Computer Forensik in der Praxis

Heise CeBIT Forum 2006

Alexander Geschonneck

Leitender Sicherheitsberater
HiSolutions AG, Berlin

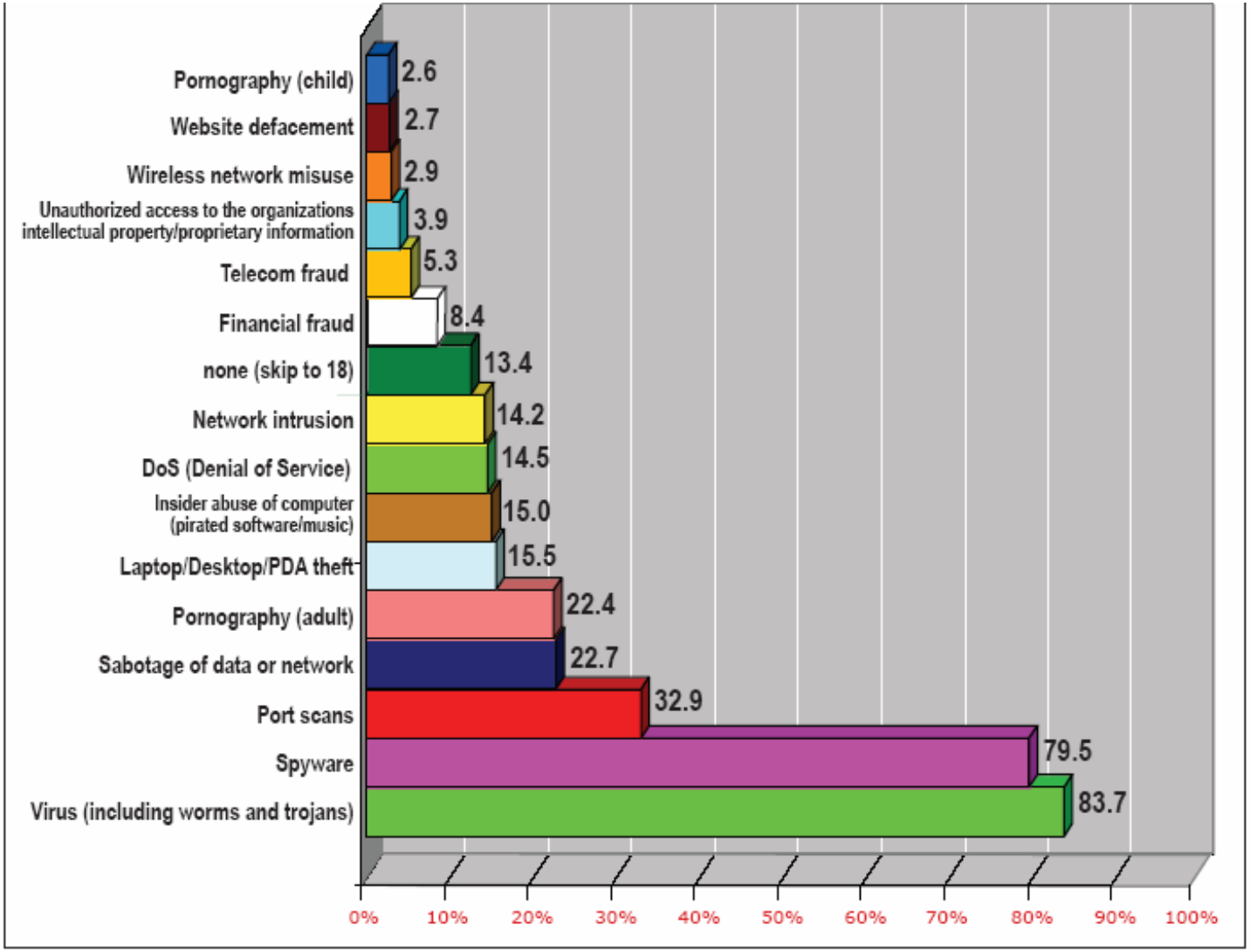
Visitenkarte HiSolutions AG

Gründung	1994
Vision	Der sichere und effiziente Umgang mit Informationen macht unsere Kunden erfolgreicher
Mission	Wir schützen und optimieren die Informationsverarbeitung unserer Kunden mit Organisations- und Technologiekompetenz
Felder	▪ IT-Service Management ▪ Information Security
Mitarbeiter	45
Firmensitz	Berlin
Awards	Innovationspreis Berlin/Brandenburg Fast50 Germany Fast500 Europe

Deloitte. 2004 Technology Fast 50 Deutschland

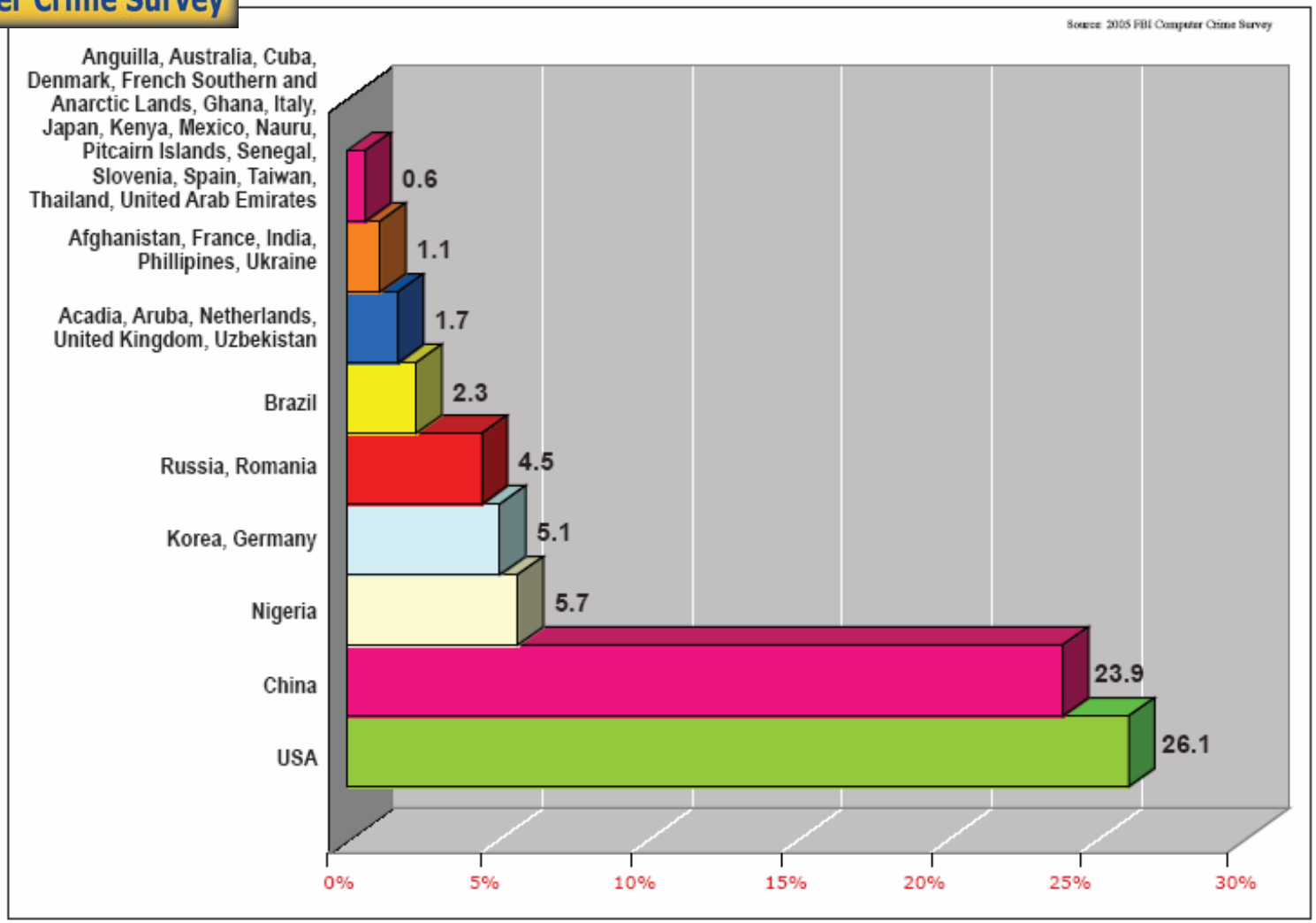
Deloitte. 2005 Technology Fast 50 Deutschland

2005 FBI Computer Crime Survey



Question 7: **Which types of computer security incidents has your organization detected within the last 12 months?** (select all that apply)

2005 FBI Computer Crime Survey



Question 12: What country was the most common source of the intrusion attempts against your organization?

Question 15: If your organization has experienced a computer security incident within the last 12 months, which actions did your organization take? (select all that apply)

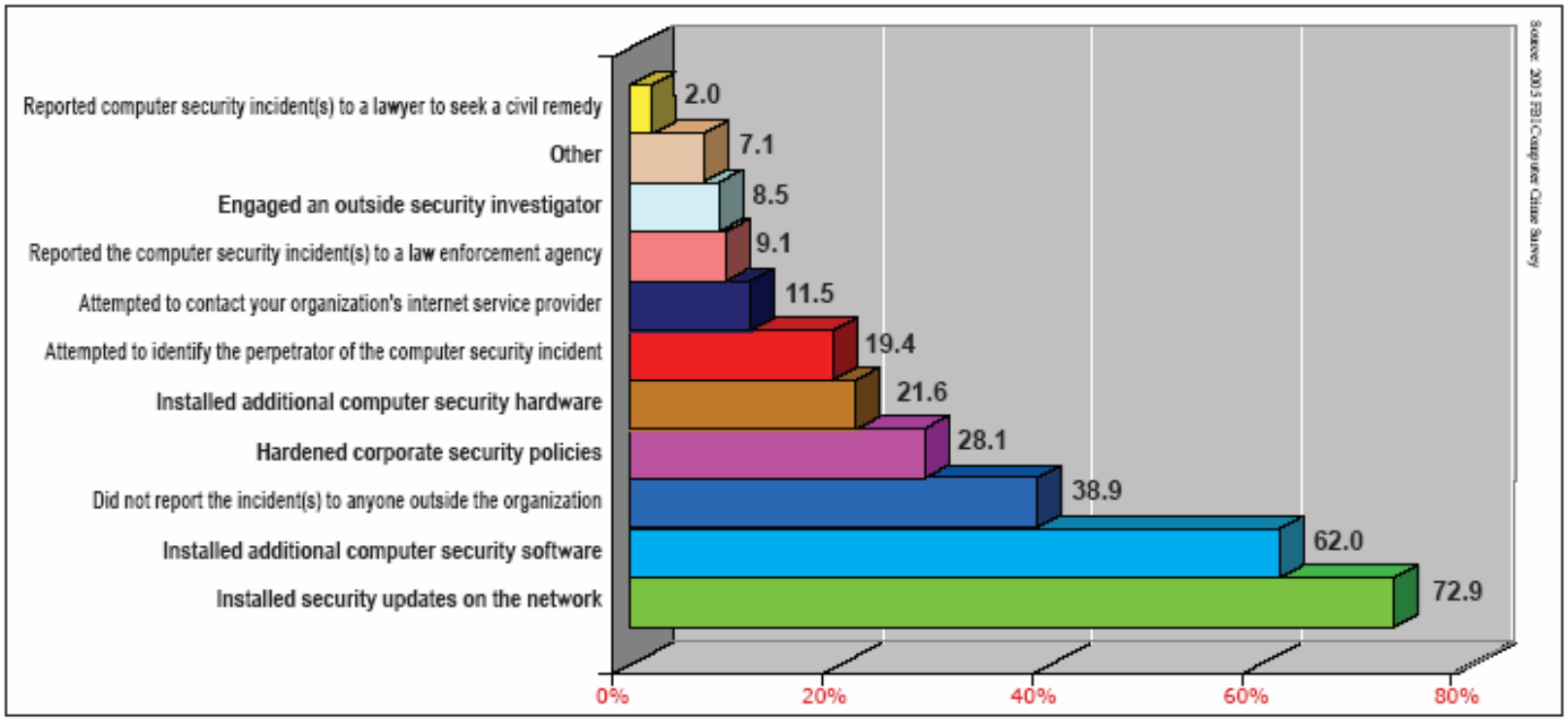
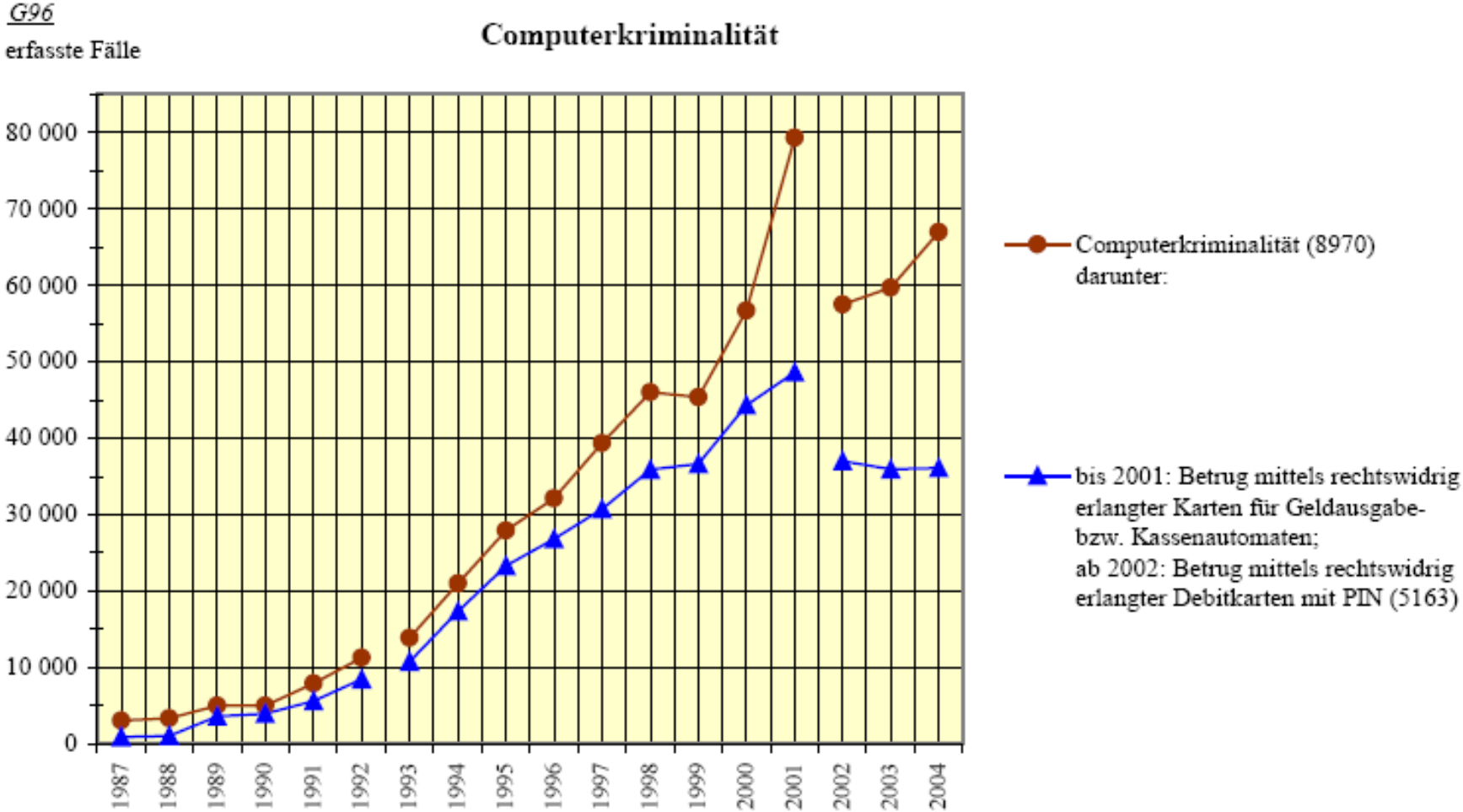


Abbildung 3: Verbreitung von Angriffsmethoden in deutschen und schweizerischen Unternehmen [8]

PKS 2005: Computerkriminalität

G96

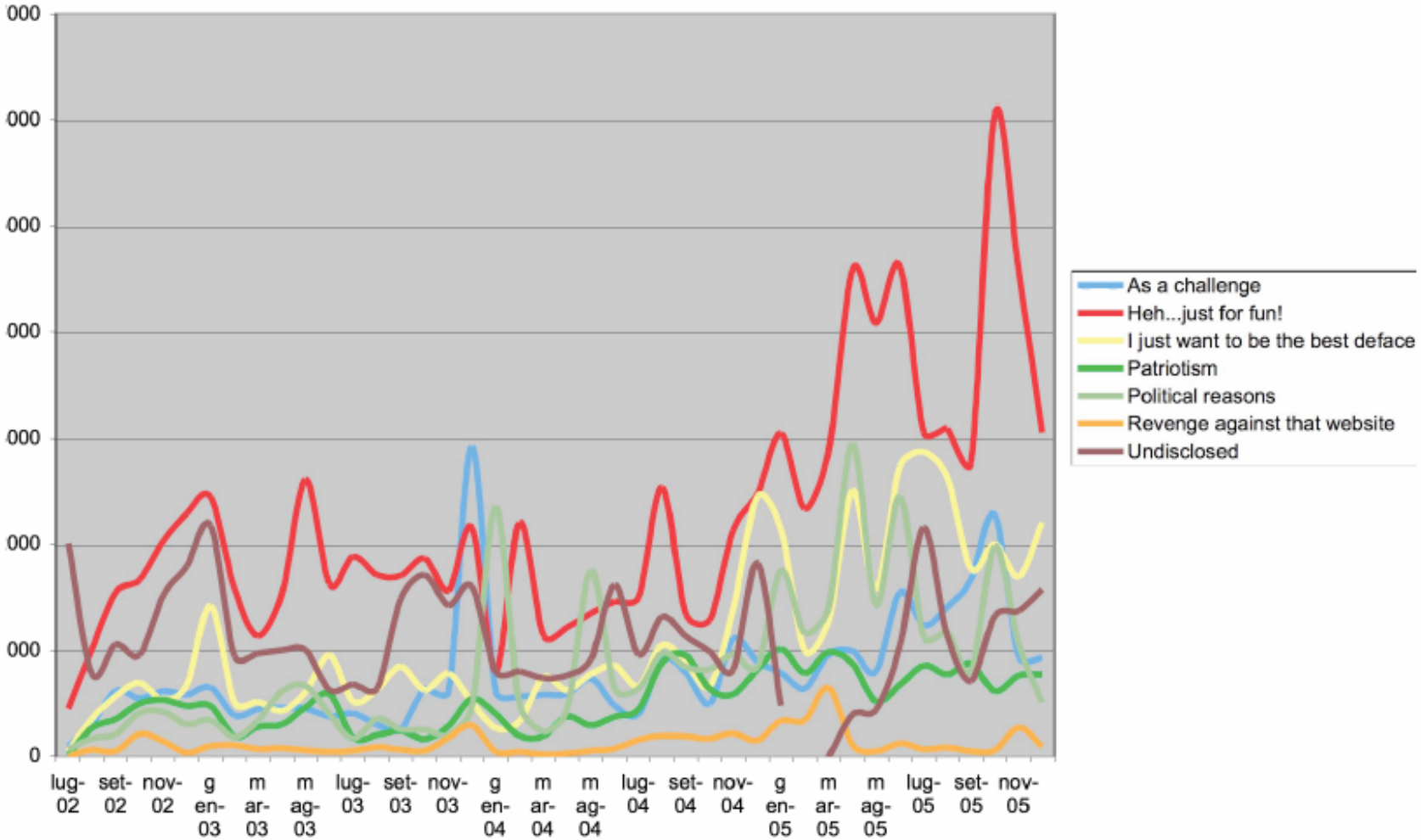


Hinweis:

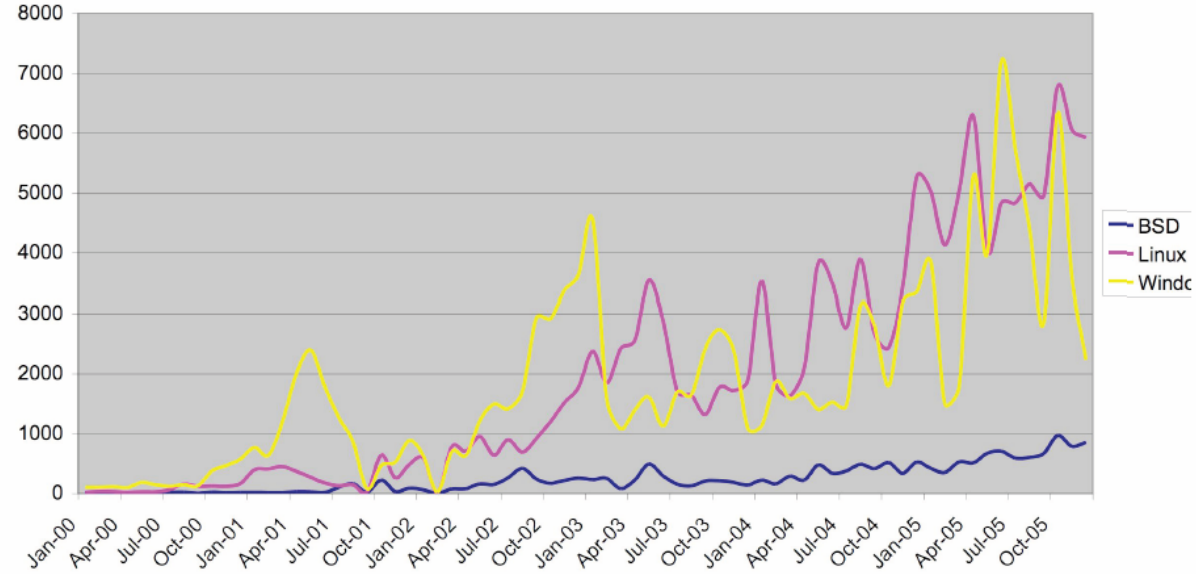
1987 – 1990:	alte Länder
1991 – 1992:	alte Länder mit Berlin
ab 1993:	Bundesgebiet insgesamt
1998:	Wegen zusätzlicher Aufnahme von Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (Schlüssel: 5179) ist ein Vergleich der Computerkriminalität (8970) zum Vorjahr beeinträchtigt.

Keine Aussagen zu kommerziellen Interessen

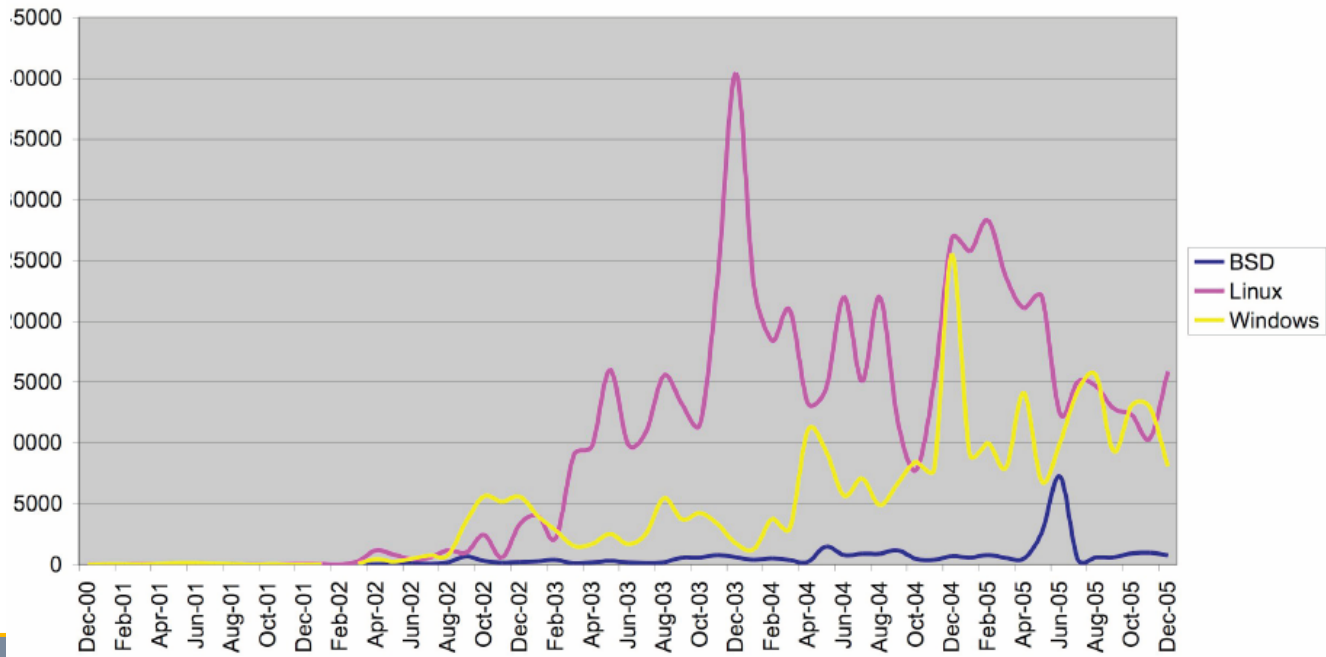
zone-h
unrestricted information



OS families single IP 2000-2005 by month



OS families mass 2000-2005 by month



Computer Forensik

Was ist Computer-Kriminalität

Im engeren Sinne:

- alle Delikte, bei denen der Computer Werkzeug oder Ziel der Tathandlung ist, wobei die Tat durch den Einsatz des Computers
  - ermöglicht oder
  - erleichtert oder
  - die Entdeckung erschwert wird

Im erweiterten Sinne:

- alle rechtswidrigen und sonst wie sozialschädlichen Verhaltensweisen die unter Einbeziehung von IT vorgenommen wurden

Was ist Computer Forensik?

- Computer-Forensik[1] (oder auch Digitale Forensik, IT-Forensik, IuK Forensik):
  - Nachweis und die Ermittlung von Straftaten im Bereich der Computerkriminalität
  - Nachweis und Aufklärung von strafbaren Handlungen z. B. durch Analyse von digitalen Spuren

- Kriminalistische Fragestellungen:
  - **Wer, Was, Wo, Wann, Womit, Wie und Weshalb**

- Ziel der Ermittlung
  - Erkennen der Methode oder der Schwachstelle, die zum Systemeinbruch geführt haben könnte,
  - Ermittlung des entstanden Schadens nach einem Systemeinbruch,
  - Identifikation des Angreifers,
  - Sicherung der Beweise für weitere juristische Aktionen.

[1] forensisch [lat. sinngemäß]: gerichtlich oder auch kriminaltechnisch; andere Beispiele: forensische Medizin; forensische Psychologie

Grundfragen zur Computer-Forensik

Es muss sichergestellt werden, dass soviel Informationen wie möglich von einem kompromittierten System gesammelt werden können, ohne dabei den aktuellen Zustand dieses Systems zu verändern.

- Wie wird der Angriff oder die Straftat verifiziert?
- Wie und wann muss der kompromittierte Rechner und die zugehörige Umgebung gesichert werden?
- Welche Methoden können für die Sammlung von Beweisen verwendet werden?
- Wo sucht man nach Anhaltspunkten und wie können Sie gefunden werden?
- Wie können Entscheidungsträger überzeugt werden?
- Wie kann das Unbekannte analysiert werden?

Worum geht es?

„Eisberg“ der Daten

Daten, die von normalen Tools gefunden werden
(Windows Explorer)

Zusätzliche Daten, die nur durch Spezialwerkzeuge gefunden werden können (gelöscht, umbenannt, versteckt, unvollständig, schwer aufzufinden)

©Darren Harlow, Computer Forensics 101

Welche Daten können gesammelt werden?

- Unabhängig von der konkreten Fragestellung und dem zu untersuchenden System (Server, Workstation, PDA, Router, Notebook etc.) lassen sich grundsätzlich einige empfindliche Datentypen, die für die Ermittlung von Interesse sind, finden:
  - Flüchtige Daten
    - Informationen, die beim geordneten Shutdown oder Ausschalten verloren gehen (Inhalt von Cache und Hauptspeicher, Status der Netzverbindungen, laufende Prozesse und deren Speicherbelegung, angemeldete User etc.)
  - Fragile Daten
    - Informationen, die zwar auf der Festplatte gespeichert sind, aber deren Zustand sich beim Zugriff ändern kann
  - Temporär zugängliche Daten
    - Informationen, die sich auf der Festplatte befinden, aber nur zu bestimmten Zeitpunkten zugänglich sind, z.B. während der Laufzeit einer Anwendung.
- Die Kenntnis um die Halbwertzeit dieser Daten ist sehr wichtig, da damit die Reihenfolge der Datensammlung bestimmt wird.

Sicherungsreihenfolge

- Die Halbwertzeit der Informationen bestimmt die Sicherungsreihenfolge

- Routingtabellen, ARP-Cache, Prozessliste, angemeldete User, Netzstatus, Kerneldaten, Hauptspeicherinhalt (durch Prozesse belegt)
- Temporäre Dateisysteme, SWAP-Bereiche, etc
- Der komplette Inhalt der Datenträger
- Relevante Logging und Monitoringdaten auf zentralen Loggingservern
- Physische Konfigurationen und Netzwerktopologien
- Archivierte Medien

Siehe auch RFC 3227 - Guidelines for Evidence Collection and Archiving

Grundsätzlich gilt: SAP-Modell

- **Secure** (Erfassung der Daten)
  - „Tatort“ und Untersuchungsbereich absichern
  - Beweisspuren sorgfältig sichern
  - Integrität der Daten bewahren bzw. nachweisen: Hashes, Vieraugenprinzip, Protokollierung
  - Rechtmäßigkeit beachten
- **Analyze** (Auswertung der Daten)
  - Spuren sorgfältig auswerten
  - Ergebnisse objektiv bewerten
  - Schlüsse kritisch hinterfragen
- **Present** (Präsentieren der Ergebnisse)
  - Detaillierungsgrad und Methoden sind abhängig von der Fragestellung
  - Erkenntnisse schlüssig und nachvollziehbar dokumentieren
  - Erkenntnisse überzeugend zielgruppenorientiert präsentieren

Beweisspurengruppen

- Während der Analysephase werden die vorher erfassten Daten untersucht, ob sich darin Beweisspuren oder Teile davon befinden.

- Es lassen sich grob drei Gruppen von Beweisspuren unterscheiden:

  - Beweisspuren, die eine bestimmte Theorie **untermauern**,

  - Beweisspuren, die **gegen** eine bestimmte Theorie sprechen und

  - Beweisspuren, die keine bestimmte Theorie unterstützen oder wiederlegen, sondern lediglich zeigen, dass das System **verändert** wurde, um (eventuell) Informationen oder Spuren zu verbergen.

Ist erfolgsentscheidend!

dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,
dokumentieren, dokumentieren, dokumentieren, dokumentieren, dokumentieren,

Ohne feste Meinung herangehen

- Es hat durchaus Vorteile, den »Tatort« des Geschehens aufzusuchen, ohne eine konkrete Vorstellung davon zu haben, was man dort genau finden wird.

- Diese Unvoreingenommenheit bei der Analyse eines Sicherheitsproblems sollte immer angestrebt werden.

- Die Antwort »derzeit unbekannt« hat in manchen Situationen durchaus ihre Berechtigung und kann gerade am Anfang einer Ermittlung den Blick für die nicht offensichtlichen Spuren freihalten.

- Antworten, die zu schnell und ohne sorgfältige Überprüfung gefunden werden, könnten den echten und wichtigeren Beweis eventuell »vergiften«.

- Es kommt auch immer wieder mal vor, dass ein Angreifer absichtlich falsche Spuren hinterlässt, um die Ermittler auf die falsche Fährte zu locken (auch Trugspuren genannt). Diese können z. B. aus falschen IP-Adressen oder Logfile-Einträgen bestehen.

Werkzeugkiste der Ermittler

- Tools zum Erstellen und Prüfen von Prüfsummen (mehrere Verfahren)
- Tools zur Sicherung von flüchtigen Daten zur Laufzeit
- Schlüsselwortsuchtools (auch fremde Zeichensätze) in logischen und physischen Strukturen von Datenträgerimages
- Tools zur Dateianalyse und –wiederherstellung anhand von Dateisignaturen
- Tools zum kompletten oder gefilterten Wiederherstellen von gelöschten Daten
- Tools zum Betrachten unterschiedlicher Dateiformate
- Tools zum Erstellen Timeline durch Auswertung der MAC-Times
- Tool zum Erstellen und Zusammenfassen aller Berichte mit bedarfsweisen Detailinformationen
- Hardware Writeblocker mit Adaptern für unterschiedliche Speichermedien
- Tool zum Löschen der verwendeten eigenen Speichermedien vor Aufnahme von Beweisspuren
- Verschlüsselungswerkzeuge zur Sicherung der Ermittlungsergebnisse

Die verwendeten Werkzeuge müssen beherrscht werden – vorher üben!

Fragestellungen für die Ermittlung

Fragestellungen für die Ermittlung

- Welche Kennung hatte (unberechtigten) Zugriff, Zugang bzw. Zutritt?
- Welche Personen(-gruppen) könnten diese Kennung nutzen?
- Was hat der Angreifer auf dem System gemacht?
- Zu welchem Zeitpunkt fand der Vorfall statt?
- Welche Systeme sind zusätzlich betroffen?
- Warum ist gerade dieses Netz oder System angegriffen worden?
- Wie konnte der Angreifer Zugriff erlangen?
- Ist der Angriff vor kurzem geschehen? Was macht der Angreifer jetzt?
- Was konnte der Angreifer auf diesem/von diesem System einsehen?
- Hat der Angreifer etwas zurückgelassen?

Weitere Fragestellungen für die Ermittlung

- Welche Tools kamen beim Angriff möglicherweise zum Einsatz?
  - Wie kamen diese Tools zum Einsatz?
  - In welcher Programmiersprache wurden die Tools geschrieben?
  - Haben diese Dateien Ähnlichkeiten mit Dateien, die auf dem System eines Tatverdächtigen gefunden wurden?
- Welche Ereignisse wurden protokolliert ?
- Was wird durch die Protokolldaten enthüllt?
  - Protokolldaten von Firewall, IDS, RAS, Zutrittskontrollsystemen
- Was ist auf den Datenträgern gespeichert?
  - Welche Spuren sind durch die verwendeten Applikationen hinterlassen worden?
  - Welche Dateien wurden gelöscht?
  - Existieren versteckte Dateien?
  - Existieren verschlüsselte Dateien oder -bereiche?
  - Existieren versteckte Partitionen?
  - Existieren Backdoors, Keylogger, Sniffer, Fernzugriffstools oder Rootkits?
  - […]

Analyseansätze

Unterschiedliche Analyseansätze

- **Live Response (Untersuchung am Live System)**
  = Notaufnahme

- **Post Mortem Analyse (Untersuchung einer Forensischen Kopie)**
  = Pathologie bzw. Gerichtsmedizin

Live Response vs. Post Mortem

- Live Response
  - Wenn,
    - wertvolle flüchtige Daten verloren gehen könnten,
    - das System nicht heruntergefahren werden kann, da es Business Critical ist,
    - Passwörter von evtl. verschlüsselten Dateisystemen nicht bekannt sind,
    - man herausfinden möchte, ob das System wirklich gehackt wurde.
  - Vorteile
    - Prozessspeicher kann gesichert werden,
    - Flüchtige Daten können gesichert werden,
    - Analyse der gerade auf dem System ablaufenden Ereignisse möglich.
  - Nachteile
    - Schwierigkeiten mit der richtigen Reihenfolge,
    - Flüchtige Daten könnten durch die Live Response verfälscht werden,
    - fragile Daten können zerstört werden,
    - unnötig, wenn der Vorfall länger zurück liegt.

Live Response vs. Post Mortem

- Post Mortem Analyse
  - Wenn,
    - der flüchtiger Speicher nicht relevant ist,
    - der aufzuklärende Vorfall länger zurück liegt,
    - das System mehrfach gebootet wurde,
    - der First Responder das Stromkabel bereits gezogen hat.
  - Vorteile
    - Flüchtige Daten können nicht aus Versehen zerstört werden,
    - Dadurch planbares Vorgehen.
  - Nachteile
    - Keine Informationen zur Laufzeitumgebung,
    - Wesentliche Spuren könnten verborgen bleiben.

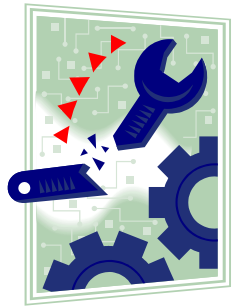
Forensische Duplikation als Basis der Post Mortem Analyse

- Findet in der „Secure“-Phase statt
- 1:1 Bit-Kopie eines sichergestellten Datenträgers
- Grundsätzlicher Ablauf
  - Hasherstellung der Quelle
  - Image Datei der Quelle erstellen (niemals auf die Quelle schreiben!)
  - Hasherstellung des Images
  - Hashvergleich: Image-Datei und Quelle → müssen im Idealfall übereinstimmen

- Varianten der Duplikation:
  - Ausbau der verdächtigen Festplatte aus dem verdächtigen System und Anschluss an das Analysesystem
  - Anschluss einer zusätzlichen leeren(!) Festplatte an das verdächtige System
  - Transport der kopierten Daten über ein geschütztes Netz vom verdächtigen System zum Analysesystem

Unbedingt Writeblocker für die verdächtigen Datenträger verwenden!

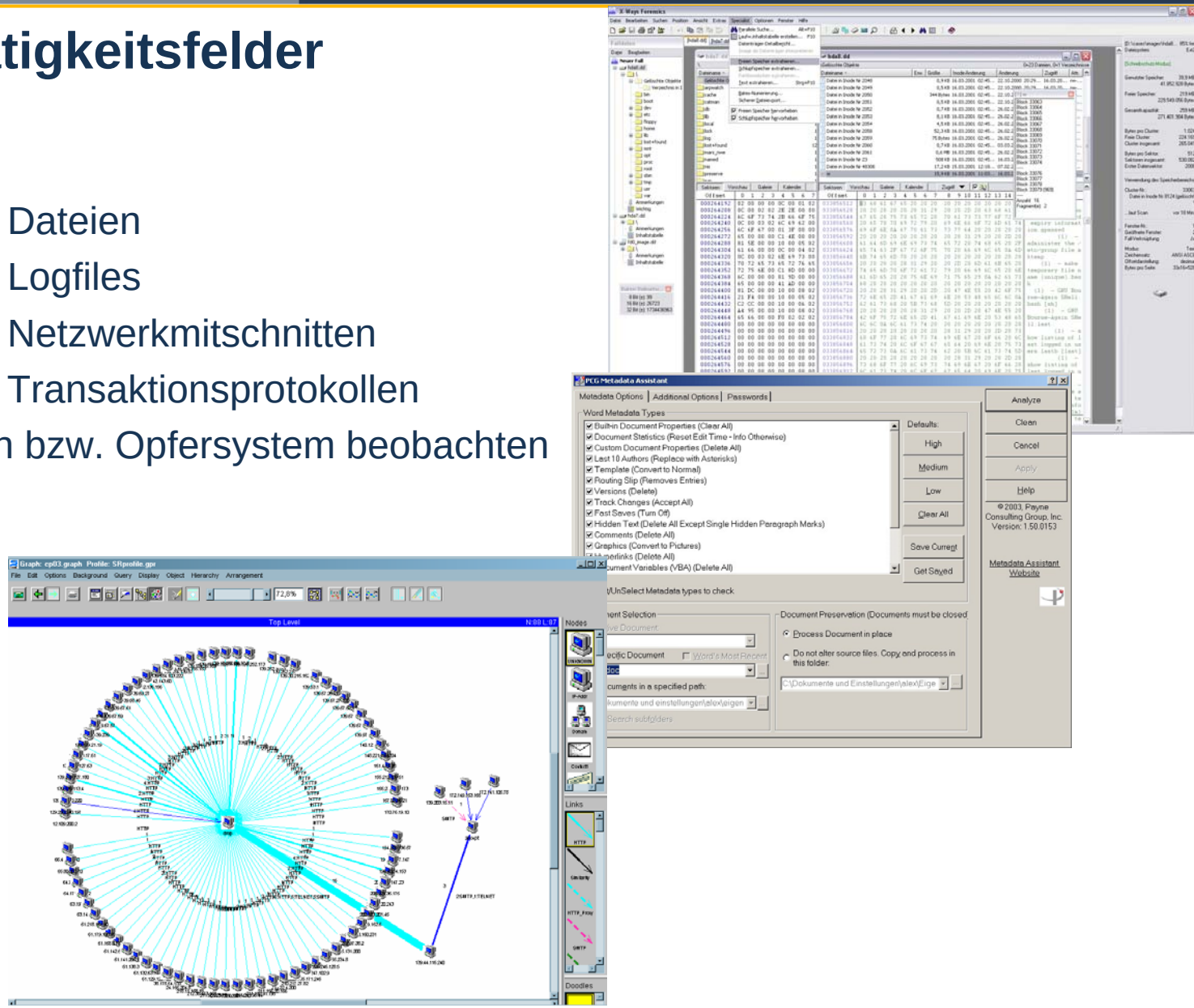
Forensische Duplikation: Toolauswahl



- Anforderungen an verwendete Imaging Tools
  - Die Übertragung der Daten muss bitweise erfolgen. Jedes Bit des Untersuchungsmediums muss übertragen werden.
  - Lesefehler müssen zuverlässig und robust behandelt werden. Nach mehrfachem Leseversuch muss der fehlerhafte Sektor markiert und mit Platzhalter versehen werden. Kein Abbruch
  - Es dürfen keine Änderungen am Originalmedium vorgenommen werden.
  - Die Anwendung muss nachvollziehbar arbeiten. Alle Aktionen müssen durch einen Dritten die gleichen Ergebnisse liefern.
  - Das erstellte Image muss durch kryptografische Verfahren (Checksummen oder Hash-Algorithmen) „geschützt“ werden können

Weitere Tätigkeitsfelder

- Analyse von Dateien
- Analyse von Logfiles
- Analyse von Netzwerkmitschnitten
- Analyse von Transaktionsprotokollen
- Verdächtigen bzw. Opfersystem beobachten
- …



Netzkabel ziehen?

- System Shutdown
  - Zerstört einige fragile Daten (SWAP, pagefile)
  - Sehr viele MAC-Timestamps werden zerstört
  - Logische Bomben könnten gestartet werden
  - **NACH MÖGLICHKEIT KEINEN NORMALEN SHUTDOWN DURCHFÜHREN**

- Stromkabel ziehen
  - Zerstört alle flüchtigen Daten in Hauptspeicher, Informationen über laufende Prozesse und angemeldete User → **vorher sichern**! → **Live Response**
  - Stoppt alle Prozesse sofort ohne dass logische Bomben gestartet werden können
  - **BEVORZUGTE METHODE**

Häufige Ermittlungsfehler

Fehler bei der Ermittlung

- Unkenntnis beim Tooleinsatz
- Betriebsblindheit
- Keine durchgängige Dokumentation der durchgeführten Aktionen
  - Jeder Vorgang am oder mit dem Beweis muss lückenlos dokumentiert sein
- Keine rechtzeitige Meldung über den Vorfall (Eskalation)
- Entscheidungsträger sind nicht oder nur unzureichend informiert
- Digitale Beweise sind unzureichend vor Veränderung geschützt
- Unterschätzen der Tragweite des Vorfalls
- Keinen Incident Response Plan in Vorbereitung

Eigentore, die nicht sein müssen

- Zeitverzögerungen durch organisatorische Mängel
- Verändern von Zeitstempeln auf den verdächtigen Systemen (MAC-Times) durch Zugriff
- Beenden eines verdächtigen Prozesses auf dem System
- Security Patch installieren, bevor das Response Team weitere Maßnahmen empfiehlt
- Kommandos ausführen, die niemand protokolliert hat
- Tools mit GUI lokal verwenden
- Nicht vertrauenswürdige Programme und Systemtools verwenden
- Zerstören von möglichen Beweisen durch Installieren oder Deinstallieren von Software
- Zerstören von möglichen Beweisen durch Programme, die Output auf der Beweisplatte generieren
- unter Umständen auch Shutdown

Das Verbrechen folgt den Möglichkeiten

- Erweiterte Angriffstools benötigen auch erweiterte Ermittlungsstrategien
- Angreifer können heutzutage zahlreiche Tools verwenden (einige normalerweise von jedem guten Sicherheitsberater empfohlen)
  - Wiping Tools / „Spurenvernichter“
  - Verschlüsselung
  - Date/Time Manipulation
  - Metadaten Manipulation
  - Backdoors, Keylogger, Sniffer etc. und Rootkits (um diese Tools zu verstecken)
  - sog. „Anti Forensics“ Tools

Probleme in der Computer Forensik

- Suche auf zugriffskontrollierten Systemen
- Unzureichende und fehlerhafte Werkzeuge
- formatierte, unlesbare oder zerstörte Datenträger
- Wiped oder degaussed Datenträger
- Cleaner & Cloaker
- Angriffstools im Kernelspace
- Vorschnelles Handeln bei den Administratoren
- Proprietäre Systeme ohne forensische Zugriffsmöglichkeiten

Trend: Hightech statt körperlicher Gewalt

- Auftragsviren und –würmer
- Schutzgelderpressung via Internet
- Botnets stundenweise mieten für eine Hand voll Dollars
- Aktienbetrug online „pump & dump“
- Dialerbetrug
- Gezieltes Phishing
- kein Interesse an Öffentlichkeit (zone-h.org, vuln-dev)

- **Cybermafia:** Das Gesicht des Internet-Verbrechens wandelt sich – weg vom isolierten, von seinem Schlafzimmer aus agierenden Computerfreak hin zu einer organisierten Cybermafia. Der Anteil von "einfacheren" Delikten wie „Hacking“ hat in den vergangenen zwei Jahren abgenommen.
- **IT-Söldnertum:** Das organisierte Verbrechen kauft IT-Fachwissen auf dem hierfür bestehenden Schwarzmarkt ein, um online klassische Verbrechen wie Diebstahl, Schutzgelderpressung und Betrug zu begehen und tauscht zunehmend die traditionellen Werkzeuge der Gewalt und Einschüchterung gegen die Hightechwaffen des 21. Jahrhunderts ein.

McAfee Studie „virtuelle Kriminalität“

Herausforderungen in der Computer Forensik

- Verschlüsselung vs. Datenauswertung
- Verlust der flüchtigen Daten nach einem Shutdown
- Umgang mit fremden Sprachen (und Zeichensätzen)
- Schwierigkeiten die Tragweite des Angriffs frühzeitig zu erkennen
- Schnelles Wiederherstellen der Services und Systeme vom Business Owner erwünscht
- Umfangreicher Einsatz von Personal und Technik (Plattenplatz!)
- Sicherer Umgang mit Beweismitteln
- Verhindern von weiteren Einbrüchen
- Kontrolle der Veröffentlichung von Informationen in der Öffentlichkeit

Kontakt

Anschrift

HiSolutions AG
Bouchéstraße 12
D-12435 Berlin

Fon: +49 30 533289-0
Fax: +49 30 533289-99
www.hisolutions.com

Information Security

Alexander Geschonneck
Leitender Sicherheitsberater
geschonneck@hisolutions.com

http://geschonneck.com
http://computer-forensik.org