# ... mehr als die Internet-Feuerwehr

**DFN-CERT Services GmbH**
**Dr. Klaus-Peter Kossakowski**
**kossakowski@dfn-cert.de**

## Agenda:

- Das DFN-CERT – Entstehung und Entwicklung
- Die Säulen der CERT-Arbeit
  - Proaktive Komponenten
  - Reaktive Komponente
- Die Bedrohungslage / Aktuelle Trends
- CERTs im nationalen und internationalen Verbund
- Neue Dienste und Möglichkeiten

DFN CERT

# Entstehung und Entwicklung

# Wer sind wir ?

- DFN-CERT Services GmbH
  - 1993 bis 1999 als Projekt an der Uni Hamburg
  - Kunde: DFN-Verein
  - Betreute Klientel: Anwender des DFN-Vereins
- Organisationsstruktur
  - Computer-Notfallteam
  - PKI Team
  - Infrastrukturteam
- Veranstaltungen
  - Jährlicher DFN-Workshop „Sicherheit in vernetzten Systemen“
  - Tutorien und Schulungen

# Aufgaben des Notfallteams

- Prävention
  - Security Advisories, Alarmmeldungen, Risiko Analyse, etc.
  - Schwachstellen Analyse, Intrusion Detection
  - Schulung und Ausbildung im Security Bereich
  - Ansprechpartner für Sicherheitsfragen / „Hotline“
- Reaktion
  - Incident Response Support
  - Aufarbeitung und Auswertung von Vorfällen
  - Koordination der Bewältigung, Information anderer
  - Zusammenarbeit mit anderen Notfallteams
- Verbesserung des Risikomanagements

DFN CERT

# Prävention
# Eine Säule
# der CERT-Arbeit

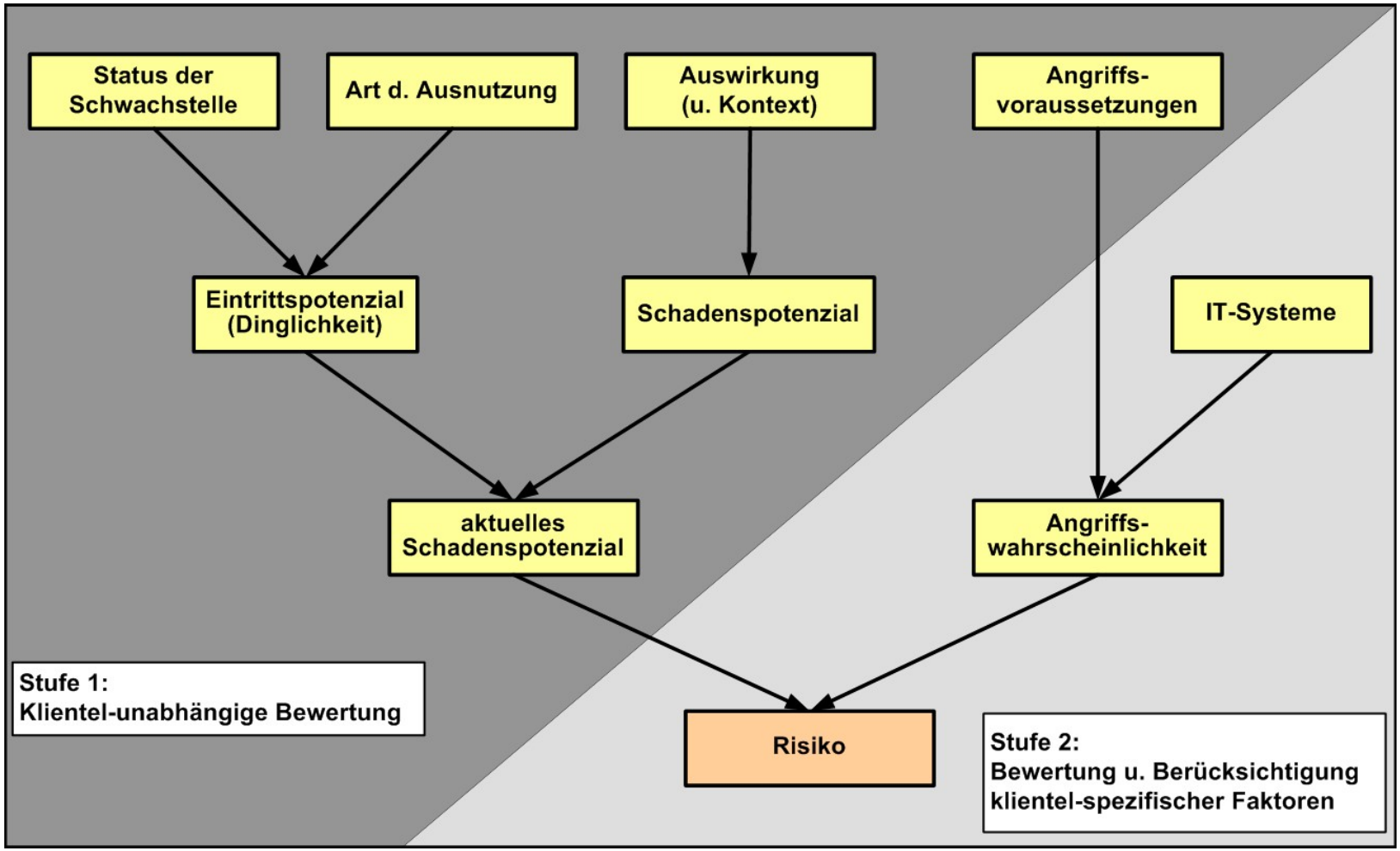
# Prävention: Security Advisories

Grundlage: Deutsches Advisory-Format (DAF)

- Einheitliches Format für Erstellung und Austausch von Sicherheits-Advisories
- Entwickelt und gepflegt von
  - Cert-BUND, DFN-CERT, Siemens CERT und PRESECURE
- XML-Format basierend auf EISPP (www.eispp.org)
- Mittelpunkt: eine Schwachstelle in einer Software oder Hardware
- Weiteres Ziel: Kundenportal („massgeschneiderte“ Advisories)

# Prävention: Security Advisories

## DAF: Klassifizierungsschema für Schwachstellen



# Prävention: Security Advisories

## DAF: Ermittlung der Eintrittswahrscheinlichkeit

**Dringlichkeit / Eintrittspotenzial**

| Eintrittspotenzial | Verbreitungsmethode | | |
|---|---|---|---|
| Status der Schwachstelle | manuell | automatisch | replizierend |
| theoretisch | sehr gering | gering | mittel |
| ausnutzbar | gering | mittel | hoch |
| aktiv | mittel | hoch | hoch |
| Exploit veröffentlicht | mittel | hoch | sehr hoch |

# Prävention: Security Advisories

## Ermittlung des potentiellen Schadens

**Schadenspotenzial**

| Schadenspotenzial | Kontext | | | |
|---|---|---|---|---|
| Verlust | Benutzer | Dienst | System | Netzwerk |
| Übernahme der Kontrolle | hoch | hoch | sehr hoch | sehr hoch |
| Übernahme von Berechtigungen | mittel | mittel | hoch | hoch |
| Integrität | gering | mittel | hoch | hoch |
| Vertraulichkeit | sehr gering | gering | mittel | hoch |
| Verfügbarkeit | sehr gering | gering | mittel | hoch |
| Umgehung von Sicherheitsmaßnahmen | sehr gering | gering | mittel | hoch |

# Prävention: Security Advisories

## DAF: Ermittlung des Gesamt-Risikos einer Schwachstelle

**aktuelles Schadenspotenzial**

| aktuelles Schadenspotenzial | Schadenspotenzial | | | | |
|---|---|---|---|---|---|
| Eintrittspotenzial | sehr gering | gering | mittel | hoch | sehr hoch |
| sehr gering | sehr gering | sehr gering | gering | gering | mittel |
| gering | sehr gering | gering | gering | mittel | hoch |
| mittel | gering | gering | mittel | hoch | hoch |
| hoch | gering | mittel | hoch | hoch | sehr hoch |
| sehr hoch | mittel | hoch | hoch | sehr hoch | sehr hoch |

# Prävention: Security Advisories

| | |
|---|---|
| **Plattform Categorisation** | Windows, Windows 95/98/ME, Windows NT, Windows 2000, Windows XP, Windows Server 2003 |

**Plattform Description**

Microsoft Windows NT Server 4.0 Service Pack 6a
Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
Microsoft Windows 2000 Service Pack 3 und 4
Microsoft Windows XP, Microsoft Windows XP Service Pack 1 und 2
Microsoft Windows XP 64-Bit Edition Service Pack 1
Microsoft Windows XP 64-Bit Edition Version 2003
Microsoft Windows Server 2003
Microsoft Windows Server 2003 64-Bit Edition
Microsoft Windows 98,
Microsoft Windows 98 Second Edition (SE)
Microsoft Windows Millennium Edition (Me)

| | |
|---|---|
| **Software Categorisation** | Client |

**Software Description**

Internet Explorer 5.01, 5.5 und 6

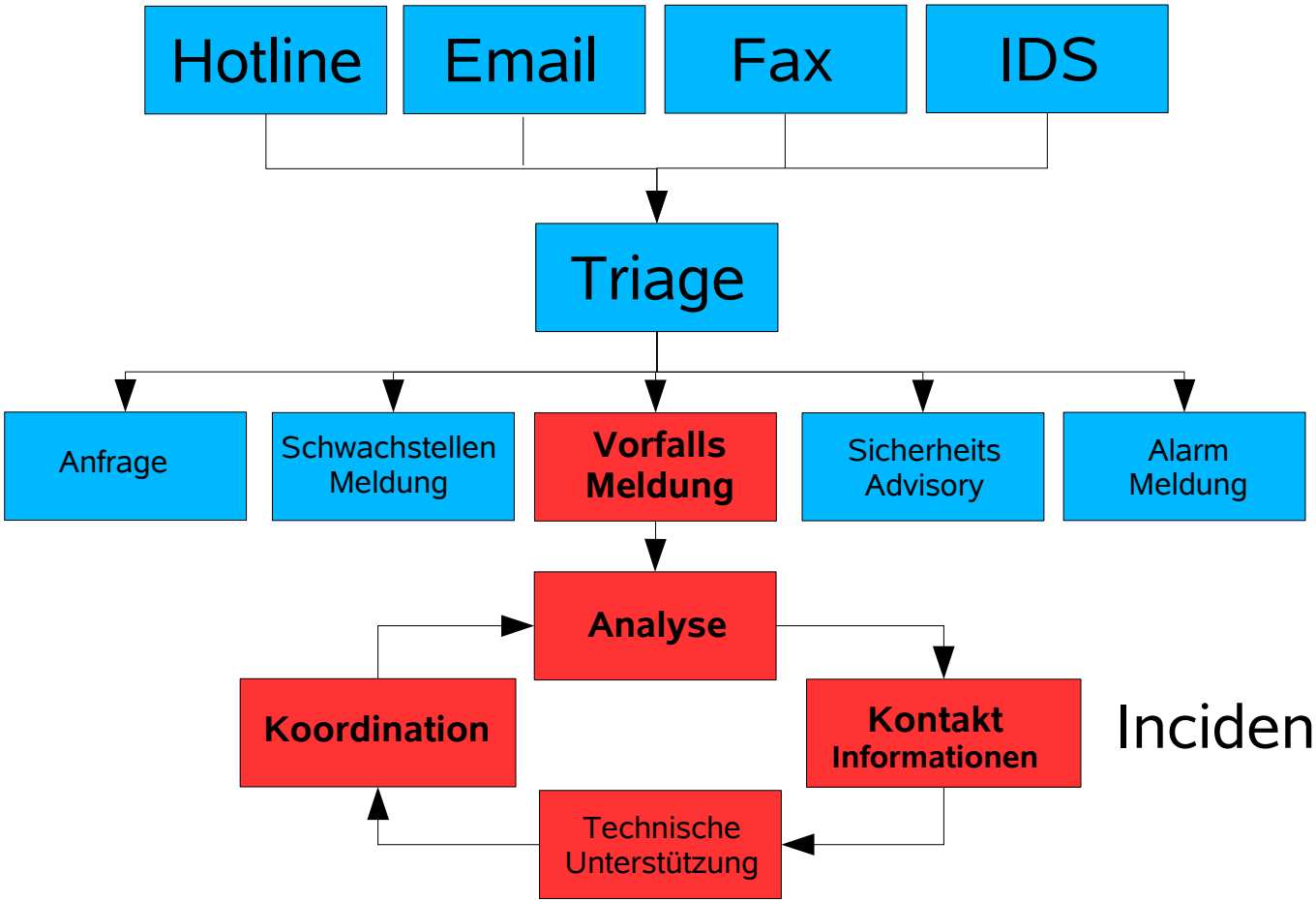
**Vulnerabilities**

| | |
|---|---|
| **Status** | Exploit published |
| **Propagation** | Automated |
| **Scope and Loss** | Code Execution as Admin (very high impact) |
| **Requirements** | Victim interaction: access content |
| **Categorisation** | Buffer Overflow, Heap Overflow, Cross-site Scripting |
| **Immediacy** | High (Proposal: High) |
| **Current Impact** | Very high (Proposal: Very high) |

DFN CERT

# Reaktion
# Eine Säule der CERT-Arbeit

# Betreuung und Koordinierung




Incident Handling

# Aufgaben der Experten

DFN CERT

Typische Aufgaben eines Incident Handlers

- Analyse von Vorfallsmeldungen
- Analyse von Vorfallsmaterial (Logfiles, Artefakte, etc.)
- Recherche nach Ansprechpartnern
- Technische Unterstützung der „Opfer“ (Telefon, Email, seltener vor Ort, etc.)
- Koordination und Verteilen von Informationen
- Zusammenarbeit mit anderen Teams, Einrichtungen, etc.

# Was wird gemeldet?

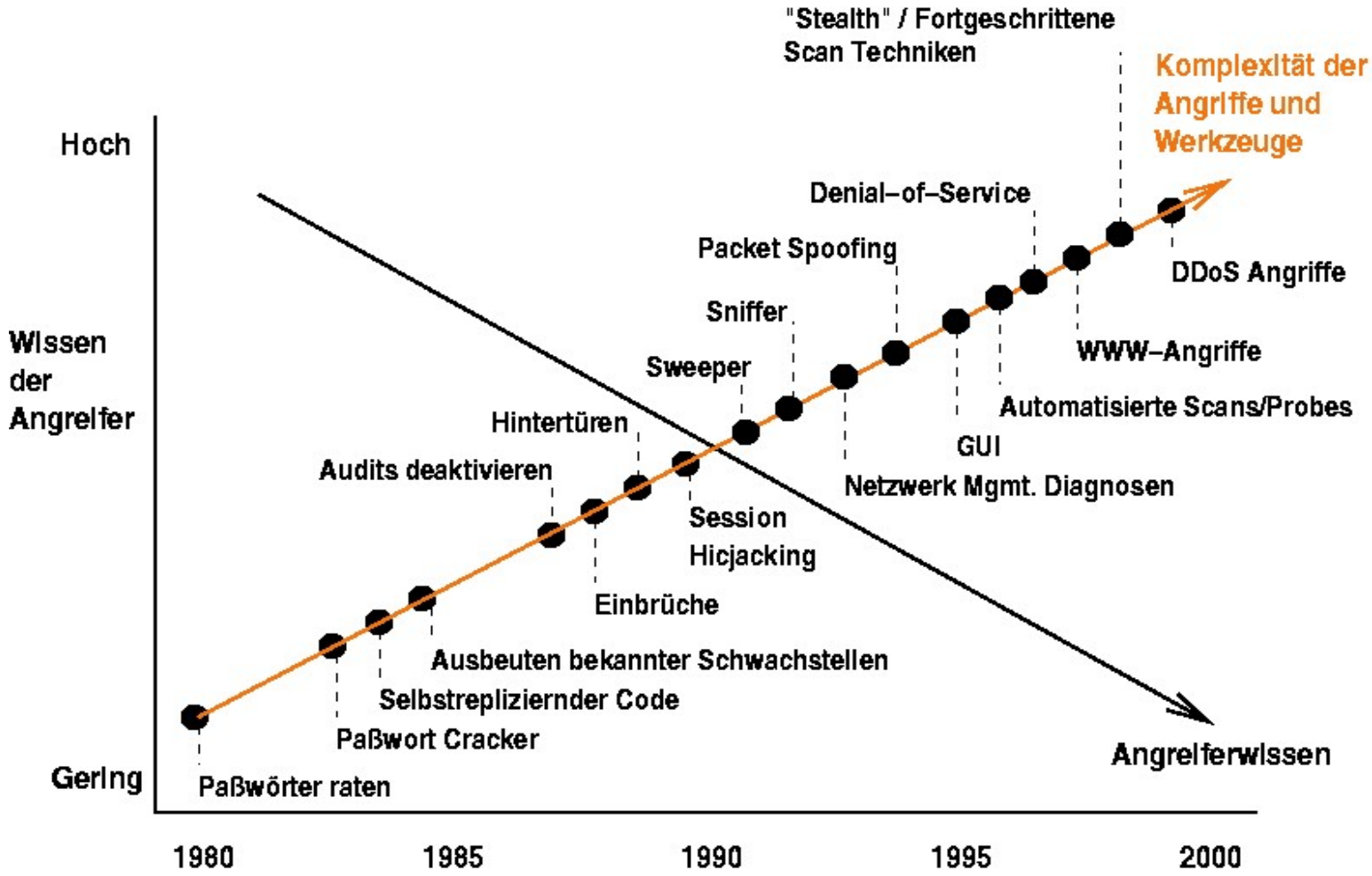
Typische Beispiele von Vorfallsmeldungen

- Einrichtung meldet kompromittierter Server mit sichergestelltem Material (Artefakte)
- Anderes CERT berichtet von einem kompromittierten System im Verantwortungsbereich
- Portscan-Meldungen (automatisiert und manuell)
- Viren- und Proxy-Meldungen (meist automatisiert)
- Anfragen von Strafverfolgungsbehörden
- Weniger: augenblicklich stattfindende Angriffe

DFN CERT

# Bedrohungslage und Trends

# Trends 1: Angreiferwissen

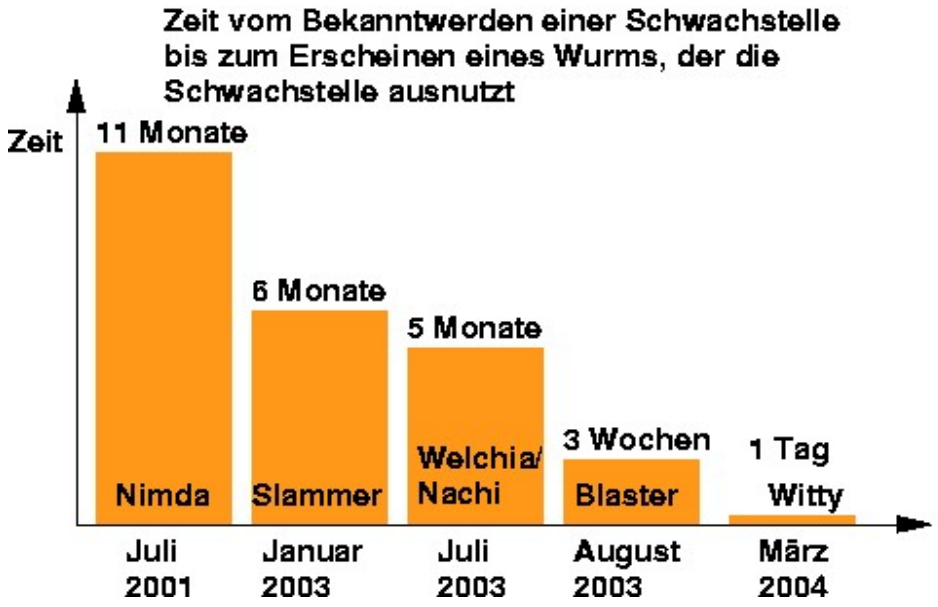


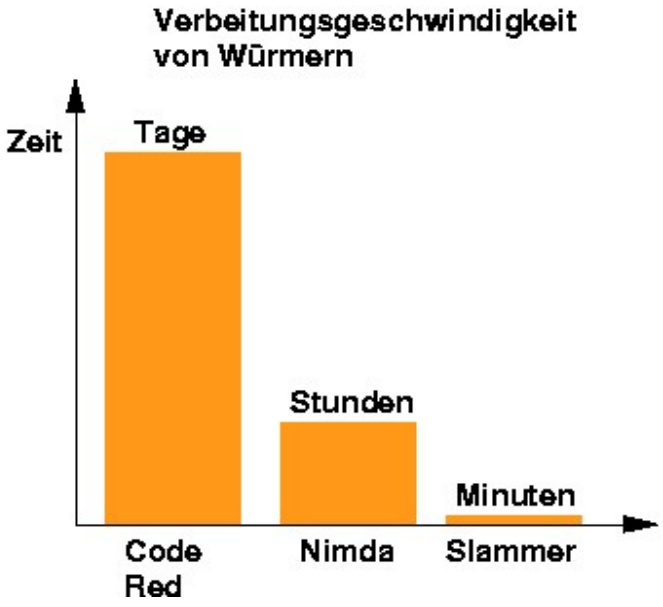

Original Copyright 2001 Carnegie Mellon University

# Trends 2: Zeitfenster

- Automatisierte Schwachstellensuche
- Automatisiere Exploit-Entwicklung
  - Open Source Werkzeuge: Metasploit, CANVAS, SPIKE

➔ Weniger Zeit für Systemverwalter



# Trends 3: Leistung gegen Geld

- Zusammenschluß verschiedener Gruppen
  - UNIX Cracker: Know-How über Netzwerke, Rootkits
  - Windows (Spiele) Cracker: Reverse Engineering
  - Spammer: Geld
  - Script-Kiddies: Zeit, kriminelle Energie, Bot-Armeen
- Entstehen einer Untergrund-Ökonomie
  - Malware-Entwicklung gegen Geld (Exploits, Features)
  - Spam Verteilung gegen Geld (via Botnet)
  - DDoS Angriffe gegen Geld (via Botnet)
- Einstieg der organisierten Kriminalität
  - 1. Halbjahr 2004: Schutzgelderpressung mittels DDoS gegen Online-Wettbüros

# Trends 4: Allzweck-Malware

- Beispiel heutiger Malware: PhatBot
  - Wurm und IRCBot in einem
    - Nutzt verschiedene Schwachstellen zur Verbreitung
    - Nimmt zur Steuerung Verbindung mit einem IRC-Server auf
    - Online-Update via P2P-Netzwerk (Gnutella)
  - Modularer Aufbau
    - Funktionen können leicht hinzugefügt werden
    - Hunderte von Varianten, kein AV-Scanner findet alle
  - Späht Daten aus: Lizenzschlüssel, Kreditkartennummern, Passworte, etc.
  - Weitere Features: DDoS Agent, FTP-Server, HTTP-Proxy, Sniffer, Spam-Agent, beendet AV-Programme, etc.
  - Weitere Informationen: http://www.lurhq.com/phatbot.html

DFN CERT

# Nur im Verbund sind CERTs stark!

# CERT im nationalen Verbund

## Nationaler CERT-Verbund (www.cert-verbund.de)

Allianz deutscher Sicherheits- / Computernotfallteams

CERT-BUND (BSI)
DFN-CERT
IBM BCRS
S-CERT (SIZ Sparkassen)
Siemens-CERT
Telekom-CERT
PRESECURE
RUS-CERT (Uni Stuttgart)
CERTBw (Bundeswehr)
COMCert (Commerzbank)
CERT-VW (Volkswagen)

## Nationale CERT AG

Informelle Arbeitsgruppe deutscher CERT

# ... in Europa und Global

## FIRST (www.first.org)

- Weltweiter Dachverband
- Zusammenarbeit auf technischer Ebene

## TERENA TF-CSIRT (www.terena.nl)

- Europaweite Arbeitsgruppe
- Zusammenarbeit auf technischer und konzeptioneller Ebene; Kontakte zur EU
- Trusted Introducer (TI, nächste Folie)
- IODEF (jetzt IETF Working Group)
- Erweiterung der RIPE-Datenbank: IRT Objekt
- CHIHT: Sammlung von Informationen zu Security Tools

# Akkreditierung für CERTs

Trusted Introducer TI (www.ti.terena.nl)

- Ziel: Objektive und aktuelle Informationen über Notfallteams
  - Ermöglicht es neuen (und etablierten) Teams, sich in einer Weise zu präsentieren, die anderen Teams das Auffinden der Informationen erleichtert.
- Unterstützung der Kommunikation und Erleichterung der Zusammenarbeit
- Überprüft durch das TI Review Board
  - verfügt über Sanktionsmöglichkeiten
- Akkreditierung, keine Zertifizierung

DFN CERT

# Neue Dienste und Möglichkeiten

# Woran arbeiten wir?

- Neighbourhood Watch
  - Sehr „harmloser“, aber effektiver Test aus dem Internet erreichbarer Systeme
  - Landkarte mit Systemen und Diensten
  - Monatliche Aktualisierung und Auswertung
- Aufbau von Sicherheitsorganisationen
  - Neuer Bedarf für Hilfe-zur-Selbsthilfe
  - Tutorien zunächst in Hamburg
- Frühwarnung
  - CERT-Verbund Projekt mit u. a. SIEMENS und Telekom
  - Zusammenführung von verfügbaren Daten über Angriffe, z. B. Darknets, Firewall-Logs, ...
  - Verteilte Analyse und Bewertung

DFN CERT

# Vielen Dank
# für Ihre Aufmerksamkeit!

# Kontakt

Dr. Klaus-Peter Kossakowski

WWW: https://www.dfn-cert.de
Email: kossakowski@dfn-cert.de
Mobil: (+49) 0171 / 5767010

Vorfälle: cert@dfn-cert.de
PKI: pca@dfn-cert.de