Aspekte der Online-Durchsuchung aus Sicht eines Forensikers

a-i3 Tagung

9. Oktober 2007 Ruhr-Universität Bochum

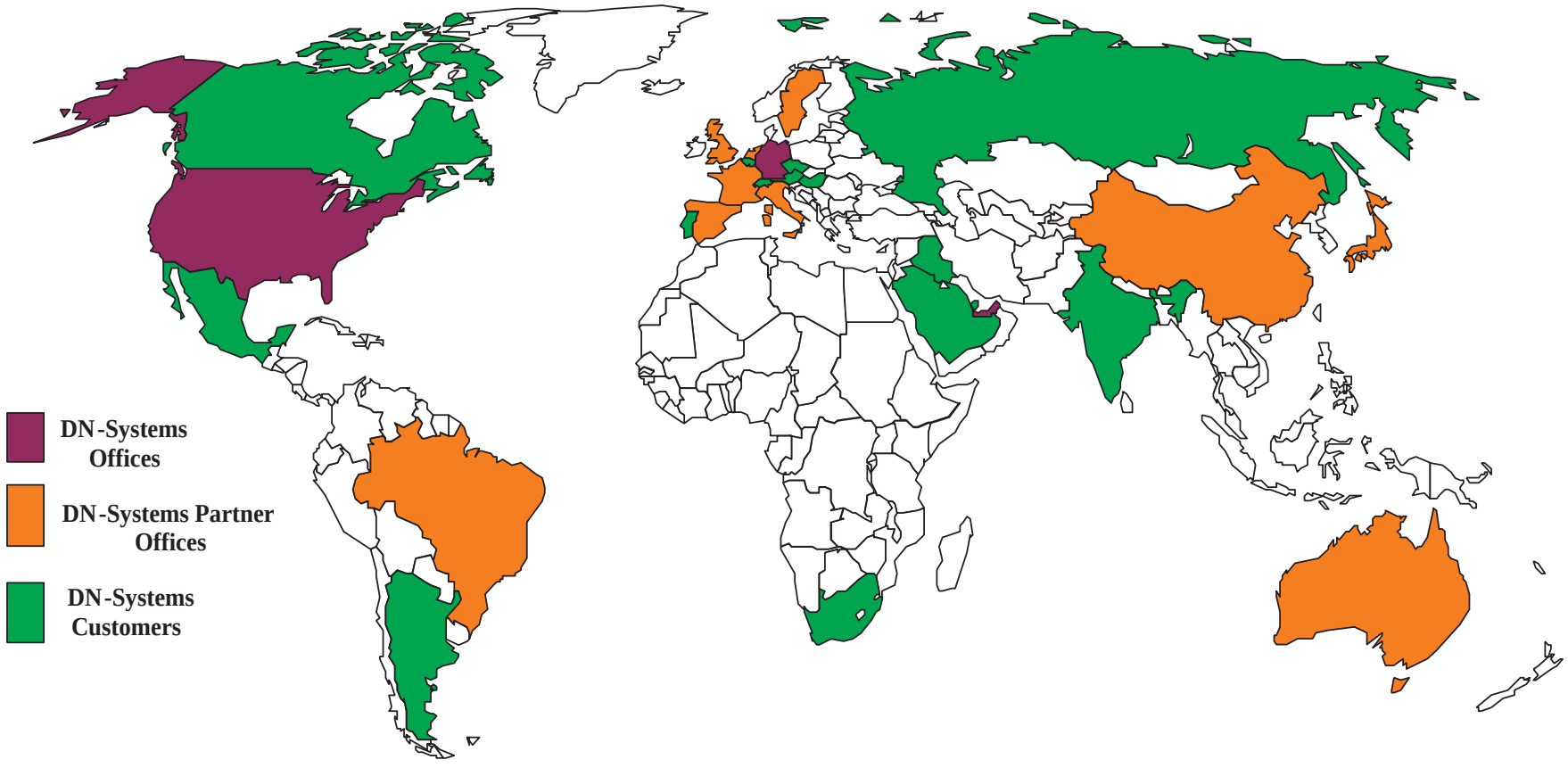
Lukas Grunwald

DN-Systems GmbH - Hildesheim - San Francisco - Dubai

DN-Systems

- digitale Forensik
  - präventiv
  - investigativ
  - Organisation
- Security
  - Integrale Sicherheit
  - Labor (Forschung)
  - Organisation / Umsetzung
  - Design / Integration
  - IT-Security
    - Firewall, IDS, IPS, VPN, Content-Security, RFID

DN-Systems - global tätig



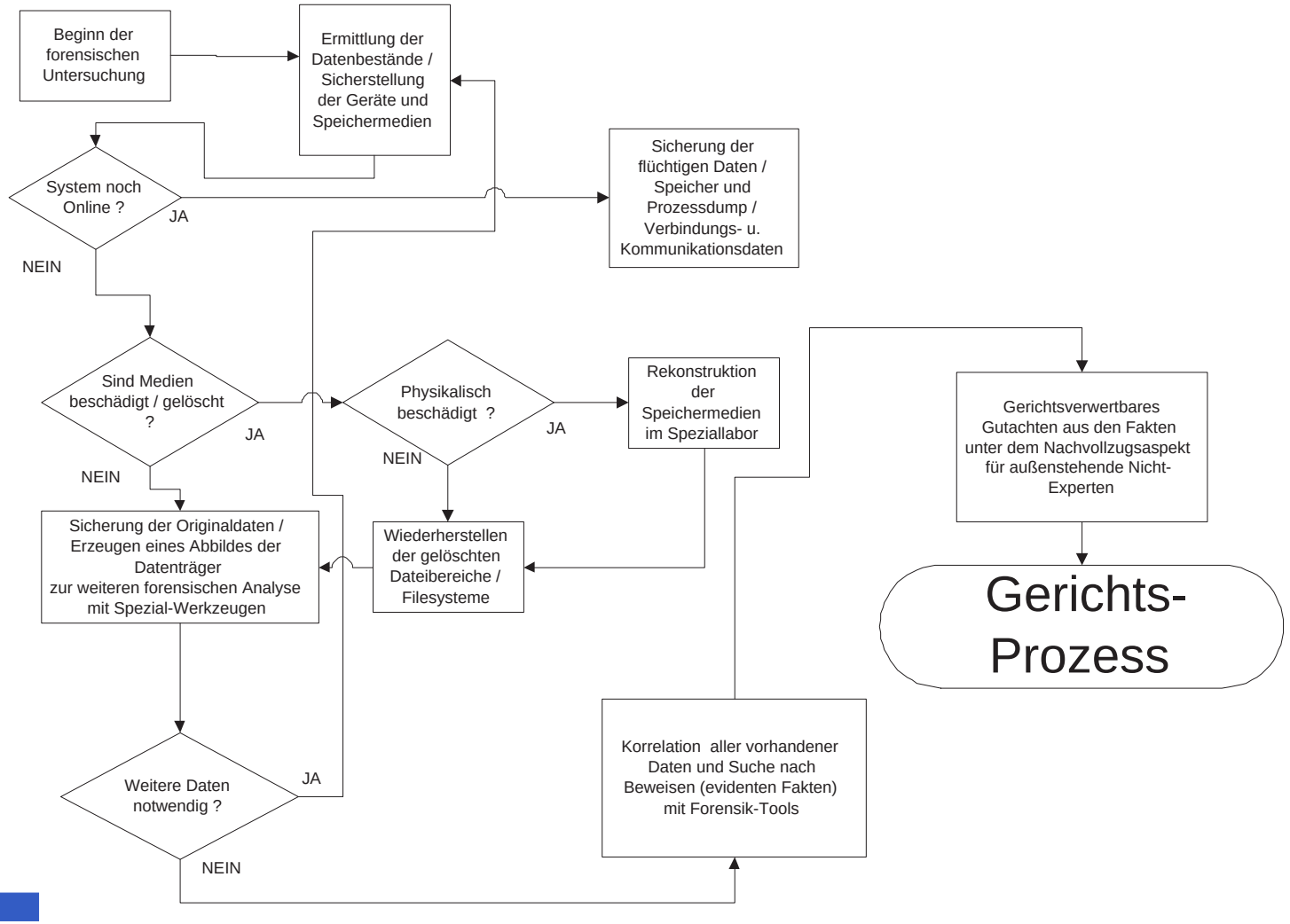
Die Aufgabe

- dokumentiertes und nachvollziehbares Auffinden von evidenten Daten
  - es müssen be-/entlastende Beweise gefunden werden

Die Aufgabe

- Das wird sichergestellt durch:
  - logische Analysen
  - physikalische Analysen
  - Datenintegritätsanalysen
  - Täterprofile/Zugriffsanalysen
- Sicherheit bei einem Gerichtsverfahren durch:
  - nachvollziehbare Vorgehensweise
  - Absicherung gegen Vorwürfe der Manipulation an Beweismitteln

Logische Struktur



Die Online-Durchsuchung

- Einbringen von versteckter Software (Trojaner)
  - Onlinesuche auf dem Datenbestand der Festplatte
  - Speichern von Suchmustern und Schlüsselwörtern auf dem Zielsystem
  - Manipulation am Betriebssystem des durchsuchten Rechners
  - Keine logischen / physikalischen Analysen oder Täterprofile/Zugriffsanalysen möglich
  - Durch die Suche werden Systemzeitstempel zerstört
  - Suche ist von Unbefugten manipulierbar

Die Online-Durchsuchung

- Probleme (Trojaner)
  - Bemerkbar vom Betroffenen
- Sicherheit / Beweiskraft bei einem Gerichtsverfahren?
  - Keine nachvollziehbare Vorgehensweise
  - Ermöglicht Vorwürfe der Manipulation an Beweismitteln

Kriterien zur Analyse

- Wie wird mit meinen Daten im Analyseprozess umgegangen?
- Wie ist gewährleistet, dass weder Daten vernichtet,
  - noch verfälscht werden können?
- Wie ist die Kenntnis und das Know-How des Labors
  - für mein spezifisches Betriebssystem?
- Sind Spezialkenntnisse für Server-Forensik-Analysen vorhanden?
- Sind weitere Fertigkeiten notwendig wie z.B. das
  - physikalische Restaurieren eines beschädigten Datenträgers?

Problem Online-Durchsuchung

Manipulation und Zerstörung von Beweismitteln

- Mögliche Folgeschäden
  - Verfügbarkeit
  - Integrität
  - Authentizität
  - Verschwiegenheit
  - Geheimhaltung

Online-Durchsuchung

Die Analyse eines Servers

Sicherstellung der Informationen

- Sicherstellung der Daten von Log- und Zeitservern
- Festplatten lokal oder Daten im SAN?
- Welche Metadaten könnten manipuliert sein?
- RAID oder Plain-Disk?
  - de-striping für Analyse notwendig?
- Welche Filesysteme?
  - (NFS,Server-Filesysteme,NTFSv5..)
- Sicherung allgemeiner Betriebsdaten
  - (MAC, CPU-ID, System-ID...)

Die Analyse eines Server

Sicherstellung der Informationen

- Welche Kommunikationsbeziehungen?
- Physikalischer Zugriff?
- Zuführung einer Plattenforensik

Die Analyse von Arbeitsplätzen

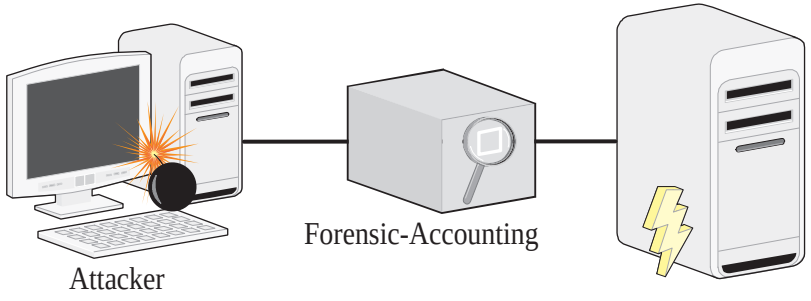
Sicherstellung der Informationen

- Sicherstellung der Festplatten und anderer Medien
  - CDRs, Tapes, Token-Speicher, Internetzugangsdaten ..
- sofortiges Abschalten des Systems, um Löschen von temporären Daten zu verhindern
  - Browser-Cache, E-Mails, Downloads, NEWS-Verzeichnisse
- Zuführung einer Plattenforensik

Die Analyse

weitere Daten:

- Firewall- und IDS-Logs
- Radius/TACAS+ und Einwahl-Logs vom ISP
- weitere Zugriffskontrollinformationen



Die Analyse

Begutachtung der Speichermedien

- Medien verschlüsselt, nicht lesbar?
- physikalische Rekonstruktion durch Datenrettungslabor
- Erzeugung eines identischen Abbildes mit allen Meta- und Filesystemdaten
- Wiederherstellen der gelöschten Dateibereiche im Filesystem auf dem Abbild

Einige Probleme

- es gibt eine Vielzahl von Betriebssystemen, Encodierungen und Dateiformaten.
- oft sind evidente Daten gelöscht oder nur noch bruchstückhaft auf dem Datenträger vorhanden.
- Encodierung der Daten muss gewandelt werden
  - z.B. EBCDIC -> ISO-Latin-1, UNICODE, UCF, UTF ...
- RAID und SAN-Systeme
  - es müssen die Volumen als Image gedumpt und de-striped werden.

Die verschiedenen Ebenen

1. File-System Layer
   - z.B.: Filenames, Directory-Einträge, NTFS Index Trees
2. Meta-Data Filesystem Layer
   - z.B.: UNIX INODES, NTFS MFT Einträge
3. Logical Disk Layer
   - z.B.: Logische Blöcke und HD-Cluster, IP-Einkapselung
4. Physical Layer
   - z.B: ATAPI- oder SCSI-Zugriff über den Hostadapter, Ethernet-Encoding
5. Physical Media Layer
   - z.B: magnetische Aufzeichnungsschicht auf dem Datenträger, Modulation auf dem Netzwerk (HDB-3, QPSK)

Die Analyse

Sicherstellung der Informationen

- Server Forensik oder Analyse eines Arbeitsplatzes?
- Server noch online?
- Informationen noch im Arbeitsspeicher?

Schwere Entscheidung, da evidente Daten vernichtet werden könnten !

- POWER-OFF und forensische Filesystem- und Festplattenanalyse
- DUMP von Speicherbereichen von Prozessen, welche evidente Informationen in ihrem Adressraum beherbergen

Top-Down Analyse

- erst mit Mitteln des Betriebssystems nach Dateien im logischen Filesystem suchen
- spezielle Software, welche die Dateitypen an Hand von „Magic-Bytes “erkennt, hilft schnell, auch gelöschte Datenbestände zu klassifizieren
- Analyse der Zugriffsberechtigungsdaten wie Permissions, ACLs, Filesystem und Objekt-Rechte
  - z.B. Suche nach SUID Daten bei UNIX Systemen, User-Policy bei W2k, XP

Top-Down Analyse

- Analyse der META-Daten wie Zeitstempel von wichtigen System-Dateidaten
  - z.B. wichtige Dateien für den Systemzugang, wie PAM, RADIUS, PASSWD, Registry-Daten
- Integritätsanalyse der META-Daten, um manipulierte Zeitstempel und Zugriffsdaten zu erkennen
  - z.B. ACCESS-Time ist vor der CREATE-Time

Die Aufgabe

- Rekonstruktion
  - Auffinden von evidenten Daten
  - Wiederherstellen von gelöschten Festplattenbereichen
- manipulationssicher ein Speichermedium duplizieren ohne Beweise zu verfälschen
- Auswerten von Datenformaten
  - Mail-Folder, Bild-Dateien

Weitere Aufgaben

Es muss zwischen Arbeitsstations-Tools und Server-Analysewerkzeugen unterschieden werden.

- Sichern von flüchtigen Daten
  - Speicherabzug von Prozessen, Disassemblierung von SWAP und Proc-Dumps
- Analyse von Zugriffs- und Berechtigungs-Metadaten
- Erzeugen von Suchmustern inkl. Cross-Platform-Konvertierung

Fazit

Mittels verdeckter Online-Durchsuchung ist eine zu verwertbaren Beweismitteln führende Analyse nicht möglich.

- Einbringen von Suchpattern, die false positive Ergebnisse liefern (ohne die false positive Ergebnisse erkennen zu können)
- Zerstören von Informationen und Meta-Informationen, die Indizien liefern
- Kein Sichern von anderen wichtigen Nicht-Online Daten (Externe Datenträger)
- Manipulation an Beweismitteln (Installation von Software)

DANKE

Danke für Ihre Aufmerksamkeit!
Noch Fragen?

l.grunwald@dn-systems.de
c.boettger@dn-systems.de