IT-Forensik im Unternehmen

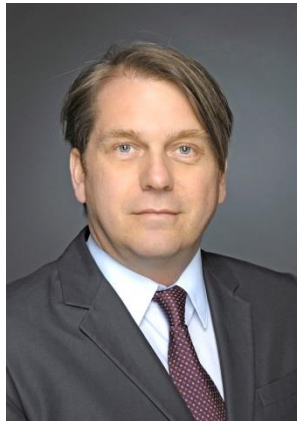
Herausforderungen durch Big Data und Beispiele aus der Beratungspraxis

4. IT-Forensik Workshop@ FH Aachen, 7. Mai 2014

Helmut Brechtken
Director IT-Forensik & eDiscovery, it.sec GmbH & Co KG

Vorstellung

Helmut Brechtken



- Director IT-Forensik & eDiscovery, it.sec
- zuvor 6 Jahre bei KPMG: Forensic Technology
- eDiscovery und Forensic Data Center bei KPMG in Deutschland aufgebaut
- Investigation ca. 100 Fälle
- IT-Forensik, Incident Response Investigation, Kartelluntersuchungen, eDiscovery, Cybercrime, Data Leakage
- davor 12 Jahre bei Evonik (Degussa): IT-Leitung, Data Center, IT-Security, Inhouse Consulting
- Diplom-Physiker
- * in Dortmund, über Würzburg nach Köln

XING

LinkedIn

IT-Forensik und Big Data

- **Wikipedia:** „Die ***IT-Forensik*** behandelt die Untersuchung von verdächtigen Vorfällen im Zusammenhang mit IT-Systemen und der Feststellung des Tatbestandes und der Täter durch Erfassung, Analyse und Auswertung digitaler Spuren. …“
- Gerichtsfestigkeit
- **Wikipedia:** „***Big Data*** bezeichnet Daten-Mengen, die zu groß oder komplex sind, um sie mit händischen und klassischen Methoden der Datenverarbeitung auszuwerten. …“

IT-Forensik

Aufgabenstellungen im Beratungsumfeld

- Verdacht auf Straftat (Betrug, Untreue, Unterschlagung, Korruption), Beweise gesucht
- Verdacht auf „undichte Stellen“: Finden und Abstellen
- Verdacht auf Datendiebstahl: Beweise
- Incident Response: Aufklärung von Cybercrime
- Kartelluntersuchungen
- eDiscovery

IT-Forensik

Bereiche & Kategorien im Unternehmensumfeld

- Anlass: Wirtschaftskriminalität (Fraud), Incident Response, eDiscovery, …
- Art: Strukturierte (Datenbanken) / unstrukturierte Daten (eMails, Office Doks, Web usw.)
- Lokale Systeme, SAN-Speicher, Cloud (international), soziale Netzwerke
- Quellen: Festplatten, eMails, Backups, RAM, Netzwerkgeräte, Applikationen, GPS, Zutrittskontrolle
- Lebende / tote Systeme

Klassik vs. Trends

Klassische Bereiche der IT-Forensik

- Klassische Festplattenforensik
- Incident Response
- Live (RAM, Prozesse, Netzwerk) - Analyse
- eMail-Analyse & Review (unstrukturierte Daten)
- Analyse strukturierter Daten aus Datenbanken (Fraud Shemes, Benford etc.)

Trends und neue Felder

- Smartphone-/Tablet-Analyse
- MacOS Forensik
- Virtualisierung
- Cloud-Forensik
- „Big Data“
- Social Media
- APT (Stuxnet et al.)

Abgrenzung

Wer betreibt IT-Forensik in Deutschland?

- Universitäten, Forschungseinrichtungen (z.B. FH Aachen, Fraunhofer SIT, CASED)
- Spezialisierte Dienstleister
- Wirtschaftsprüfungsgesellschaften
- Chaos Computer Club CCC
- Konzerne (Siemens, Daimler, Bayer, etc.)
- Bundesamt für Sicherheit in der Informationstechnik BSI
- Polizei: LKA, BKA
- Bundesnachrichtendienst BND und verwandte Organisationen
- Bundeswehr (MAD)
- …

Datenschutz

Spannungsfeld IT-Forensik und Datenschutz

- IT-Forensik Projekte umfassen meist auch persönliche Daten Einzelner
- Dilemma zw. Aufklärungswillen und -pflicht sowie Schutzregelungen nach BDSG
- Lösung unter Einhaltung aller rechtlichen Vorgaben meist möglich
- Umsetzung der Lösung manchmal mühselig und zeitaufwändig (RA, DSB, BR, Anonymisierung), aber letztendlich fast immer möglich

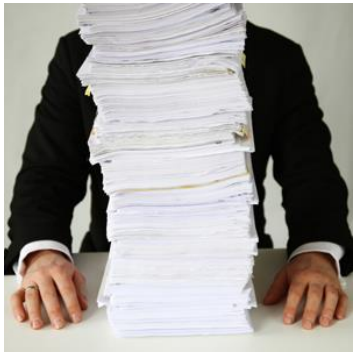
Fallbeispiele (1/4): Projekt Z

Projekt Z

- Energiesektor
- Projektziel: Identifizierung aller kartellrechtlich relevanten Dokumente in einem Geschäftsbereich.
- eDiscovery, 120 Mitarbeiter, 16 TB Daten - **BIG DATA**
- Entwicklung spezifischer Collector, Handling verschlüsselter Daten
- Datentransfer Kunde – it.sec mittels 60 High-Security HDs

Fallbeispiele (1/4): Projekt Z

- **BIG DATA**: weitere Verarbeitung nur automatisiert und vollständig dokumentiert
- Mehrfache Filterung der Daten auf 2,9 TB
- Verbleibend 8,5 Mio Dokumente zum Review
  - Papierstapel 3 km Höhe oder
  - 51 000 Papierpakete (a 500) oder
  - 10.000 PT (8,3 Jahre) oder
  - 21 Mio € Anwaltskosten



- Einsatz von Keyword-Search und Künstlicher Intelligenz - KI - zur computergestützten Datenanalyse
- Ergebnis: Projekt läuft noch…

Fallbeispiele (2/4): Projekt P

Projekt P

Data Leakage Investigation: Informationen aus engstem Führungskreis eines Unternehmens der chemischen Industrie in der Zeitung.

Investigation und Analyse der Prozesse.

- Chemische Industrie
- Verdacht auf Malware auf CEO-Notebook. Projektziel: Identifizierung der Schwachstelle für Informationsabfluss (kleiner Kreis, brisante Personalinformation)
- Untersuchung des Endgerätes. Ergebnis: eMails nicht verschlüsselt, Festplatte nicht verschlüsselt, Prozessschwächen beim Gerätetausch durch ext. IT-Support: Daten des CEO waren für unbestimmte Zeit auf einer externen Festplatte (natürlich unverschlüsselt).
- Untersuchung der eMail Berechtigungen des „kleinen Kreises“: 4 Vorstände mit 16 Vertretern, Assistentin etc.: Kreis von 20+ Zugriffsberechtigten
- Ergebnis: einige Prozessschwächen entdeckt => Empfehlungen

Fallbeispiele (3/4): Project X

Project X

- Industrieunternehmen, ca. 350 Mitarbeiter
- berichtet 13 Vorfälle / Störungen im Netzwerk April – August 2013
  - Ausfall Fileserver (2x)
  - Ausfall Logistiksystem (ca. 2 Mio € Schaden pro Tag)
  - Massiver Virenbefall (> 300 Viren entdeckt)
  - MS Windows AD (Domäne umbenannt – 1 Tag Ausfall)
  - Hardware Vorfall Domain Controller
  - Manipulation Überwachungskamera im Serverraum
- einige Vorfälle sicher interne Sabotage
- Forensische Untersuchung: Identifizierung der Ursache, Empfehlungen

Fallbeispiele (3/4): Project X

Untersuchungsplan:

- Corporate Intelligence / Background Research (~ 5 Firmen, 20 Player)
- Informationssammlung intern
- Interviews
- IT-Forensische Analysen
- Profiling

Geplant: Undercover Untersuchung

Fallbeispiele (3/4): Project X

- **Durchführung (September 2013 bis heute):**
  - Projekt Team on Site, Steering Committee, Abstimmung mit RA, DSB, BR
  - CI: keine Auffälligkeiten
  - Informationssammlung, umfangreiche Bestandsaufnahme, Timeline erweitert auf (heute) 45 Incidents. 7 waren eindeutig Sabotage, z.B.:
    - EMC SAN logisch zerstört
    - Logistik System: OS-HD von 3 Servern gelöscht
  - BIG DATA: 26 HD mit digitalen Beweismitteln (von 11 Incidents) - TMI
  - 20 forensische Interviews – undercover (?)
  - Detaillierte IT-Forensische Analysen für 5 Prio1 Incidents
  - Profiling: abgeschlossen

Fallbeispiele (3/4): Project X

- **Ergebnis:**
  - Fall ist noch nicht gelöst
  - 5 Monate keine Ausfälle (24. September 2013 – 24. Februar 2014)

- **Weitere Erkenntnisse / Empfehlungen:**
  - Incident Response Plan
  - Sehr großer Optimierungsbedarf:
    - Organisation (4 Player, diverse Berater):
      - Verantwortlichkeiten,
      - Kommunikation,
      - Prozeduren,
      - Policies, etc. pp.
    - Technisch:
      - IT-Security (Account Mgmt, Passwörter),
      - AV,
      - Patching,
      - Backup,
      - Internet GW

Fallbeispiele (4/4): Projekt K

Project K

Vorwurf: Mobbing.

- Telekommunikationsanbieter
- Starker Verdacht auf Mobbing durch 4, z.T. leitende, Mitarbeiter
- Konzertierte Aktion mit Security, RA, Aufsichtsrat, IT-Forensik, Forensik aus Polen: Freistellung, Konfiszierung der IT-Geräte und Telefone

- Forensische Analyse 7 Notebooks und 9 Smartphones
- eDiscovery der vorgefunden eMails und Dokumente

Fallbeispiele (4/4): Projekt K

- eDiscovery der vorgefunden eMails und Dokumente
- Zwischenergebnis:
  - Mobbing bestätigt
  - 7 weitere Mitarbeiter durch eMail-Kommunikation belastet
  - Austausch pornografischen Materials (über Firmencomputer)
  - Beifang: Absprache von Drogengeschäften (über Firmencomputer)
  - Beifang: Material im Grenzbereich zur Kinderpornographie (auf Firmencomputer)
  - Beifang: Ausschließlich private Verwendung von Firmencomputern, dabei Verletzung des Urheberrechts
- Vorstand zweifelt neue Vorwürfe an. Klärung durch Präsentation von Auszügen des Beweismaterials zusammen mit RA
- Nach Abschluss des Falles: Anfrage des Aufsichtsrates nach Einsicht in die Beweismittel

Ihre Fragen