Technische Grundlagen von Online-Durchsuchung und -Beschlagnahme

Markus Hansen

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Vorlesung Datenschutz: Recht und Technik
Sommersemester 2007
Institut für Informatik
Christian-Albrechts-Universität Kiel

markus.hansen@privacyresearch.eu

ULD-i
Datenschutz innovativ

Wer erzählt Ihnen heute was?

- **Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)**
  - **Aufsichtsbehörde für Verwaltung und Wirtschaft (öffentlicher und privater Bereich)**
  - **Beratung zu technischen und rechtlichen Datenschutzfragen**
  - **Zertifizierende Instanz für Datenschutz-Gütesiegel und Datenschutz-Audit**
  - **Fort- und Weiterbildung (z.B. Datenschutzakademie)**

https://www.datenschutzzentrum.de/

Wer erzählt Ihnen heute was?

- **Innovationszentrum Datenschutz & Datensicherheit (ULD-i)**
  - **Beratung über Fördermöglichkeiten**
  - **Vermittlung von Kooperationspartnern**
  - **Unterstützung bei der Entwicklung von datenschutzgerechten Produkten und Geschäftsmodellen**
  - **Wissenstransfer**
  - **Durchführung und Begleitung von Datenschutz- und Datensicherheitsprojekten**

ULD-i
Datenschutz innovativ

Der „Bundestrojaner“

Bildquelle:
www.ccc.de

Gliederung

- Einführung: Online-Durchsuchung
- Vergleich: Offline-Durchsuchung
- Phasen einer Online-Durchsuchung
  - Infiltration
  - Datengewinnung und Kommunikation
  - Beendigung der Maßnahme
- Kernbereich privater Lebensführung
- Fazit
- Literatur

Einführung: Online-Durchsuchung

- **Im „Programm zur Stärkung der Inneren Sicherheit“ (PSIS), das der Bundesminister des Innern am 10. Oktober 2006 vorlegte, wird die**
  „*technische Fähigkeit, entfernte PC auf verfahrensrelevante Inhalte hin durchsuchen zu können, ohne selbst am Standort des Geräts anwesend zu sein*“
  als wichtiger Baustein der Fortentwicklung der kriminalistischen Sachaufklärung bezeichnet.

  Sind Online-Durchsuchungen erforderlich?

Einführung: Online-Durchsuchung

- **VSG NRW (seit Dez. 2006):**
  „§ 5 Befugnisse
  [...] heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel. [...]“

  Vergl. http://www.heise.de/tp/r4/artikel/24/24727/1.html

  => Verfassungsbeschwerde
  Verhandlung BVerfG verm. Herbst 2007

Einführung: Online-Durchsuchung

- **Bundesregierung zum Nutzen der Online-Durchsuchung:**
  „Im Zuge von Online-Durchsuchungen können regelmäßig dieselben Erkenntnisse gewonnen werden, wie durch „offene“ Durchsuchungen und die Auswertung sichergestellter Computerdateien. Die Durchführung einer „offenen“ Durchsuchung beim Beschuldigten setzt diesen jedoch notwendig von den gegen ihn geführten Ermittlungen in Kenntnis. [...] “

  http://dip.bundestag.de/btd/16/039/1603973.pdf

Einführung: Online-Durchsuchung

- **Regelmäßig dieselben Erkenntnisse wie bei der Auswertung sichergestellter Computerdateien?**
- **„Herkömmliche“ forensische Analyse von Computerdateien per Online-Durchsuchung abbildbar?**

Vergleich: Offline-Durchsuchung

Technisch-organisatorische Anforderungen an die Beweiserhebung auf Computersystemen:

- **Rechner wird in Anwesenheit von Eigner/Vertreter und Zeugen sichergestellt.**
- **Sachverständige Kriminaltechniker führen Analyse durch.**
- **Festplatten werden schreibgeschützt (um Veränderung auszuschließen) vollständig ausgelesen, Image-Kopie erstellt.**
- **Über Image wird kryptographische Prüfsumme (Hash) errechnet und dokumentiert.**

Vergleich: Offline-Durchsuchung

- **Untersuchungen werden ausschließlich an Image-Kopie durchgeführt.**
- **Alle Schritte der Untersuchung inkl. verwendeter Auswertungsverfahren sind zu dokumentieren.**

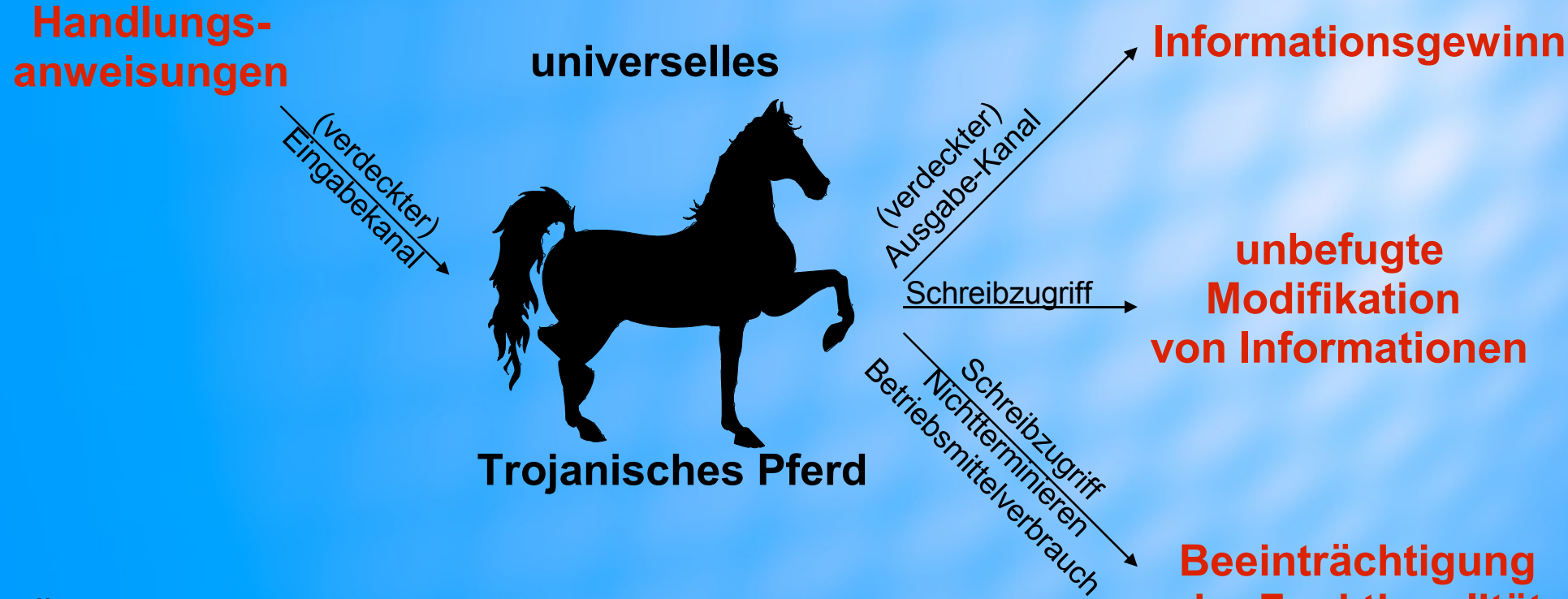
- **Nur so hält das Verfahren einer kritischen Prüfung stand (Revisionsfähigkeit);**
  von einer Echtheit gewonnener Informationen kann andernfalls nicht ausgegangen werden.

Vergleich: Offline-Durchsuchung

Zum Nachlesen:

- **Alexander Geschonneck: Computer-Forensik, 2., aktualisierte Auflage, dpunkt.verlag, Heidelberg, 2006, S. 84.**
- **Fall am AG Lübeck; Peter Mühlhauber: Wie verläßlich sind digitale Beweise?, in Telepolis, Verlag Heinz Heise, 2007, http://www.heise.de/tp/r4/artikel/24/24638/1.html.**
- **Wolfgang Bär: Handbuch zur EDV-Beweissicherung im Strafverfahren, Richard Boorberg Verlag, 2007, S. 282.**

Universelles Trojanisches Pferd



Quelle:
Andreas Pfitzmann: Sicherheit in Rechnernetzen: Mehrseitige Sicherheit in verteilten und durch verteilte Systeme, Dresden, 2000, S. 9 ff, online: http://dud.inf.tu-dresden.de/~pfitza/DSuKrypt.pdf.

Phasen der Online-Durchsuchung

- **Infiltration**
  bezeichnet den Vorgang, das Zielsystem zu kompromittieren, indem ein Trojanisches Pferd, d.h. die Softwarekomponente, die Ermittlern den Zugriff per Internet erlaubt, installiert wird.

- **Datengewinnung und Kommunikation**
  Eigentliche Online-Durchsuchung.

- **Beendigung der Maßnahme**
  z.B. wenn Verdacht entkräftet wird.

Infiltration

Mit „Hilfe“ des Nutzers:

- **Verheißungsvolle E-Mails (Instant Message ...)**
  - **Pornographische Inhalte, Bedrohungsszenarien, ...**
- **Web-Seiten verleiten zum Klicken von Links**
  - **Gratis-„Zugangstools“**
- **„Herumliegenlassen“ von CDs, USB-Sticks, ...**
  - **Autorun-Funktion von Windows :-(**

- **Wie zielgenau sind diese Angriffe?**
  - **Wie merkt man, dass man den Falschen hat?**
  - **Was bedeutet das für Betroffene?**
  - **Filterprobleme bei mehreren Infiltrationen?**

Infiltration

Ohne „Hilfe“ des Nutzers:

- **Ausnutzen von Sicherheitslücken in Programmen oder Betriebssystemen.**

  Zeitfenster bei
  bekannten Lücken: Stunden bis wenige Tage bei guten Herstellern.
  Zero-Day-Exploits: Durchschnitt ein Jahr.

- **Hintertüren „ab Werk“**

  Vergl. Diskussion um „_NSAKEY“ in Windows NT 4.0 (jetzt: „_KEY2“) oder April-Scherz des CCC: „Bundestrojaner in ELSTER gefunden“.
  Kann auch in Hardware realisiert werden.

- **Infektion von Downloads „on the fly“**

  Kleiner Ansatz: Manipulation beim Provider.
  Großer Ansatz: Z.B. am DECIX.

Infiltration

Ohne „Hilfe“ des Nutzers:

- **Physischer Zugriff auf den Rechner durch heimliches Eindringen in Räumlichkeiten.**
  => Einziger Infiltrationsvorgang, der ohne Hilfe des Nutzers auskommt und Infektion Unbeteiligter (nahezu) ausschließt.
- **Infiltration ohne physischen Zugriff ist Beleg, dass auch Dritte den Rechner infiltriert haben können.**
- **Ermittler sind auf gleiche Methoden angewiesen wie Virenautoren, Betreiber von Bot-Netzen, ausländische Geheimdienste, org. Kriminalität.**

Datengewinnung und Kommunikation

- Ermittler greifen per Internet auf den Rechner zu und können auf dem System vorhandene Daten auslesen oder verändern sowie neue Daten schreiben.
- Keine exklusive Kontrolle über Rechner => keine Echtheitsbestätigung!
- Bei online infiltriertem System: Weitere Infiltration durch Dritte kann nicht ausgeschlossen werden. Diese können Daten zu Täuschungszwecken manipulieren.

Datengewinnung und Kommunikation

- **Abfangen von Tastatureingaben**
  Keylogger, z.B. für Passworte, ggf. Zwischenspeicherung bis zur Online-Verbindung.
  => Sicherheitsrisiko!
- **Abfangen von Ende-zu-Ende-Kommunikation, z.B. Instant Messaging, Internet-Telefonie, Video-Konferenzen.**
- **Zugriff auf angeschlossene Mikrofone, Kameras.**

Datengewinnung und Kommunikation

Möglich: Aufdeckung der Überwachung.

- **Bestenfalls: Ende der Maßnahme.**
- **Einspeisung von Datenmüll.**
- **Einspeisung gezielter Falschinformationen.**
- **Einspeisung Trojanischer Pferde (Gegenangriff).**

Aufdeckung lässt sich technisch nicht ausschließen.

Beendigung der Maßnahme

- **Funktion zur Beendigung der Maßnahme erforderlich, z.B.**
  - **... falls Verdacht entkräftet (manuelle Auslösung).**
  - **... falls Durchsuchungserlaubnis aufgehoben wird (manuelle Auslösung).**
  - **... falls keine Verbindung zu Steuersystem mehr aufgebaut werden kann, um Sicherheitslücken (Hintertür) zu vermeiden (automatische Auslösung).**
- **Was ist, wenn der Nutzer nach Beendigung ein „infiltriertes“ Backup wieder einspielt?**

Kernbereich privater Lebensführung

- **BVerfG zum Großen Lauschangriff:**
  Es gibt einen Kernbereich privater Lebensführung, der grundsätzlich vor staatlichem Zugriff geschützt ist. (2003)
- **BVerfG zum niedersächsischen Polizeigesetz:**
  Entsprechende Anforderungen gelten für jegliche Art von verdeckten Ermittlungsmaßnahmen.
  Erhebungsverbot – Wissentlicher Eingriff in den Kernbereich in keinem Fall zu rechtfertigen.
  Bloße Verwertungsverbote reichen in diesen Fällen nicht aus. (2005)

Kernbereich privater Lebensführung

- **Aus der Praxis, Beispiel „Jugend von heute“:**
  - **Jugendliche eröffnen Freundschaften, Beziehungen per Internet (Instant Messaging).**
  - **Tagebücher sind heute zunehmend digital auf dem eigenen Rechner.**
  - **Fotos sehr persönlicher bis intimer Natur werden auf der eigenen Festplatte gespeichert.**
  - **Entwicklungsprozesse, z.B. Findung der eigenen sexuellen Identität, zunehmend per Internet geprägt.**

=> Kernbereich privater Lebensführung von Online-Durchsuchungen deutlich betroffen.

Fazit

- Auch Trojanisches „Ermittlungspferd“ kann und wird Fehler enthalten und infiltrierte Systeme damit gefährden.
- Online-Infiltrationsverfahren können eine Beeinträchtigung Unbeteiligter nicht ausschließen.
- Bei Aufdeckung:
  Täuschung durch Falschinformationen oder Gegenangriff möglich.
- Erfolgreiche Infiltration ist Beleg, dass auch Dritte Zugriff haben können.

Fazit

- **Per Online-Durchsuchung erlangte Informationen sind nicht annähernd so verläßlich wie bei forensischer Analyse sichergestellter System.**
- **Infiltration ist Manipulation des Untersuchungsgegenstandes.**
- **Da exklusiver Zugriff durch Ermittler nicht sicherzustellen ist, ist die Echtheit der gewonnenen Informationen regelmäßig anzuzweifeln.**

Fazit

- **Eine Online-Durchsuchung widerspricht allen Anforderungen, die aus technisch fundierten Gründen an einen sachverständigen Gutachter im Rahmen einer forensischen Analyse gestellt werden.**

Literatur

- ***Grundlage dieses Vortrags:***

  Markus Hansen, Andreas Pfitzmann:
  Technische Grundlagen von Online-Durchsuchung und -Beschlagnahme,
  im Erscheinen: DRiZ – Deutsche Richterzeitung, (voraussichtlich Ausg. 8/2007).

Kontakt:
Markus Hansen: markus.hansen@privacyresearch.eu
Andreas Pfitzmann: pfitza@inf.tu-dresden.de

Weitere Literatur

- Unabhängiges Landeszentrum für Datenschutz: Stellungnahme des ULD vom 27.06.2007 zum Gesetzesentwurf der Bundesregierung für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BR-Drucksache 275/07, https://www.datenschutzzentrum.de/polizei/20070627-vorratsdatenspeicherung.htm.
- Ulf Buermeyer: Die „Online-Durchsuchung“. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, in: HRRS. Heft 4, 2007, S. 154, http://www.hrr-strafrecht.de/hrr/archiv/07-04/index.php?sz=8.

Veranstaltungshinweis

Datenschutz-Sommerakademie

Offene Informationsgesellschaft und Terrorbekampfung – ein Widerspruch?

2007-08-27
Maritim Hotel Bellevue

Anmeldung bis 2007-08-08, Teilnahme kostenfrei.

Programm und Information:
https://www.datenschutzzentrum.de/sommerakademie/2007/

ULD-i
Datenschutz innovativ


ULD-i
Datenschutz innovativ
http://www.uld-i.de/