# Hacking Day 2014 – Datenschutz

## Digital Forensics –
## die Jagd nach digitalen Spuren

Christoph Baumgartner - CEO & Inhaber - OneConsult GmbH

# Agenda

- → Vorstellung
- → Einleitung
- → Projektgliederung
- → Tools
- → Praxisbeispiele
- → Do’s & Don’ts

# Über mich

- Christoph Baumgartner
- Studium der Wirtschaftsinformatik Universität Zürich (MSc UZH IS)
- Seit 1996 Berater in den Bereichen IT Security und Strategie: Spezialgebiete:
  - Konzeptionelle Security Audits
  - Sicherheitsrichtlinien und -konzepte
  - Digital Forensics
- Gründer der OneConsult GmbH im Jahr 2003
- Seither CEO und Inhaber
- ISECOM Board Member

# OneConsult GmbH

- → IT Security Consulting
- → Kein Verkauf von Hard- und Software
- → Kunden
  - Mehr als 200 Unternehmen in der Schweiz, Europa und Übersee (inklusive ein Dutzend der «Fortune Global 500 Corporations»)
  - Kunden gleichmässig auf alle Branchen verteilt (Finanz-, Pharma-, Industrie-Branche sowie öffentliche Verwaltungen (Bund, Kantone und Städte))
- → Standorte
  - Schweiz: Hauptsitz in Thalwil
  - Weitere Büros in München (Deutschland) und Wien (Österreich)

# Dienstleistungsportfolio

**Technische Security Audits**

(12 zertifizierte Penetration Tester / Security Analysten z.B. OPST & OSCP)

**Konzeptionelle Security Audits**

(3 zertifizierte ISO/IEC 27001 Lead Auditors)

**Digitale Forensik**

(4 köpfiges Team: 2 SANS-zertifizierte GCFE Forensiker)

**Security Consulting**

**Training** (2 zertifizierte OSSTMM Trainer)

Security Services

# Agenda

- → Vorstellung
- → Einleitung
- → Projektgliederung
- → Tools
- → Praxisbeispiele
- → Do’s & Don’ts

# Darum geht es bei der Digitalen Forensik

- Extraktion und Untersuchung von Daten auf digitalen Geräten, wie Computern, Mobiltelefonen, Druckern, Digitalkameras, Memory Sticks, etc.
- Üblicherweise in Verbindung mit einer kriminellen Handlung mit dem Ziel, (gerichtsverwertbare) Beweise zu identifizieren und sicherzustellen
- Es sollen Antworten auf folgende Fragen geliefert werden:
  - Wer tat
  - Was,
  - Wann,
  - Wo,
  - Und wie (mittels Nutzung welcher Mittel/Schwachstellen)?

# Potentielle Auslöser

Beispiele für Vorfälle, die mittels Digitaler Forensik untersucht werden können, sind:

→ Datendiebstahl

→ Besitz und Verteilung von digitalen illegalen Inhalten

→ Malware-Befall

→ Hacker-Angriffe

→ Vorsätzliches Löschen von Daten

→ Industriespionage / Cyber Warfare

→ Betrug

→ Mobbing

# Digital Forensics: Typen

→ Computer Forensics
→ Network Forensics
→ Mobile Forensics
→ Memory Forensics (z.B. für Malware Forensics)

# Digital Forensics: Ansätze

→ Post-Mortem Analyse
- Zu untersuchendes System wurde bereits abgeschaltet: z.B. per Shut Down oder Stecker ziehen
- Arbeit an Arbeitskopie => weniger fehleranfällig

→ Live Response
- Arbeit am laufenden System
  - Systeme, welche nicht über einen längeren Zeitraum nicht zur Verfügung stehen dürfen (z.B. Mailservercluster bei Grosskonzern)
  - Systeme, deren Abschaltung zu irreversiblem Datenverlust führt (z.B. bei Mobile oder Memory Forensics)
- Fehleranfällig, da jede Aktivität (mit hoher Wahrscheinlichkeit) das Untersuchungsobjekt verändert

# Rechtliche Aspekte (Auswahl)

→ Untersuchung durch Nicht-Strafverfolgungsbehörden (= private Untersuchungen)

- Müssen Datenschutzgesetz befolgen: so darf z.B. Untersuchung nicht von IT Abteilung initiiert werden (sondern üblicherweise durch HR in Kombination mit Vorgesetzten und Legal)
- Können nur Untersuchungen im eigenen «Hoheitsgebiet» bzw. dem des Auftraggebers (z.B. eigene Gebäude, eigene Infrastruktur, eigene Mitarbeitende) durchführen, nicht bei Dritten (z.B. Provider)

# Rechtliche Aspekte (Auswahl)

→ Untersuchung durch Strafverfolgungsbehörden (= offizielle Ermittlungen, z.B. durch Polizei, Staatsanwaltschaft und deren Beauftragte):

- Werden in vielen Fällen erst aktiv, nachdem Anzeige erstattet wurde
- Können im Gegensatz zu privaten Untersuchungen via Gerichtsbeschluss bzw. Rechtshilfegesuch (Ausland) auch auf Daten/Systeme Dritter zugreifen bzw. deren Herausgabe einfordern
- Können ohne Einschränkung auf alle relevanten Daten zugreifen

# Rechtliche Aspekte (Auswahl)

→ Es müssen bestimmte Kriterien bei der forensischen Untersuchung strikt eingehalten werden, damit die Resultate als Beweis vor Gericht voraussichtlich (liegt im Ermessen des Gerichts) anerkannt werden, z.B.:

- Integrität der Datenträger
- Nachvollziehbarkeit / lückenlose Dokumentation
- Vertrauenswürdigkeit der Gutachter / der eingesetzten Tools

# Knackpunkte

- → Untersuchung kann publik werden (Medien)
- → Verhältnismässigkeit
  - Berechtigter Verdacht vs. Rufmord
  - Gerechtigkeitssinn vs. Image Schäden / (potentielle) Verluste
- → Erfolgswahrscheinlichkeit
- → Börsenkotierte Unternehmen sind verpflichtet über Sachverhalte zu informieren, welche einen Einfluss auf den Börsenkurs haben können: aber nur wenn ein Schaden entstanden ist
- → Es gibt keine Garantie, dass Beweise gefunden werden (nur Spurensuche)

# Knackpunkte

→ Dilemma Security Incidents
- Entscheid ob
  - Möglichst rasch Normalzustand wiederherstellen
  - Oder ob man die Beweise sichern möchte für eine forensische Analyse (= dauert dann länger)
- Oft nicht oder erst spät erkennbar, ob möglicherweise eine strafbare Handlung vorliegt

→ Folge: die meisten Fälle enden nicht vor Gericht

# Agenda

- → Vorstellung
- → Einleitung
- → Projektgliederung
- → Tools
- → Praxisbeispiele
- → Do’s & Don’ts

# Phasen: Übersicht

- → Briefing / Vorbereitung
- → Forensische Daten Akquisition
- → Datenanalyse
- → Dokumentation
- → Optional: Präsentation / Diskussion

# Phase 1: Briefing / Vorbereitung

- → HR/Legal/Management initialisieren forensische Untersuchung
- → Ermittler (extern oder intern) werden mit der Untersuchung beauftragt und erhalten die nötigen Informationen
- → Tools werden ausgewählt und vorbereitet
- → Auftrag, Ziele, Projektrollen und jegliche Aktivitäten werden lückenlos dokumentiert

# Phase 1: Briefing / Vorbereitung (Details)

Diese Phase muss folgende Punkte abdecken

→ Was passierte bisher?

- Fakten
- Vermutungen

→ Was sind die Projektziele?

- Ansatz:
  - So rasch wie möglich zurück zum Normalbetrieb (reine Wiederherstellung => keine forensische Analyse = Projektabbruch)
  - Kurzanalyse (ohne Option rechtlich gegen Verursacher vorzugehen)
  - Gründliche Analyse (Wahrung aller rechtlichen Optionen)

# Phase 1: Briefing / Vorbereitung (Details)

- Projektscope:
  - Erwartete Resultate und Lieferergebnisse
  - Welche Fragen sollen beantwortet werden
  - Systeme in / out of Scope

→ Anderes

- Projektteam
- Eskalationspfad
- Zeitplanung
- Abbruchkriterien
- …

# Phase 2: Forensische Datenakquisition

- → Zu untersuchende Systeme und Datenträger sammeln bzw. bestimmen
- → Bei Post-Mortem Analyse: Forensische Kopien der Datenträger erstellen
  - Forensische Tools verwenden, um binäre Manipulation der zu untersuchenden Datenträger (= Quelldatenträger) zu verhindern
  - Kopien erstellen
    - › Mindestens 1 für Archivzwecke und 1 als Arbeitskopie
    - › Optional: 1 für den Auftraggeber, dass der mit den Daten weiterarbeiten kann
  - Diese Aktivität kann abhängig von Speicherkapazität und nutzbaren Schnittstellen von 1 bis über 24 Stunden dauern!
- → Jeden Schritt dokumentieren

# Phase 3: Datenanalyse

→ Analyse
- Bei Post-Mortem Analyse: Arbeitskopie(n) mit geeigneten Tools analysieren
- Bei Live Response: Originalsystem(e) mit geeigneten Tools analysieren
- Gemäss Projektauftrag nach Spuren suchen

→ Jeden Schritt dokumentieren

# Phase 4: Dokumentation

Abzudeckende Punkte

- → Projektteam
- → Auftrag
- → Scope
- → Findings (inkl. Herleitung)
- → Timeline (was wann passierte)
  - Projekttasks
  - Findings
- → Ergebnisse / Beurteilung
  - Fakten (keine Annahmen) nennen, keine Partei ergreifen, Meinungen klar als solche bezeichnen
  - Nur über Daten(spuren) nicht über Leute schreiben
- → Optional: Empfehlung
- → Eingesetzte Tools (inkl. Versionen)
- → Unterschrift des leitenden Forensikers
- → Optional: Screenshots (falls sinnvoll)

# Optional: Phase 5: Präsentation / Diskussion

→ Präsentation und Besprechung des Projekts und der Findings
- In einer neutralen und objektiven Art
- Fakten (keine Annahmen) nennen, keine Partei ergreifen, Meinungen klar als solche bezeichnen
- Nur über Daten(spuren) nicht über Leute sprechen

→ Optional: weitere Schritte besprechen

# Agenda

- → Vorstellung
- → Einleitung
- → Projektgliederung
- → Tools
- → Praxisbeispiele
- → Do’s & Don’ts

# Tools


# Hardware

- → Write Blocker (benötigt Notebook / PC)
- → Forensic Duplicator (stand alone)
- → Forensic Workstation
  - Laufwerke
    - › Schnelle Laufwerke (Zugriffszeiten / Durchsatz)
    - › Ausreichend Speicherplatz
    - › Optimal: Kombination von SSDs und konventionellen Festplatten
  - Schnelle CPU
  - Viel RAM
  - Optional: Datenträgerkopiergeräte


# Software (Auswahl)

→ **MoonSols DumpIt**
Werkzeug um den Arbeitsspeicher von Windows Systemen (32 und 64 Bit) zu sichern:
http://www.moonsols.com/resources/

→ **Mandiant's Memoryze**
Werkzeug zur Sicherung des Arbeitsspeichers von Windows Systemen (MemoryDD.bat) und für Arbeitsspeicheranalysen:
http://www.mandiant.com/resources/download/memoryze/


# Software (Auswahl)

→ **LiME**
Zur Sicherung des Arbeitsspeichers von Linux- und auf Android basierenden Systemen:
https://code.google.com/p/lime-forensics/

→ **FTK Imager (Lite)**
Zum Sichern des Arbeitsspeichers von Windows Systemen, Erstellen und Betrachten von Festplattenabbildern:
http://www.accessdata.com/support/product-downloads


# Software (Auswahl)

→ **Magnet Encrypted Disk Detector**
Erkennt mit TrueCrypt, PGP, Safeboot und Bitlocker verschlüsselte Datenträger unter Windows:
http://info.magnetforensics.com/encrypted-disk-detector/

→ **Dcode**
Zur Decodierung von Zeitstempeln von verschiedenen Systemen, läuft unter Windows:
http://www.digital-detective.co.uk/freetools/decode.asp


# Software (Auswahl)

→ **Volatility Framework**
Toolbox zur RAM Analyse, nahezu Betriebssystem-unabhängig, da Python-basiert:
https://code.google.com/p/volatility/

→ **Event Log Explorer**
Zur Analyse von Event Logs unter Windows:
http://www.eventlogxp.com/


# Software (Auswahl)

Die renommiertesten kommerziellen Forensik Tool Suites (weltweit bei Behörden und Firmen im Einsatz):

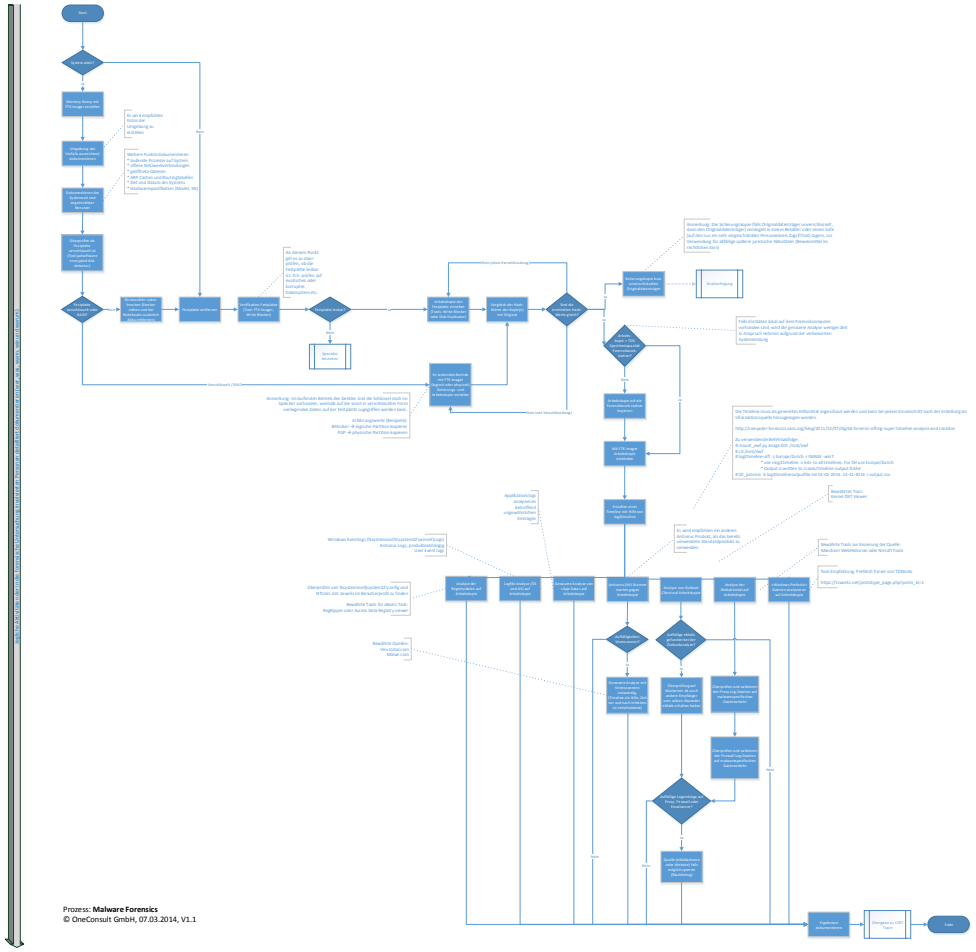
→ **AccessData Forensic Toolkit (FTK)**
http://www.accessdata.com/products/digital-forensics/ftk

→ **Guidance Software EnCase Forensic**
http://www.guidancesoftware.com/

# Agenda

- → Vorstellung
- → Einleitung
- → Projektgliederung
- → Tools
- → Praxisbeispiele
- → Do’s & Don’ts

# Beispiele



# Beispiele

- → Finanzunternehmen: Rufschädigung
- → Industriekonzern 1: Informationsvorsprung
- → Industriekonzern 2: Industriespionage
- → Medienunternehmen 1: Hacker-Attacke
- → Medienunternehmen 2: Hacker-Attacke
- → Energiekonzern: Mobbing
- → Detailhandelskonzern: Malware-Attacke

# Agenda

- → Vorstellung
- → Einleitung
- → Projektgliederung
- → Tools
- → Praxisbeispiele
- → Do’s & Don’ts

# Do's & Dont's

1. Unrecht nicht mit Unrecht bekämpfen: sich immer an die Gesetze halten. Bei Unsicherheit: Rechtsdienst/-anwalt konsultieren
2. Den Personenkreis so klein wie möglich halten, welcher über die Untersuchung informiert ist
3. Analyse nicht an Originaldatenträgern durchführen (Ausnahme: Live Response)
4. Sämtliche Schritte und Aktivitäten lückenlos dokumentieren (Nachvollziehbarkeit)
5. Trennung der betroffenen Systeme (zu untersuchende Systeme und Systeme, welche für die Untersuchung benötigt werden) von den anderen Systemen im Netzwerk ((W)LAN/WAN) – idealerweise dedizierter Raum (Forensic Lab) ohne Netzwerkverbindung

# Do’s & Dont’s

6. Falls möglich nur bekannte Forensik Tools einsetzen
7. Genau wissen, was und wie (Vorgehen und Tools) gemacht wird: falls nicht, interne oder externe Spezialisten beiziehen
8. Nur Fakten zählen – keine Vermutungen als Fakten «verkaufen»
9. Argumentationskette muss schlüssig und komplett sein
10. Beurteilung ob gegen Gesetze oder organisationsinterne Weisungen verstossen wurde, ist nicht Aufgabe des mit der forensischen Analyse betrauten Personals

# Danke für Ihre Aufmerksamkeit, Fragen?

Christoph Baumgartner
MSc UZH IS, OPST
CEO & Owner

christoph.baumgartner@oneconsult.com
+41 79 256 25 25

**Hauptsitz**
OneConsult GmbH
Schützenstrasse 1
8800 Thalwil
Schweiz

Tel +41 43 377 22 22
Fax +41 43 377 22 77
info@oneconsult.com

**Büro Deutschland**
Niederlassung der OneConsult GmbH
Karlstraße 35
80333 München
Deutschland

Tel +49 89 452 35 25 25
Fax +49 89 452 35 21 10
info@oneconsult.de

**Büro Österreich**
Niederlassung der OneConsult GmbH
Wienerbergstraße 11/12A
1100 Wien
Österreich

Tel +43 1 99460 64 69
Fax +43 1 99460 50 00
info@oneconsult.at