Deloitte.

INFOLAW
WWW.INFOLAW.AT

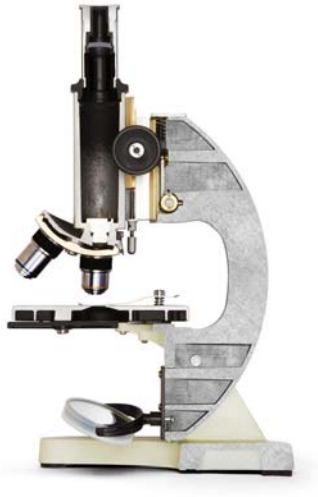
Deloitte Forensic
Forensische Nutzung von IT und Daten

24. Mai 2013

Agenda

- Forensische Untersuchung – Überblick
- Rechtliche Aspekte in forensischen Untersuchungen
- Fallbeispiel: Betriebsspionage / Diebstahl von geistigem Eigentum
- Forensische Untersuchung – eDiscovery

Forensische Untersuchung
Überblick



Korruption
Aktuelle Zahlen und mögliche Begriffsdefinitionen

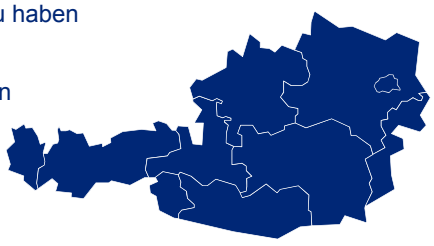
Korruption ist der Missbrauch von anvertrauter Macht zum privaten Nutzen oder Vorteil.

Quelle: Transparency International Austrian Chapter

Korruption ist der Missbrauch einer Vertrauensstellung in einer Funktion in Verwaltung, Wirtschaft oder Politik, um einen materiellen oder immateriellen Vorteil zu erlangen, auf den kein rechtlich begründeter Anspruch besteht.

Quelle: Universität Zürich

- 20% der österreichischen UnternehmerInnen sind überzeugt, durch korrupte Mitbewerbe Aufträge bzw. Kontakte verloren zu haben
- 22% der Unternehmen haben Maßnahmen in ihrem Unternehmen getroffen, um Meldungen von Hinweisgebern entgegen zu nehmen
- Volkswirtschaftlicher Schaden in Österreich bedingt durch Korruption beläuft sich auf ca. EUR 18 Milliarden für das Jahr 2012



Quellen: Transparency International`s Bribe Payers Survey 2012;
Friedrich Schneider „Der Einfluss eines abgeschwächten Wirtschaftsaufschwunges auf die Schattenwirtschaft und Korruption in Deutschland und in Österreich in 2013: Ein erneuter Rückgang"
http://www.econ.jku.at/members/Schneider/files/publications/2013/SchattenwirtschaftKorruption_2013_D_Oe.pdf

Elemente einer (forensischen) Untersuchung

Forensische Untersuchungen

Was

- **Anlassbezogene** oder **präventive Untersuchung** bei Wirtschaftskriminalität:
  - Forensische Untersuchung: anlass- bzw. verdachtsbezogen (z.B. bei Bestechung, Kickback-Zahlungen, Kartellrechtsverletzungen, Unterschlagung)
  - Korruptionsprävention: Compliance- bzw. Good Governance-induziert (z.B. Integrity Due Diligence, Fraud Risk Assessment, Mock Dawn Raid, Pre-Employment Screening)

Warum

- **Beauftragung** einer forensischen Untersuchung:
  - Compliance, Risk- und Reputation-Management
  - Schnelle und zuverlässige Untersuchungsergebnisse
  - Einhaltung der Verwahrungskette (Chain-of-Custody) bei Datensicherung und –verwahrung (Gerichtsverwertbarkeit)
  - Strukturierte und konzise Bereitstellung der Untersuchungsergebnisse
  - Ermittlung durch Behörden (BWB, Staatsanwaltschaft)

Wann

- **Mögliche Auslöser**:
  - Verstoß gegen nationale Rechtsnormen (z.B. Korruptionsstrafrechtsänderungsgesetz, VerbandsverantwortlichkeitsG, Wettbewerbsrecht) und international wirksame Rechtsvorschriften (z.B. FCPA, U.K. Bribery Act)
  - Whistleblowing
  - Gerichtsverfahren
  - Externe und interne Untersuchungen (z.B. durch Interne Revision, Compliance)

Rechtliche Grundlagen

WOLF THEISS

- Annahme: Konkreter Anlassfall, begründeter Verdacht auf Fraud / Compliance-Verstoß
- Datenkategorien
  - Externe Daten (Firmenbuch, Grundbuch, KSV etc)
  - Unternehmensdaten (Rechnungswesen, Zahlungsverkehr, Projektunterlagen etc)
  - Kritisch: Unternehmensdaten mit Personenbezug (E-Mail, Dokumente, Logfiles etc)
  - Kritisch: Private Daten mit Personenbezug
- Betroffene
  - Arbeitnehmer (Einzelpersonen, Abteilungen etc)
  - Dritte (zB Geschäftspartner)

7

Rechtliche Grundlagen

WOLF THEISS

- Kontrollbefugnisse und Persönlichkeitsrechte
  - Pflicht zur Achtung der Privatsphäre des AN als Teil der Fürsorgepflicht des AG
    - Grundrecht auf Datenschutz (unmittelbare Drittwirkung)
    - Art 8 EMRK via § 16 ABGB (mittelbare Drittwirkung)
  - Interessenabwägung anhand des *objektiven*
    - Informations-, Kontroll- und Schutzinteresses des AG
    - schutzwürdigen Geheimhaltungsinteresses der Betroffenen
- Wahrung der Verhältnismäßigkeit und Angemessenheit
- Interventions-, Informations- und Beratungsrechte bzw echte Zustimmungsrechte eines allfälligen Betriebsrats

8

Datenschutz

- Informations- und Kontrollmaßnahmen → Erhebung „personenbezogener Daten“ („*Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist*“, vgl § 4 Z 1 DSG 2000)
- Verarbeitung personenbezogener Daten grs nur unter den im DSG 2000 aufgelisteten Voraussetzungen zulässig, insb
  - Zustimmung
  - Überwiegendes berechtigtes Interesse des Auftraggebers oder eines Dritten

9

Datenschutz

- Zustimmung
  - Frei, ohne Zwang und in Kenntnis der Sachlage
  - Aufgrund Abhängigkeitsverhältnisses Wirksamkeit fraglich
  - Einholung der Zustimmung von Dritten schwer möglich
  - → Datenschutzrechtlich nicht zielführend
- Überwiegendes berechtigtes Interesse an der Durchsuchung von Geschäftskorrespondenz und -dokumenten
  - Geldbußen und Schadenersatzansprüche
  - Abstellen weiterer Angriffe / Compliance-Verstöße
  - Beweissicherung für Verteidigung und etwaige "leniency application“
  - Anhaltspunkte für Regressforderungen gegen Mitarbeiter

10

Datenschutz

- Kein überwiegendes berechtigtes Interesse an der Durchsuchung von Korrespondenz mit privaten Inhalten
  - grundsätzlich unzulässig
  - bei Zweifeln über die Zuordnung ist der Mitarbeiter zu befragen
- „Stufenweise Kontrollverdichtung“ (Rsp/DSK)
  - Stufe 1: Gewährleistung der Systemfunktionalität
  - Stufe 2: Signifikante Abweichungen von „normaler“ IT-Nutzung
  - Stufe 3: Zugriff auf Kommunikationsdaten im begründeten Verdachtsfall
  - Stufen 1 und 2 können auch obsolet sein, wenn Kontrollverdichtung durch andere Maßnahmen bereits eskaliert

11

Datenschutz

- Datenschutzrechtliche Konsequenzen:
  - Zulässigkeit erfordert Trennung in private und geschäftliche Korrespondenz und Dokumente
  - Differenzierung anhand von "key words" zu empfehlen (elektronische Stichwortdurchsuchung)
  - Feinabstimmung im Einzelfall, ggf unter Befragung des Mitarbeiter
- Informationspflicht: Betroffene sind „aus Anlass“ der Ermittlung von Daten (= zum Zeitpunkt der Ermittlung) über den Zweck der Datenanwendung sowie über Name und Adresse des Auftraggebers zu informieren (§ 24 DSG 2000)

12

Datenschutz

WOLF THEISS

- Dienstleistervertrag
  - Forensiker verarbeiten personenbezogene Daten im Auftrag des Auftraggebers und damit als Dienstleister
  - gesetzliche Pflichten des Dienstleisters nach dem DSG näher auszugestalten (§ 14 Abs 2 DSG), hier insb
    - Protokollierung von Zugriffen/Änderungen
    - Dokumentation obiger Maßnahmen

    „Chain of Custody“ / „Digital Case“ → Beweisverwertbarkeit!
- DVR-Meldung
  - *vor* Aufnahme der Datenanwendung
  - „neutrale“ Bezeichnung der Datenanwendung?
  - Rechtsgrundlage (Zustimmung / überwiegendes berechtigtes Interesse)
- Datenübermittlung, insb an Konzerngesellschaften

13

Arbeitsrecht

WOLF THEISS

- Technische Kontrollmaßnahmen, die die Menschenwürde *verletzen* sind jedenfalls unzulässig; unabhängig von allfällige Zustimmung
- Kontrollmaßnahmen, die die Menschenwürde *berühren*
  - Zustimmung des Betriebsrats erforderlich (§ 96 ArbVG)
  - Wenn es keinen Betriebsrat gibt: Individualvereinbarungen mit jedem Arbeitnehmer erforderlich (§ 10 AVRAG)
- Sonstige elektronische Arbeitnehmer-Datenverarbeitungen
  - Zustimmung des Betriebsrats erforderlich (§ 96a ArbVG)
- Kontrollmaßnahmen nicht auf Dauer angelegt oder sonst systematisch → keine BR-Zustimmung notwendig, Informationspflicht
- Einbindung von BR und Datenschutzbeauftragten auch ohne Verpflichtung sinnvoll

14

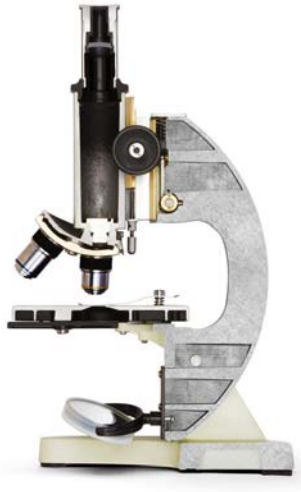
WOLF THEISS

Beweisverwertung

- Forensische Datensicherung zur Verwertung als Beweis im Zivilverfahren
  - Manipulationsgeschützte Beweissicherung und -auswertung
  - Nachvollziehbare Rekonstruktion (Digital Case)
  - Nachvollziehbare Präsentation
- Intrinsischer Beweiswert von elektronische Dokumenten?
  - Digitale Spuren idR nicht manuipulationsresistent
  - Bestreitung der Echtheit, Richtigkeit, Zugang, Zeitpunkt etc

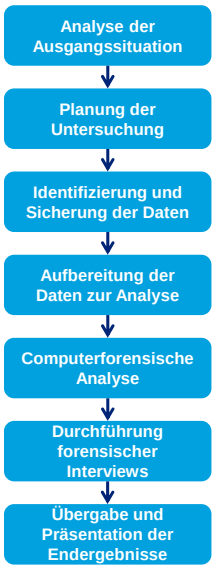
  → Trifft auf konventionelle Beweismittel ebenfalls zu
- Mittel zur Beweiskrafterhöhung (*sound forensic procedure*)
  - Hashes, Signaturen, Zeitstempel,
  - Vier-Augen-Prinzip bei Beweissicherung, Dokumentation
- Kein Beweismethodenverbot iSd Ausschlusses rechtswidrig erlangter Beweise

Fallbeispiel Computerforensik
Betriebsspionage / Diebstahl von geistigem Eigentum



Klient verdächtigt einen Angestellten, geistiges Eigentum an einen Mitbewerber zu verkaufen

- Die IT-Abteilung des Klienten stellte an mehreren Wochenenden außergewöhnlich hohen Datenverkehr im Netzwerk fest; die Ziel-IP-Adresse ist einem Mitbewerber zuzuordnen.
- Die IT-Abteilung informierte den Chief Information Security Officer, der anschließend den Vorstand informierte.
- Der Vorstand möchte den “Vorfall” untersuchen und autorisiert Deloitte Forensic, die Thematik zu untersuchen.



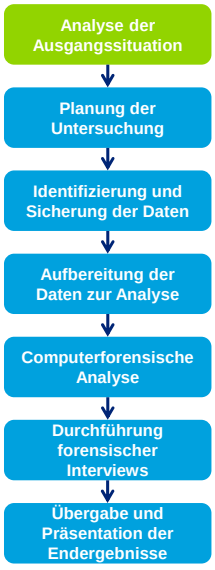
Erstes Meeting zur Einschätzung der aktuellen Situation und zur Planung der sofortigen/zukünftigen Maßnahmen

Erstes Meeting mit dem Klienten, um den aktuellen Status und die weitere Vorgehensweise zu besprechen.

Mögliche Diskussionspunkte sind:

- Welche Informationen hat der Klient bereits (z.B. Name des Mitbewerbers, IP-Adressen, Namen der möglichen Custodians)?
- Welche Maßnahmen wurden vom Klienten bereits durchgeführt und mit welchem Ergebnis?
- Welche Sachverhalte möchte der Klient geklärt wissen?
  - Wurden Daten an den Mitbewerber übermittelt
  - Wer oder was hat die Daten transferiert
  - Über welchen Zeitraum wurden Daten übermittelt

Der Klient verdächtigt zwei Personen (Custodians), Daten weitergegeben zu haben.



Basierend auf dem ersten Meeting wird ein Untersuchungsplan definiert

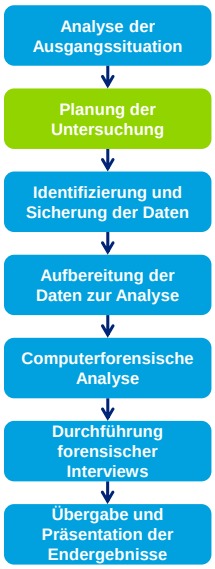
Im Untersuchungsplan werden der Leistungsumfang für den Klienten sowie die durchzuführenden computerforensischen Analysen definiert.

Phase 1: Forensische Datensicherung

– PC-Daten der zwei Custodians
– Live-E-Mail-Postfächer der zwei Custodians, monatliche Backups und E-Mail-Archive
– Alle verfügbaren Log-Dateien

Phase 2: Forensische Untersuchung und Berichterstattung

– Hintergrundrecherche hinsichtlich des Mitbewerbers (z.B. alle registrierten öffentlichen IP-Adressen und Domain-Namen)
– Review der Log-Dateien (wann wurden die Verbindungen zu den IP-Adressen des Mitbewerbers erstellt?
– Computer-/Mobile-Forensic- und eDiscovery-Untersuchung

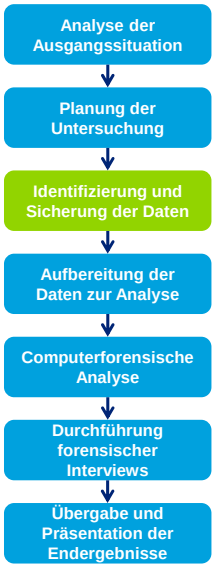


19

Da der Bereich der Datensicherung extrem wichtig und fehleranfällig ist, ist eine akribische Vorbereitung essentiell

– Definition, welche Daten gesichert werden:
  • Kommunikation an den Klienten, welche Daten gesichert werden und welche Ressourcen (Administratoren, Speicherplatz etc.) benötigt werden
  • Sicherstellung, dass nichts übersehen wird
  • Schätzung der Dauer der Datensicherung
– Zusammenstellung der forensischen Formulare, Hard- und Software

Daten, die gesichert werden müssen	Custodian 1	Custodian 2
PC-Daten	Identifikationsnr. 1	Identifikationsnr. 2
Live Mails (MS Exchange)	Identifikationsnr. 3	Identifikationsnr. 4
E-Mail-Backup Oktober 2012	Identifikationsnr. 9	Identifikationsnr. 10
E-Mail-Backup September 2012	Identifikationsnr. 11	Identifikationsnr. 12
Exchange Message Tracking Logs	Identifikationsnr. 5	
Log-Dateien VPN-Gateway	Identifikationsnr. 6	
Physische Zugangsprotokolle	Identifikationsnr. 7	
Log-Dateien Firewall	Identifikationsnr. 8	



20

In dieser Fallstudie wurde die Datensicherung aus Vertraulichkeitsgründen nachts durchgeführt

- Sichern von Notebook-/Desktop-PC-Daten der zwei Custodians
- Extraktion und Wiederherstellung von in Verwendung stehenden E-Mail-Postfächern, E-Mail-Backups und Log-Dateien mit Unterstützung der lokalen IT-Abteilung
- Dokumentation der Datensicherung mittels standardisierter Formulare
- Einhaltung des Vier-Augen-Prinzips durch Mitarbeiter der Rechtsabteilung
- Transfer aller gesicherten Daten in verschlüsselter Form auf die sogenannte Master-Festplatte
- Die Master-Festplatte wird nach Zustimmung des Betriebsrates und unter Einhaltung der Chain-of-Custody an Deloitte Forensic übergeben

Analyse der Ausgangssituation
↓
Planung der Untersuchung
↓
Identifizierung und Sicherung der Daten
↓
Aufbereitung der Daten zur Analyse
↓
Computerforensische Analyse
↓
Durchführung forensischer Interviews
↓
Übergabe und Präsentation der Endergebnisse

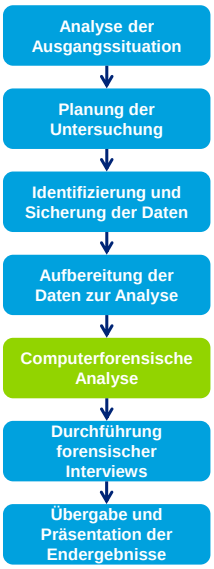
Das Ziel der Datenaufbereitung ist die Sicherstellung einer effizienten/vollständigen Analyse aller gesicherten Daten

- Erstellung einer Arbeitskopie sämtlicher sichergestellter Daten
- Folgende Datenaufbereitungen werden an den gesicherten Notebook-/Desktop-PC-Daten mittels der forensischen Standard-Software EnCase® vorgenommen:
  - Wiederherstellung gelöschter Dateien
  - Extraktion möglicher relevanter Informationen (z.B. Liste an angeschlossenen USB-Sticks oder Benutzern) aus der zentralen Konfigurationsdatenbank von Windows (Registry)
  - Identifikation und Aufbereitung von installierten und ausgeführten Anwendungen
- Import der sichergestellten Log-Dateien in eine zentrale Datenbank (z.B. Microsoft Access)
- Sämtliche sichergestellten Datenbestände werden mittels einer sogenannten eDiscovery-Software (z.B. Nuix, Relativity, Clearwell) indexiert

Analyse der Ausgangssituation
↓
Planung der Untersuchung
↓
Identifizierung und Sicherung der Daten
↓
Aufbereitung der Daten zur Analyse
↓
Computerforensische Analyse
↓
Durchführung forensischer Interviews
↓
Übergabe und Präsentation der Endergebnisse

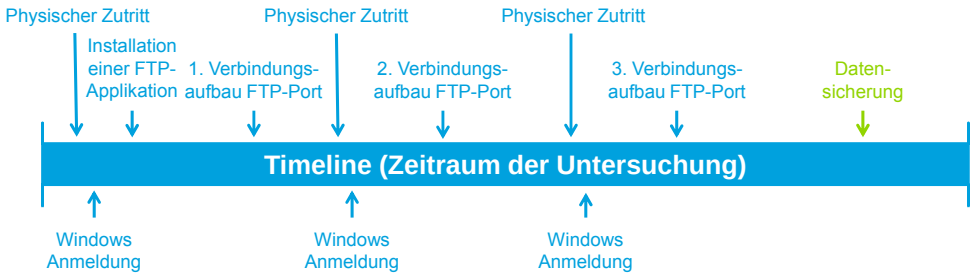
Ziel dieser Analyse ist es, herauszufinden: Durch Wen? Was? Wie? und Wann? an den Mitbewerber übermittelt wurde

1. Durchführung einer Hintergrundüberprüfung des Mitbewerbers, um bspw. öffentliche IP-Adressbereiche und Domain-Namen zu identifizieren
2. Identifikation jener Einträge in den Netzwerkprotokolldateien, welche diese IP-Adressen beinhalten – alle identifizierten Einträge stammen von drei Wochenenden
3. Korrelation Zeitstempel der drei identifizierten Einträge mit:
   - Einträgen in anderen Log-Dateien, welche den physischen Zutritt zum Unternehmen aufzeichnen
   - Einträgen in den Windows Event-Logs, welche bspw. Benutzeranmeldungen protokollieren
4. Analyse der installierten Software-Anwendungen der Notebook-/Desktop-Daten, um mögliche Datentransfer-Anwendungen zu identifizieren (z.B. FileZilla)



Die Erstellung einer Timeline ist ein wichtiges Instrument, um Zusammenhänge möglicher relevanter Ereignisse zu erkennen

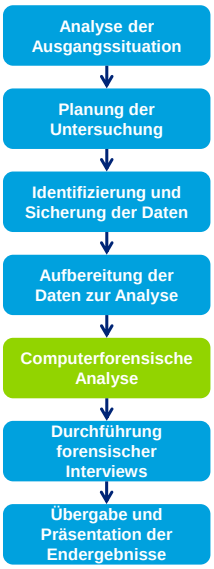
Custodian 1



Ergebnis der Analyse der installierten Applikationen

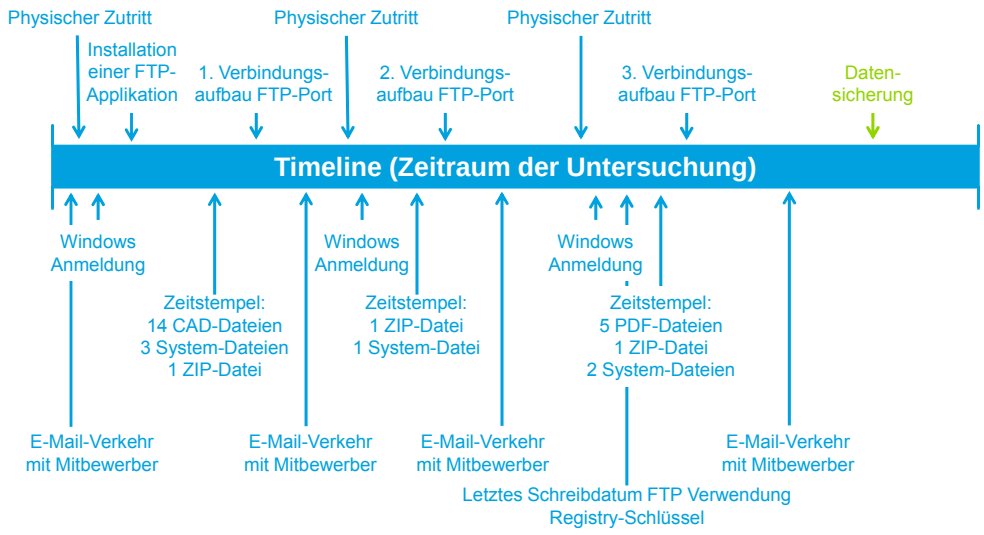
Ziel dieser Analyse ist es, herauszufinden: Durch Wen? Was? Wie? und Wann? an den Mitbewerber übermittelt wurde (fortg.)

5. Analyse von Dateien mit Dateisystem-Zeitstempeln (Erstellung, letzte Änderung oder letzte Modifikation) in zeitlicher Nähe zu den identifizierten Log-Einträgen
6. Review der E-Mails mittels einer vordefinierten Keyword-Liste (z.B. IP-Adresse des Mitbewerbers, Domain-Namen etc.) in der eDiscovery-Software Nuix



Die Erstellung einer Timeline ist ein wichtiges Instrument, um Zusammenhänge möglicher relevanter Ereignisse zu erkennen

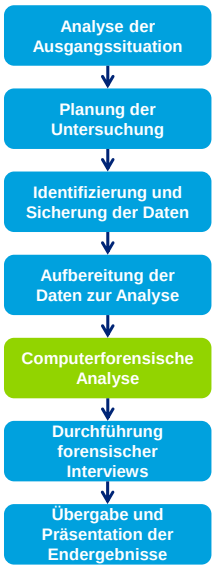
Custodian 1



Ergebnis der Analyse des E-Mail-Verkehrs und der Windows Registry

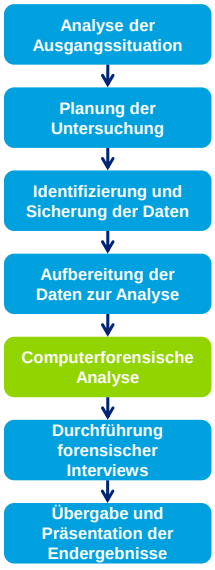
Basierend auf den Analysen wurden relevante Fakten identifiziert, welche darauf hinweisen, dass Custodian 1 Daten an den Mitbewerber transferiert haben könnte

- Die Analyse zeigt auf, dass vor jeder Verbindung zur IP-Adresse des Mitbewerbers, Custodian 1:
  - mehrere E-Mail-Konversationen mit einer E-Mail-Adresse, die vom Mitbewerber ausging, führte (geben starke Hinweise auf Betriebsspionage)
  - das Gebäude betreten hat (basierend auf der physischen Zugangs-Log Datei)
  - sich in seinen/ihren PC geloggt hat (basierend auf Log-Dateien)
  - ZIP-Dateien auf seinem/ihrem PC erstellt hat, welche CAD und PDF-Dateien beinhalteten (basierend auf Dateisystem-Zeitstempel)
  - CAD- und PDF-Dateien auf seinem/ihrem PC geöffnet hat; diese Dateien waren Teil der erstellten ZIP-Dateien



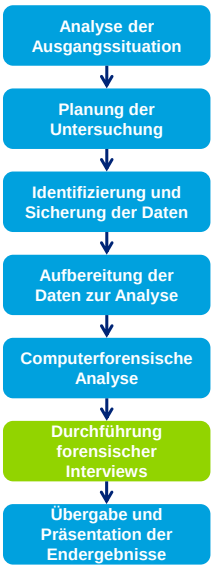
Basierend auf den Analysen wurden relevante Fakten identifiziert, welche darauf hinweisen, dass Custodian 1 Daten an den Mitbewerber transferiert haben könnte (fortg.)

- Es gibt keine direkten Beweise, dass die ZIP-Dateien tatsächlich transferiert wurden
- Eine Analyse dieser ZIP-Dateien durch den Klienten ergab, dass:
  - die Inhalte dieser ZIP-Dateien vertrauliche technische Zeichnungen und Produktbeschreibungen eines zukünftigen Produkts beinhalten
  - Custodian 1 nichts mit diesem zukünftigen Produkt zu tun hat und dass diese Dateien nicht auf seinem/ihrem Computer sein sollten
- Die aktuellen Ergebnisse der forensischen Analyse werden der Rechtsvertretung des Klienten präsentiert
- Der Klient beschließt, basierend auf den bisherigen Ergebnissen, den Vorfall der Polizei zu melden
- Custodian 1 wurde von der Polizei in Untersuchungshaft genommen



In einem forensischen Interview werden die Ergebnisse der Untersuchung Custodian 1 präsentiert

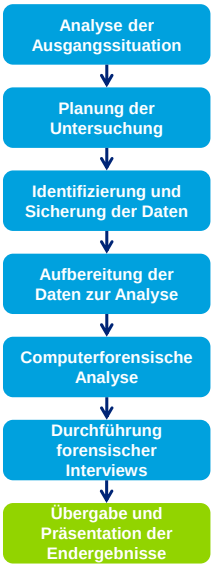
- Das Interview wird im Beisein des Rechtsanwalts von Custodian 1 gemeinsam von einem Rechtsanwalt und Mitarbeitern von Deloitte Forensic geführt
- Custodian 1 ist sehr kooperativ und gibt zu, drei ZIP-Dateien mit vertraulichen Informationen transferiert zu haben; das gesamte Interview wird dokumentiert
- Basierend auf den Ergebnissen unserer Analyse will der Klient Anklage gegen seinen Mitbewerber erheben; Custodian 1 ist bereit, vor Gericht auszusagen



Präzision, Eindeutigkeit, Objektivität, Relevanz und Aktualität sind die Kennzeichen für einen sorgfältigen Bericht

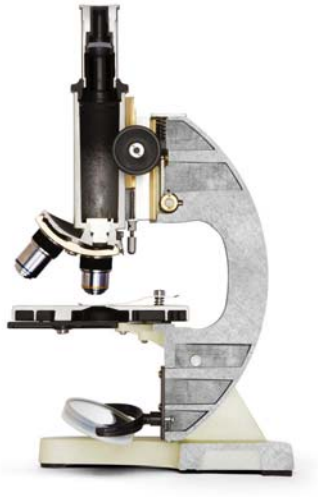
In einem Bericht werden
- die Vorgehensweise der forensischen Datensicherung / Untersuchung
- die Ergebnisse der computerforensischen Analyse und des forensischen Interviews sowie
- jene Fakten, die im Zuge der Untersuchung als relevant identifiziert wurden (z.B. relevante Log-Dateieinträge), präsentiert

Der Bericht muss unter Rücksichtnahme der folgenden Faktoren erstellt werden:
- Präzision
- Eindeutigkeit
- Objektivität
- Relevanz
- Aktualität



Quelle: International Fraud Examiners Manual (2012)

Forensische Untersuchung
eDiscovery



E-Discovery
Allgemein

E-Discovery beschreibt den Prozess der Sammlung (Sicherstellung), Aufbereitung und Durchsicht (Review) jeglicher elektronischer Informationen. Diese Daten umfassen E-Mails, Memos, Briefe, Tabellenkalkulationen, Datenbanken, Präsentationen und andere Dokumente, die auf Computern, Servern, Festplatten, CD/DVD, Handys usw. gespeichert sind.

- Juristen, Prüfer und Analyse-Teams können mithilfe von E-Discovery-Lösungen für Untersuchungen relevante Dokumente finden
- Effiziente Durchsicht eines großen Datenvolumens an elektronischen Dokumenten, da die enorme Menge an zu untersuchenden Dokumenten bei großen Gerichtsverfahren oder Untersuchungen in Unternehmen oftmals die Möglichkeiten traditioneller Untersuchungsansätze sprengt
- Reduzierung des Datenvolumens
  - Semantische Kriterien (Themen-Clustering)
  - Zeitliche Kriterien
  - De-Duplizierung
  - Data Analytics
- Beispiele für Tools: Clearwell, NUIX, Relativity

Vielen herzlichen Dank für Ihr Interesse!

Mag. Karin Mair, CFE
Partner
National Leader Forensic

Deloitte Forensic

Deloitte Financial Advisory GmbH

Renngasse 1 / Freyung
1010 Wien, Österreich

Tel +43 1 537 00 4840
Mobil +43 664 80 537 4840

kmair@deloitte.at
www.deloitte.com/at

Mag. Roland Marko, LL.M.
Counsel
Rechtsanwalt

Wolf Theiss Rechtsanwälte GmbH

Schubertring 6
1010 Wien, Österreich

Tel +43 1 51510 5090
Mobil +43 676 8785 5880

roland.marko@wolftheiss.com
www.wolftheiss.com

Lukas Reiter, MSc
Manager

Deloitte Forensic

Deloitte Financial Advisory GmbH

Renngasse 1 / Freyung
1010 Wien

Tel +43 1 537 00 4884
Mobile +43 664 80 537 4884

lreiter@deloitte.at
www.deloitte.com/at

Deloitte.

WOLF THEISS