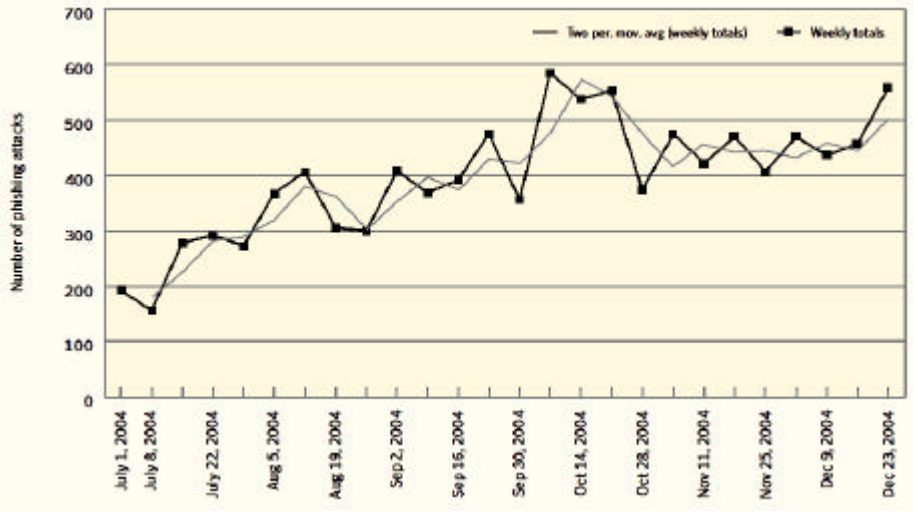
Quelle: Symantec 2006

Viren in Spam-Mail



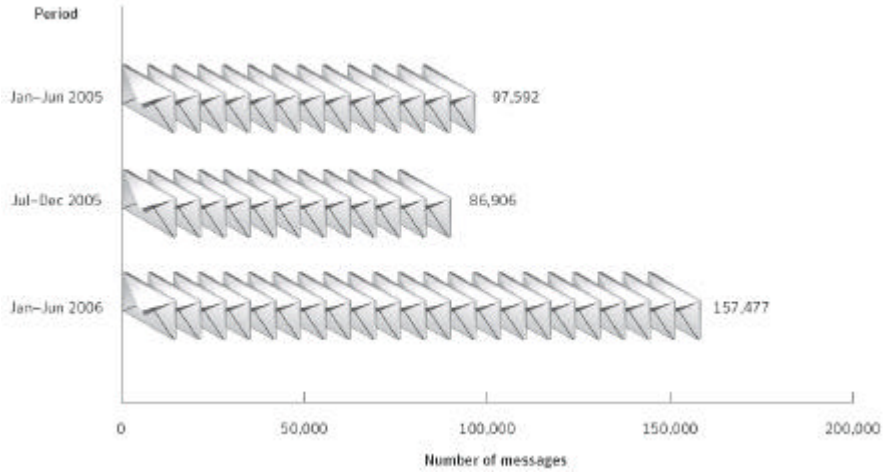
Quelle: Symantec 2006

Anzahl von Phishing-Angriffen



Quelle: Symantec, 2004

Anzahl von Phishing-Nachrichten



Quelle: Symantec 2006

Aktuelle Tendenzen

- Hacker-Szene wird immer professioneller
  - Zusammenarbeit mit der organisierten Kriminalität
  - Hauptziel ist kontinuierlicher Geldgewinn
    - Angriffe werden gezielter gegen ausgewählte Opfer gerichtet
    - keine spektakulären Angriffe, sondern schwer erkennbare Manipulationen
- Aufbau von Malware-Baukästen
  - Verbreitung über Viren / Websites
    - Laden eines fernsteuerbaren Frontends
    - Nachladen weiterer Funktionalität über HTTP / IRC
    - kollektive Steuerung der „Zombie“-Rechner in Bot-Netzen
  - Begrenzung der Größe einzelner Bot-Netze

Aktuelles in der IT-Sicherheit

Dr. G. Weck, INFODAS GmbH, Köln
Rheinlandtreffen 7./8.11.2006
Schloß Birlinghoven