Grundlagen der IT-Forensik

Eduard Blenkers
Senior Consultant

Omicron

Bitspill or Oilspill?

Exxon Valdez

- 1989 verunglückt
- Verlor 38.800 Tonnen Öl vor Alaska
- Kosten lt. Exxon: 2,1 Mrd US$ (54.000$ / Tonne)

Sea Empress

- 1996 verunglückt
- Verlor 72.000 Tonnen Öl vor Wales
- Kosten offiziell: 23 Mio GBP (400$ / Tonne)

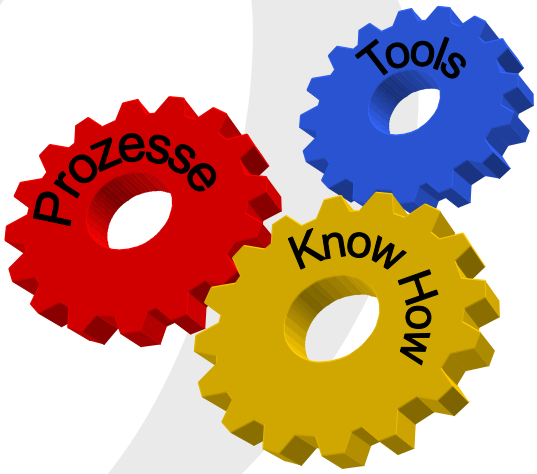
Omicron

Was jeder wissen muß

Omicron

Seite 3, Datum: 6.4.2005

Für Forensik braucht man



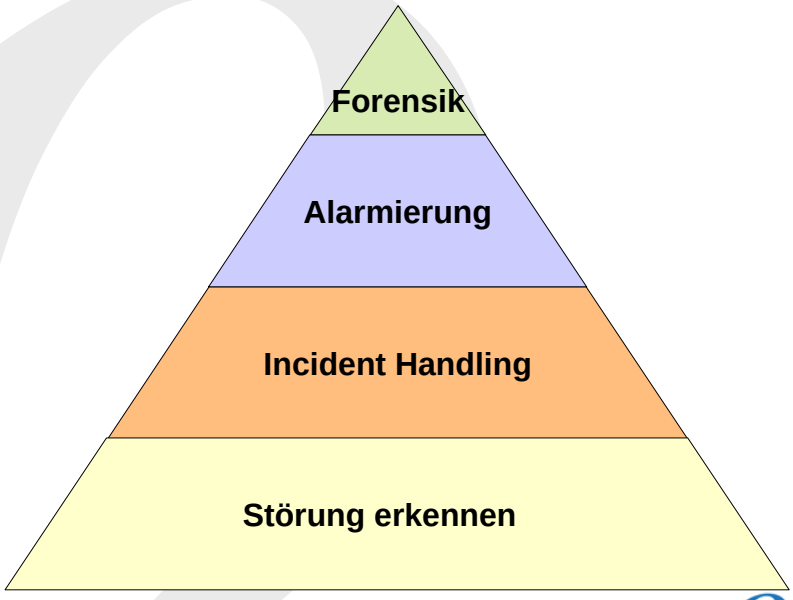
Omicron

Seite 4, Datum: 6.4.2005

Ziel der IT-Forensik

- Wer hat
- Was
- Wann
- Wo
- Wie
- Womit
- Weshalb gemacht?

Omicron



Omicron

Einsatzszenarien

- Vertrauliche Informationen landen beim Wettbewerber
- Rechtsstreit mit einem (ehemaligen) Angestellten
  - Fristlose Kündigung
  - Verdacht auf unbefugte Übermittlung von Daten
  - Zeitbomben in eigenen Programmen
- Zuviel privates Surfen im Internet
- Verdacht auf Hackerangriff

Omicron

Fallbeispiele

- Einbruch in einen Server
  - Webserver, Mailserver, Datenbank
- Insidertrading
- Private Nutzung von Firmenressourcen
  - Webshop im Firmennetz
  - Surfen
- Zurückverfolgen einer Mail zu einem PC
  - Beleidigung, Sexuelle Belästigung

Omicron

Fallunterscheidung

- Verbrechen am Computer
  - Z. B. Hackerangriff, DoS-Attacke
- Verbrechen mit dem Computer
  - Z. B. Ausspähen von Daten

Fallunterscheidung

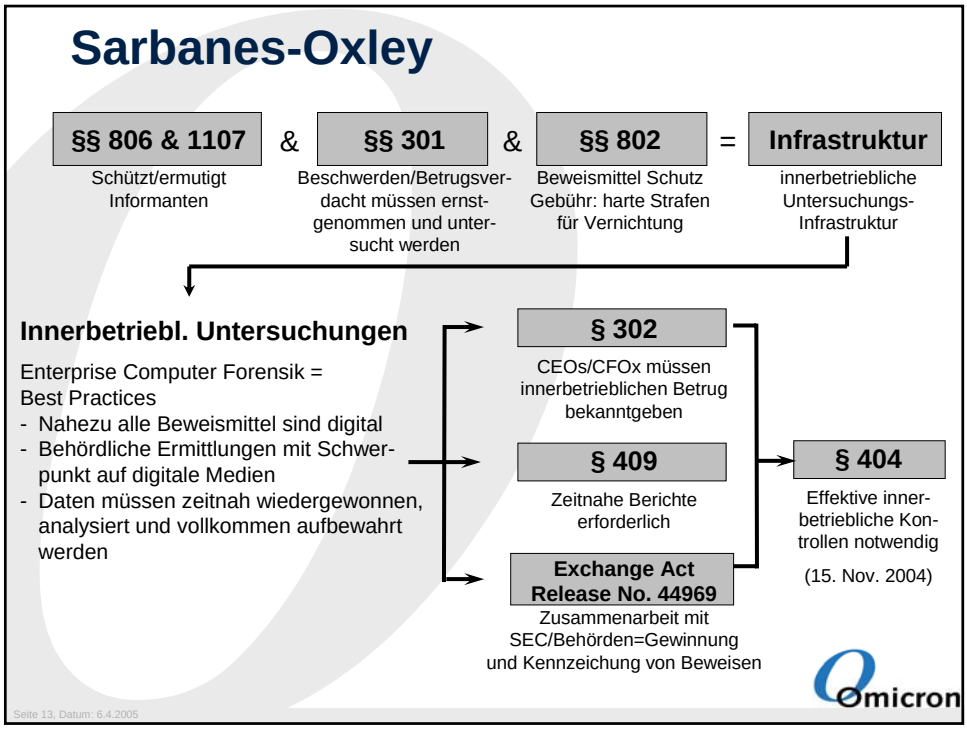
- Zivilrecht
  - Nachweispflicht des Klägers (z. B. als Arbeitgeber)
  - Beweise sammeln und gerichtsverwertbar aufbereiten
- Strafrecht
  - Anfangsverdacht erkennen
  - Untersuchung erfolgt durch Ermittlungsbehörden

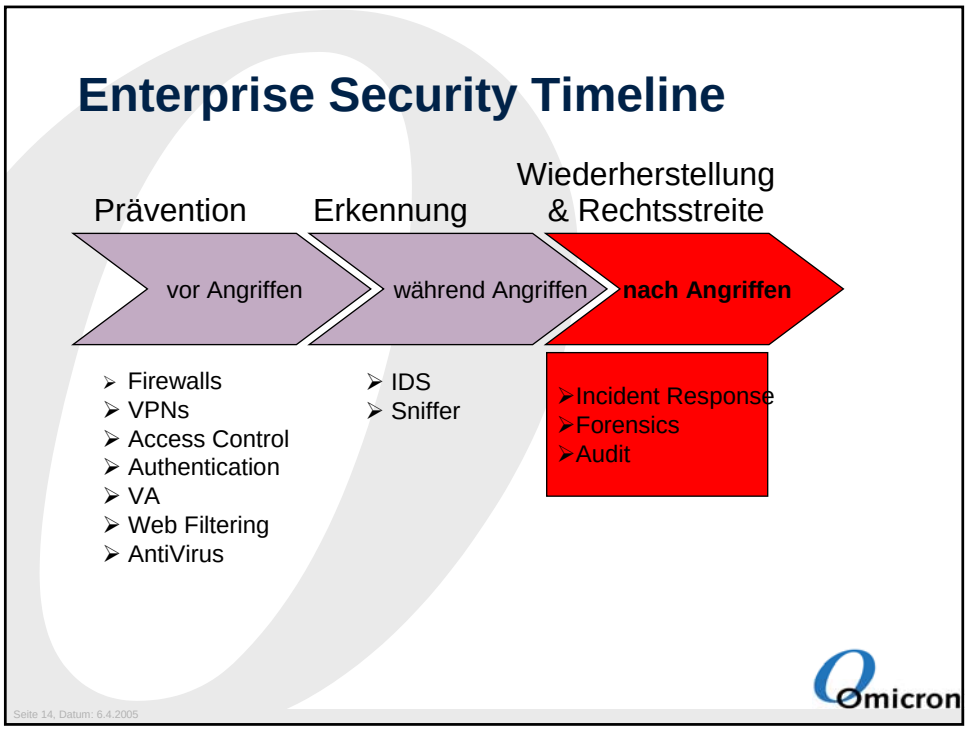
Vorher festlegen

- Wem gehören die Informationen auf einem Computer?
  - Policy definieren
  - Mitarbeiter daran erinnern über Banner oder Unterschrift

Motivation für IT-Forensik

- Sarbanes Oxley
  - Betrug in Unternehmen
- HIPAA
  - Umgang mit Daten aus dem Gesundheitswesen
- ISO 17799
  - Prozesse für Incident Response und interne Untersuchungen
- Basel II
  - Fordert angemessene Prozesse für Incident Response und
  - Prozesse zum Sammeln und Aufbewahren von forensischen Beweisen
- World Bank
  - „Best Practices“ verlangen Incident Response Prozesse


Sarbanes-Oxley
§§ 806 & 1107
Schützt/ermutigt Informanten
&
§§ 301
Beschwerden/Betrugsverdacht müssen ernstgenommen und untersucht werden
&
§§ 802
Beweismittel Schutz Gebühr: harte Strafen für Vernichtung
=
Infrastruktur
innerbetriebliche Untersuchungs-Infrastruktur
Innerbetriebl. Untersuchungen
Enterprise Computer Forensik = Best Practices
- Nahezu alle Beweismittel sind digital
- Behördliche Ermittlungen mit Schwerpunkt auf digitale Medien
- Daten müssen zeitnah wiedergewonnen, analysiert und vollkommen aufbewahrt werden
§ 302
CEOs/CFOx müssen innerbetrieblichen Betrug bekanntgeben
§ 409
Zeitnahe Berichte erforderlich
Exchange Act Release No. 44969
Zusammenarbeit mit SEC/Behörden=Gewinnung und Kennzeichnung von Beweisen
§ 404
Effektive innerbetriebliche Kontrollen notwendig
(15. Nov. 2004)
Omicron
Seite 13, Datum: 6.4.2005


Enterprise Security Timeline
Prävention
Erkennung
Wiederherstellung & Rechtsstreite
vor Angriffen
während Angriffen
nach Angriffen
Firewalls
VPNs
Access Control
Authentication
VA
Web Filtering
AntiVirus
IDS
Sniffer
Incident Response
Forensics
Audit
Omicron
Seite 14, Datum: 6.4.2005

Begriffsklärung

- **Incident Response**
  - Zeitkritische Untersuchungen nach einem Netzangriff
  - Überprüfung von Live-Systemen
  - Reihenfolge des Angriffs und betroffene Systeme ermitteln
- **Forensik:**
  - Gründliche Untersuchung eines Servers/PC‘s
  - Betrachtung gelöschter und versteckter Informationen, Dateien, Partitionen und teilweise überschriebenem Materials
  - Reihenfolge des Geschehenen feststellen
  - Vorbereitung auf Gerichtsverfahren
- **Audit:**
  - Untersuchung einer großen Anzahl von Computern
  - Ziel: Datenmissbrauch aufzudecken und zu beheben.

Omicron

Seite 15, Datum: 6.4.2005

Forensische Analyse

Omicron

Seite 16, Datum: 6.4.2005

Wer analysiert?

- Möglichst im Team
  - Mindestens ein Techniker
  - Mindestens ein Zeuge / Protokollführer
  - Juristischer Beistand auf Abruf
  - Evtl. Personalabteilung oder Betriebsrat
- Fremdmitarbeiter durch Geschäftsführung autorisieren lassen

Omicron

Seite 17, Datum: 6.4.2005

Wer analysiert ***nicht?***

Verdächtige Personen bedienen keine Computer

Omicron

Seite 18, Datum: 6.4.2005

Ist Forensik erlaubt?

- Einsatz forensischer Methoden innerhalb des Unternehmens geklärt?
- Benutzersicht:
  - „Eingriff in Privatsphäre“
  - „Überwachungsintrument“
  - Vergleich mit Telefon-Überwachung
- **Unschuld Beweisen**

Omicron

Seite 19, Datum: 6.4.2005

Forensik kostet Zeit

- Längere Ausfallzeit nach einem Hacker-Einbruch
- Besser keine Forensik als halbherzige Forensik
  - Management-Unterstützung notwendig

Omicron

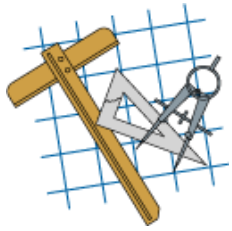
Seite 20, Datum: 6.4.2005

Forensik und Öffentlichkeitsarbeit

- Evtl. spätere Aufarbeitung vor Gericht
  - Bereitschaft zur öffentlichen Verhandlung?
- Presseerklärung vorbereiten

Omicron

Forensik als Prozess



Sammeln, Untersuchen, Analysieren, Berichten

Omicron

Sammeln

Suchen nach und Erkennen von wichtigen Beweismitteln

- Hardware
- Software
- Datenträger
- Dokumentation
- Ausdrucke, Handschriftliche Notizen
- Inhalt des Mülleimers
- …..

Omicron

Untersuchen

- Beweise sichtbar machen
  - Nicht der Datenträger ist der Beweis, sondern die gespeicherte Datei
- Identifizieren relevanter Informationen
  - Spreu vom Weizen trennen
  - Nach den niedrig hängenden Früchten greifen
- Aufgabe des Kriminaltechnikers
  - Technischer Vorgang

Omicron

Analysieren

- Verwertet das Ergebnis der Untersuchung
- Be- und Verwerten der gefunden Informationen
- Aufgabe des Ermittlers

Berichten

- Abschluß der forensischen Untersuchung
- Ergebnis muß jederzeit nachvollziehbar sein
  - Qualitativ
  - Prozedural
- KISS -> Keep It Simple, Stupid
  - Berichte sind für Manager, Revisoren, Juristen …

Und das wichtigste:

- Don‘t Panic!

Tätigkeiten vor Ort

Merke:

Erste Tätigkeit:
Die Kontrolle übernehmen

Omicron

Seite 29, Datum: 6.4.2005

Grundsätzliche Regeln

- Jede Aktivität dokumentieren
- Grundsätzlich nur mit einer Kopie arbeiten
- Keine Programme auf verdächtigen Computern starten
- Beweismittel nicht verändern

Omicron

Seite 30, Datum: 6.4.2005

Grundsätzliche Regeln

- Unbeteiligte Personen vom Tatort fernhalten
  - Nur das Incident Response Team ist vor Ort
- Verdächtige Personen nicht am Rechner hantieren lassen
  - Vorsicht vor Mittätern, die „helfen“ wollen und dann Spuren vernichten
- Tatort verwanzt?
  - Mikrofon / Lautsprecher am Computer
  - Handy unter dem Tisch?
  - ...

Omicron

Seite 31, Datum: 6.4.2005

Dokumentation des Tatorts

- Computer
  - Von allen Seiten
  - Anschlüsse
  - Vor dem Transport ins Labor: Kabel und Anschlüsse beschriften
- Umgebung / Arbeitsplatz
  - Vor allem bei Workstations
- Praktisch: Digitalkamera
  - Datum einblenden
- Skizzen anfertigen

Omicron

Seite 32, Datum: 6.4.2005

Dokumentation des Transports

- Beweiszettel für alle gefundenen Gegenstände
  - Transport
  - Lagerung
  - Zugriff

Computer eingeschaltet?

Merke:

Ausgeschaltete Computer bleiben ausgeschaltet

Omicron

Seite 35, Datum: 6.4.2005

Laufender Computer

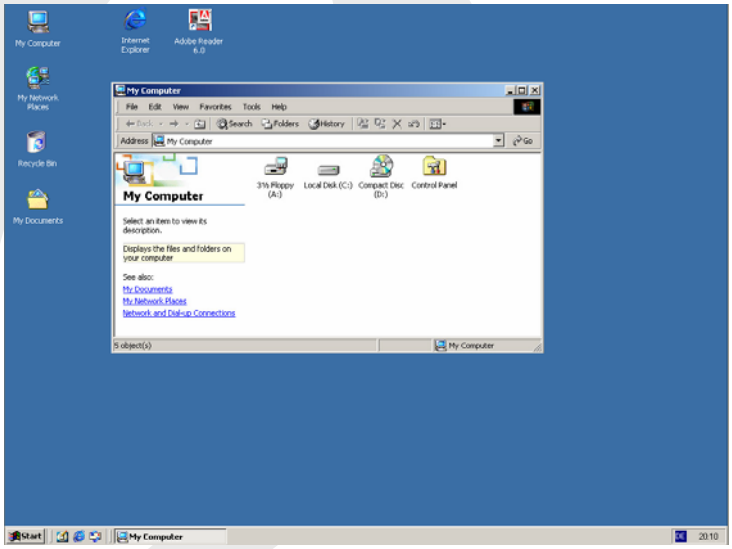
„Gretchenfragen:“

- Netzwerk:
  - Online lassen oder vom Netz nehmen?
- Betriebssystem:
  - Shutdown oder Power off?

Omicron

Seite 36, Datum: 6.4.2005

Der Bildschirm am Tatort



Omicron

Windows Crash erzwingen

- HKLM\SYSTEM\CurrentControlSet\Services i8042prt\Parameters
  - CrashOnCtrlScroll, Type DWORD, Wert 1
- Crashdump erzwingen:
  - Rechte Control-Taste gedrückt halten
  - Scroll-Lock 2 mal drücken

Omicron

Umgebung betrachten

- PDAs
- Mobiltelefon
- Mülleimer
- Logfiles Telefonanlage, Fax-Gerät
- ...

Datenträgeranalyse

Slackspace
Bitstream-Copy

Merke:

Analyse nur mit der Kopie

Omicron

Seite 41, Datum: 6.4.2005

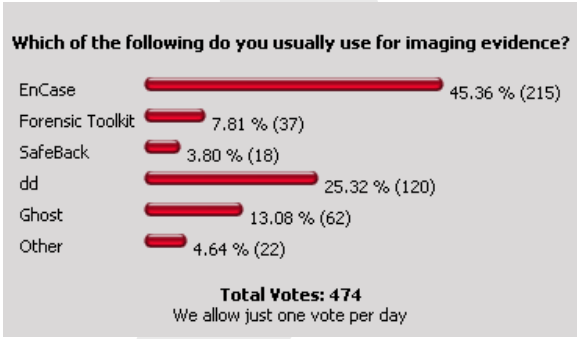
Kopieren von Datenträgern

- Physikalische Kopie des Datenträgers
  - "1:1-Kopie", "Bit-Stream-Copy", "Physical-Backup"
- Die Originalplatte nicht beschreibben
  - Jumper am Laufwerk (selten)
  - Mount-Befehl
  - Spezial-Kabel verwenden

Omicron

Seite 42, Datum: 6.4.2005

Verwendete Software



Quelle: www.forensicfocus.com

Hardware-Schreibschutz

- Drive-Lock von ICS
  - IDE-Kabel
  - Enthält kleinen Puffer
- FireFly von Digital Intelligence
  - Anschluß einer IDE-Platte am Firewire-Bus
  - Wahlweise mit oder ohne Schreibschutz
- SCSI ???

Fallstricke bei Bitstream-Copy

- Defekte Sektoren
  - Im Protokoll beschrieben?
  - Behandlung defekter Sektoren beim Restore?
- Data-Hiding über Bad-Block-Tabelle
  - Bad-Block in FAT manuell gesetzt
  - Bad-Sektor Markierung im Sektor-Header gesetzt
- Adressierung von Sektoren außerhalb des Drivespaces?

Omicron

Seite 45, Datum: 6.4.2005

Festplatten durchsuchen

Slackspace
ADS
Registry Hives

Omicron

Seite 46, Datum: 6.4.2005

Slackspace

- Plattenspeicher ist belegt, aber nicht genutzt
  `echo „hallo“ > file.txt`
- Genutzt: 5 Bytes
- Belegt: 1 Cluster (z. B. 2 kByte)
- Unterscheidung
  - RAM-Slack
  - Drive-Slack

Omicron

Seite 47, Datum: 6.4.2005

$LogFile

- Enthält Redo bzw. Undo-Logs
- Update Sequence Number (USN)
- Werkzeug: fsutil

Omicron

Seite 48, Datum: 6.4.2005

Alternate Datastreams

- ADS im Einsatz: (nur NTFS-Partition)
  - `echo hello > test.txt:mystream`
  - `dir test.txt` => Filesize 0 Byte
  - `more < test.txt:mystream`
- Eingeführt zur Kompatibilität mit Macintosh-Rechnern
- Suchen mit diversen Tools wie
  - sfind von foundstone.com
  - streams von sysinternals

Omicron

Seite 49, Datum: 6.4.2005

Dateien kopieren

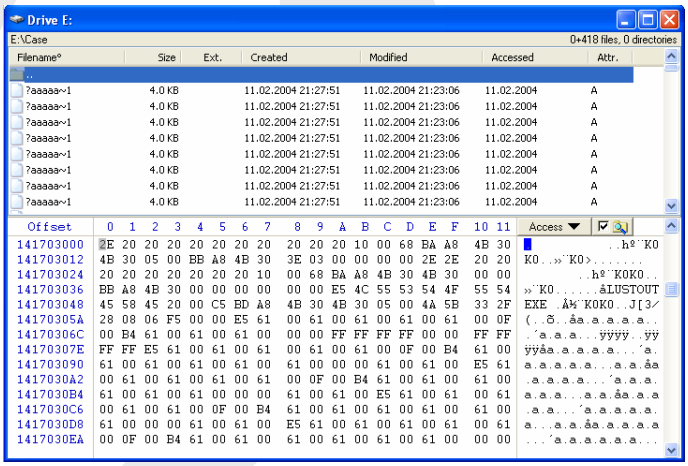
```
copy file1.gif+file2.gif file3.gif
```

- Ergebnis: File2.gif ist vor einigen Bildbetrachtern versteckt
- Rekonstruktion z. B. über gextract.exe von NTi

Omicron

Seite 50, Datum: 6.4.2005

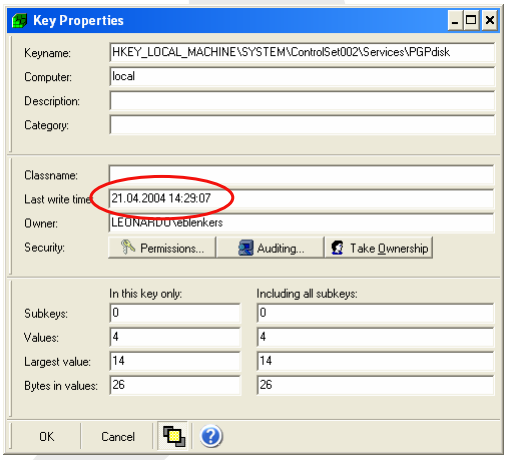
Wipe-Funktion von PGP



Datenvernichtung mit Steganos

- Überschreibt Dateiinhalt mit Zufallswerten
- Tauscht Dateinamen aus
- Kleine Dateien werden **nicht** aus der MFT gelöscht

Resplendent Registrar



Windows-Analyse Online

„Für Forensik braucht man eine Leiche.
Online-Analyse gibt es nicht.“

Special Agent Joe Enders,
Secret Service

Merke:

Online-Monitore lassen sich täuschen

Omicron

Seite 55, Datum: 6.4.2005

Analyse laufender Computer

- Eigene Programme mitbringen
  - "Known good copy", von CD starten
  - Mit Protokoll vom Virenscanner auf CD brennen
- Vorsicht vor präpariertem Computer: "Selbstzerstörungsmechanismus"
- Einmalige Chancen:
  - Verschlüsselte Dateisysteme noch gemountet
  - Laufende Prozesse

Omicron

Seite 56, Datum: 6.4.2005

Analyse laufender Computer

- Aktive Datenträger / Partitionen
  - Verschlüsselte Partitionen
- Laufende Prozesse
- Geöffnete Dateien
- Aktive Netzverbindungen
- Routing-Tabellen
- ARP-Cache
- DNS-Cache
- …

Analyse laufender Computer

Vorsicht:

- Trojanische Pferde verstecken
  - Dateien
  - Prozesse
- Besonders schwierig: LKM-Rootkits

Merke:

Manipulation der Beweismittel gefährdet den Wert vor Gericht

Omicron

Seite 59, Datum: 6.4.2005

Wichtige Utilities

- Online Monitore von
  - Foundstone.com
  - Sysinternals.com
- Zugriffe auf
  - Netzwerk
  - Registry
  - Platten bzw. Dateien
  - Serielle oder Parallel-Ports
  - ...

Omicron

Seite 60, Datum: 6.4.2005

Promiscous Mode entdecken

- Promiscdetect von Arne Vidström
  - Lokale Kontrolle der Netzwerk-Karte
  - www.ntsecurity.nu
- Promiscan
  - Scan von aussen mit speziell formatierten Paketen
  - www.securityfriday.com

Tools für Undelete

- WinHex
- PC Inspector
- Ontrack Easy Recovery

Guidance SOFTWARE

The Leader in Computer Forensics and Incident Response Solutions

Incident Response und Computer Forensics: Die letzten Grenzen für Informationssicherheit

22. April 2004

Decus Symposium, Bonn

EnCase: Das Tool für Profis

Einzelplatzversion:

- Untersuchung eines Computers
- Rekonstruktion von Dateien
- Zugriffsverlauf
- Data Hiding

Omicron

Seite 64, Datum: 6.4.2005

EnCase Enterprise

- Analysiert Server über das Netzwerk
- Besteht aus
  - SAFE Server
  - Servlets
  - Examiner
  - SnapShot Connection
  - Concurrent Connection

Seite 65, Datum: 6.4.2005

Fragen?

Omicron Deutschland
Herderstr. 26
40721 Hilden
02103 / 28 79-00
www.omicron.ch

Seite 66, Datum: 6.4.2005