Warth & Klein Grant Thornton

An instinct for growth™

IT-Forensik im Unternehmen

Herausforderungen durch Big Data und Beispiele aus der Beratungspraxis

Helmut Brechtken, Associate Partner WKGT

»Big Data – Big Evidence?«

Anwendertag IT-Forensik 2014
Gastvortrag Fraunhofer SIT
Darmstadt - 30. September 2014

Agenda

- **Vorstellung**
- **IT-Forensik:** Definition, Bereiche, Aufgabenstellungen, Datenschutz
  - Beispiel 1 - **Projekt P**: Data Leakage Investigation im Chemiekonzern
- **Incident Response:** Catch the Cracker
  - Beispiel 2 – **Projekt Midnight**: Incident Response bei einem Finanzdienstleister
- **Forensic Investigation + Incident Response**
  - Beispiel 3 – **Projekt X**: Incident Response in einer Raffinerie (**BIG DATA**)
- **eDiscovery**:
  - Beispiel 4 - **Projekt Z**: präventive Kartelluntersuchung in einem Energiekonzern (**BIG DATA**)
  - Beispiel 5 - **Projekt K**: Compliance Investigation „mit Beifang“ (**DIRTY DATA**)

Vorstellung

Warth & Klein Grant Thornton AG Wirtschaftsprüfungsgesellschaft

- 700 Mitarbeiter an 10 Standorten in Deutschland,
- Grant Thornton International mit 33.000 Mitarbeiter in 120 Ländern
- Bereich Governance, Recht, Compliance - GRC

Helmut Brechtken

- Associate Partner, Diplom-Physiker, ISO 27001 Lead Auditor
- IT-Forensik, eDiscovery, IT-Security, Data Analytics
- Leitung Investigation für über 100 Fälle: Incident Response Investigation, Kartelluntersuchungen, eDiscovery, Cybercrime, Data Leakage
- zuvor 6 Jahre bei KPMG, Forensic Technology
- davor 12 Jahre bei Evonik (Degussa): IT Leitung, Data Center, IT-Security, Inhouse Consulting

IT-Forensik und Big Data

Wikipedia:

„Die **IT-Forensik** bzw. *Digitale Forensik* ist ein Teilgebiet der Forensik. 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. Mittlerweile ist die Untersuchung von Computersystemen im Sinne einer inhaltlichen Auswertung der dort gespeicherten Informationen auch im Zusammenhang mit „herkömmlichen“ Straftaten, aber auch für Zwecke der Steuerfahndung etabliert. …“

Gerichtsfestigkeit?

IT-Forensik und Big Data

Wikipedia: „Die **IT-Forensik** bzw. *Digitale Forensik* ist ein Teilgebiet der Forensik. 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. Mittlerweile ist die Untersuchung von Computersystemen im Sinne einer inhaltlichen Auswertung der dort gespeicherten Informationen auch im Zusammenhang mit „herkömmlichen“ Straftaten, aber auch für Zwecke der Steuerfahndung etabliert.

Wesentliches Element der IT-Forensik ist die **Gerichtsfestigkeit** der digitalen Beweismittel und aller folgenden Aktivitäten, d.h. die Daten und Analyseschritte müssen den Anforderungen von Gerichten an Beweismittel genügen. Dies wird durch eine lückenlose und umfassende Dokumentation der Beweismittel (u.a. mit Fotos, Hashing, Vier-Augen-Prinzip, etc.) und aller weiteren Analyseschritte bis zum Ergebnis der forensischen Datenanalyse erreicht. …“

IT-Forensik und Big Data

Wikipedia:

„Big Data bezeichnet Daten-Mengen, die zu groß, oder zu komplex sind, oder sich zu schnell ändern, um sie mit händischen und klassischen Methoden der Datenverarbeitung auszuwerten.

Der Begriff "Big Data" unterliegt als Schlagwort derzeit einem kontinuierlichen Wandel; so wird mit *Big Data* ergänzend auch oft der Komplex der Technologien beschrieben, die zum Sammeln und Auswerten dieser Datenmengen verwendet werden. …“

IT-Forensik

Generell: „Sicherung und Analyse von Daten als Beweismittel“

Kategorien im Unternehmensumfeld

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

IT-Forensik

Generell: „Sicherung und Analyse von Daten als Beweismittel“

Aufgabenstellungen im Beratungsumfeld

- Verdacht auf Straftat (Betrug, Untreue, Unterschlagung, Korruption): Beweise gesucht
- Verdacht auf „undichte Stelle“: Finden und Abstellen
- Verdacht auf Datendiebstahl: Wer?, Was?, Wie?
- Verdacht auf Steuervergehen: Beweise gesucht
- Kartelluntersuchungen: reaktiv oder besser präventiv?
- eDiscovery

Klassik vs. Trends

Klassische Bereiche der IT-Forensik

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

Klassik vs. Trends

Trends und neue Felder

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

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 möglich unter Einhaltung aller rechtlichen Vorgaben
- Umsetzung der Lösung manchmal mühselig und zeitaufwändig (Involvierung RA, DSB, BR, LA, Berücksichtigung Policies, Anonymisierung), aber letztendlich meistens möglich

Fallbeispiel (1/5): Projekt P

Projekt P – chemische Industrie, internationaler Konzern

Data Leakage Investigation: **brisante Personalinformationen** aus dem engstem Führungskreis (2 Vorstände + Vorsitzender Aufsichtsrat) steht **in der Zeitung!**

Investigation und Analyse der Prozesse.

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

Incident Response

Besonderheiten Incident Response: „Catch the cracker“

- Schnelle Reaktion notwendig
- Schadensminimierung und Schließen der Lücke bei Erhalt der Beweise
- Verhältnis Innen/Außentäter ~ 50/50
- Gute Kenntnis großer Infrastrukturen, Applikationen und Netzwerke notwendig
- Balance zwischen Aufklärung und operativem Betrieb

Fallbeispiele (2/5): Projekt Midnight

Finanzbranche

Einbruch ins Netzwerk festgestellt. Der Cracker war 57 Stunden im Netz.
Fragestellung:

- **Wie war das möglich?**
  - Zugang über den schwach gesicherten VPN-Zugang mit einem Zugangsaccount und festem Passworts (~ 1 Faktor, dafür aber statisch).
- **Wer wars?**
  - Spur des Crackers führt zu einem Webhoster nach USA, Nachverfolgung mit oder ohne Anzeige aussichtslos.
- **Welche Systeme & Daten konnte der Angreifer kompromittieren?**
  - Spuren analysiert, betroffene Systeme identifiziert: nach Knacken eines internen Accounts war der Zugriff auf eine Vielzahl von internen Systemen möglich (Entwicklung, Test, Webserver, Knowledge Base, **Integrations- und Produktivsystem der zentralen Account-Datenbank**)

Fallbeispiel (2/5): Projekt Midnight

- **Wurden Daten aus dem Netzwerk transferiert?**

  Detaillierte Nachstellung der Zugriffe auf die Datenbankserver. Ergebnis: Es gab mehrere Versuche, den kompletten Datenbankinhalt zu transferieren. Diese blieben jedoch erfolglos, weil das notwendige Knowhow (SQL-Queries „select * from bla where blabla“) offenbar nicht vorhanden war!

  Konsequenz: **Haarscharf am Desaster vorbei** – sonst Meldung an UK FSA (Financial Services Authority = Bafin in DE) mit weitreichenden Konsequenzen: Informationspflicht an alle Kunden, nach Überprüfung des Vorfalls und Umgang mit IT-Security sicher auch Verlust der Banklizenz.

Forensic Investigation / Incident Response

Besonderheiten Forensic Investigation

- CI / Background Recherche
- Fraud Triangle: Gelegenheit – Motivation - Rechtfertigung
- Profiling
- Forensische Interviews (mit oder ohne Rechtsanwälte)
- Analyse der Finanzdaten

Fallbeispiel (3/5): Project X

Project X

- Industrieunternehmen, ca. 350 Mitarbeiter, Rohstoffe
- berichtet 13 Vorfälle / Störungen im Netzwerk April – August 2013
  - Ausfall Fileserver (2x)
  - Ausfall Logistiksystem (3x) (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

Fallbeispiel (3/5): Project X

Untersuchungsplan:

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

- Geplant: Undercover Untersuchung

Fallbeispiel (3/5): Project X

Durchführung (September 2013 bis März 2014):

- 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 (3/5): Project X

Ergebnis:

Fall ist 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,

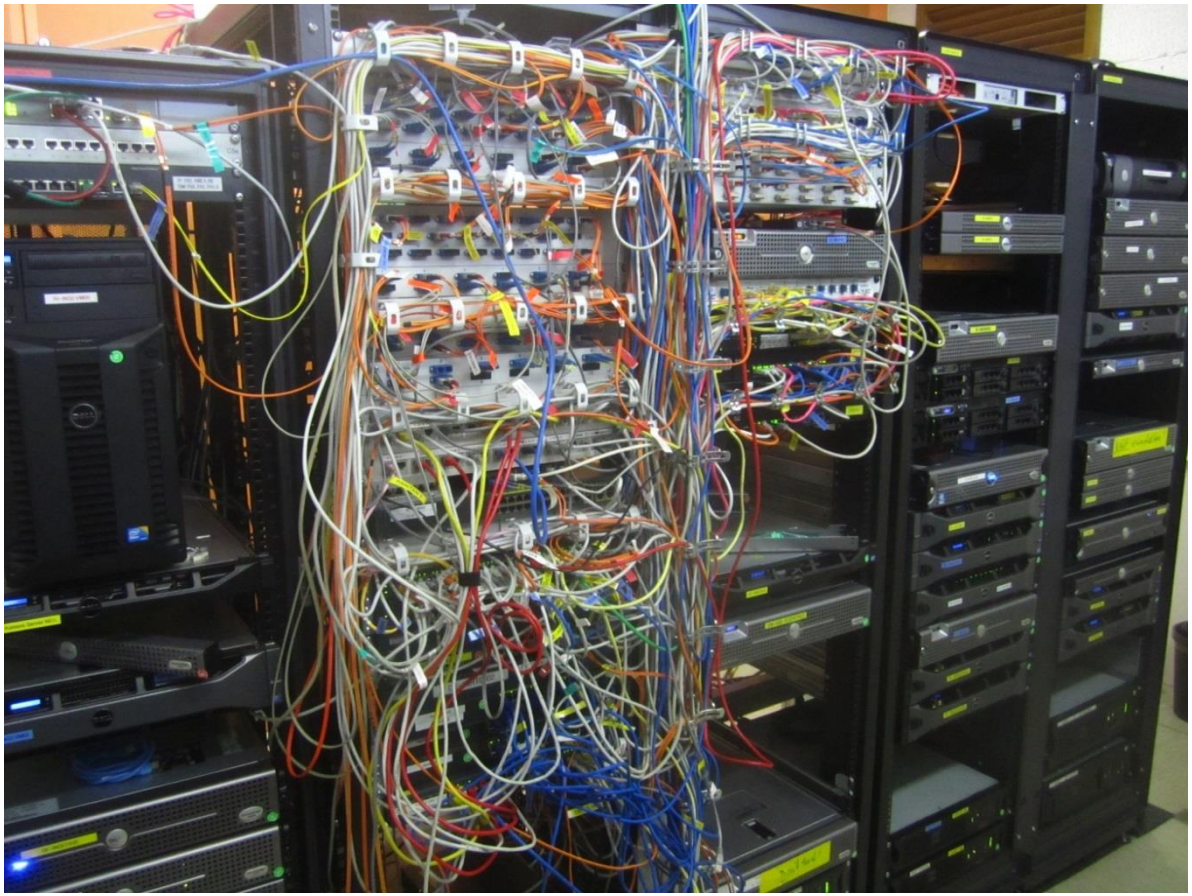
Policies, etc. pp.

Technisch:

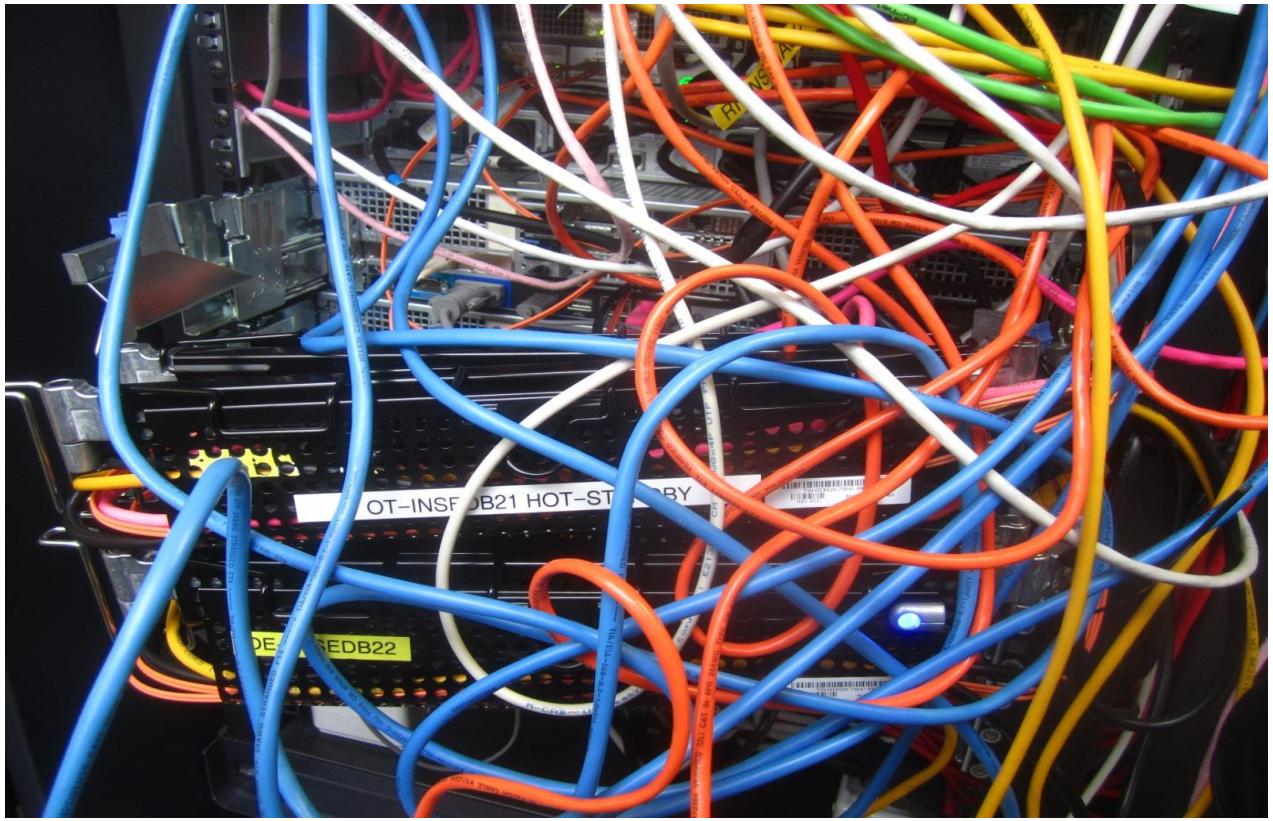
IT-Security (Account Mgmt, Passwörter),
AV,
Patching,
Backup,
Internet GW

Fallbeispiel (3/5): Project X

Fallbeispiel (3/5): Project X

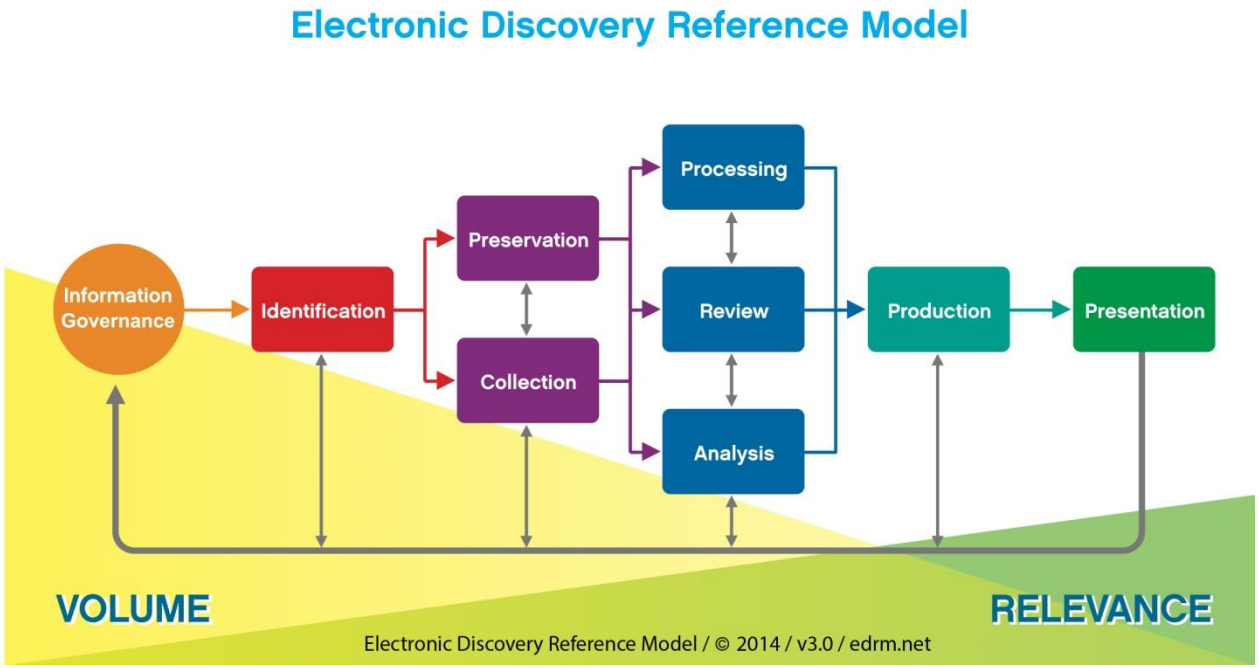


Fallbeispiel (3/5): Project X



Grant Thornton | An instinct for growth™

eDiscovery



Besonderheiten eDiscovery

- Auslöser: angloamerikanisches Rechtssystem
- große Mengen unstrukturierte Beweismittel
- geordneter, nachvollziehbarer Prozess der Qualifizierung
- meist Kooperation IT-Forensik mit Rechtsanwälten als „Reviewer“

Fallbeispiel (4/5): Projekt Z

Projekt Z

- Energiesektor, Konzern
- Projektziel: Identifizierung aller kartellrechtlich relevanten Dokumente in einem Geschäftsbereich.
- eDiscovery von 120 Mitarbeitern: 16 TB Daten - **BIG DATA**
- Entwicklung spezifischer Collector, Handling verschlüsselter Daten
- Datentransfer mittels 60 High-Security HD

Fallbeispiel (4/5): Projekt Z

- **BIG DATA** (16 TB): weitere Verarbeitung nur vollständig automatisiert und 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
  - **21 Mio € Anwaltskosten**

- Einsatz von Keyword-Search und **Künstlicher Intelligenz** - KI - zur computergestützten Datenanalyse
- Ergebnis: 80.000 Doks zum Review (300.000 € Anwaltskosten, 1,4 %)

Fallbeispiel (5/5): Projekt K

Project K

Vorwurf: Mobbing.

- Telekommunikationsanbieter in Polen
- Starker Verdacht auf Mobbing durch 4, z.T. leitende, Mitarbeiter
- Konzertierte Aktion am Stichtag mit Security, RA, Aufsichtsrat, IT-Forensik, Forensik aus Polen: Freistellung der MA, Konfiszierung der IT-Geräte und Smartphones
- Forensische Analyse 7 Notebooks und 9 Smartphones
- eDiscovery der vorgefunden eMails und Dokumente

Fallbeispiele (5/5): Projekt K

- Ergebnis:
  - **Mobbing bestätigt**
  - **7 weitere Mitarbeiter** durch eMail-Kommunikation **belastet**
  - Austausch **pornografischen Materials** (über Firmencomputer - **DIRTY DATA**)
  - 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 zweifelte neue Vorwürfe an. Klärung durch Präsentation von Auszügen des Beweismaterials zusammen mit RA
- Nach Abschluss des Falles: Anfrage des Aufsichtsrates, möchte ebenfalls Einsicht in die Beweismittel

Ihre Fragen

Kontakt

Helmut Brechtken

Associate Partner, Diplom-Physiker

Certified ISO/IEC 27001 Lead Auditor

Business Risk / Forensic Services / IT Analytics & Security

T +49 211 9524 8576
F +49 211 9524 594
M +49 177 8952 466
E helmut.brechtken@wkgt.com

Warth & Klein Grant Thornton AG
Wirtschaftsprüfungsgesellschaft
Rosenstraße 47
40479 Düsseldorf

GRC www.wkgt.com/services/wirtschaftspruefung/governance-risk-compliance

WWW www.wkgt.com

Grant Thornton | An instinct for growth™

Warth & Klein Grant Thornton AG
Wirtschaftsprüfungsgesellschaft

Warth & Klein Grant Thornton AG ist eine Mitgliedsfirma von Grant Thornton International Ltd (Grant Thornton International).

Die Bezeichnung Grant Thornton bezieht sich auf Grant Thornton International oder eine ihrer Mitgliedsfirmen. Grant Thornton International und die Mitgliedsfirmen sind keine weltweite Partnerschaft. Jede Mitgliedsfirma erbringt ihre Dienstleistungen eigenverantwortlich und unabhängig von Grant Thornton International oder anderen Mitgliedsfirmen.

wkgt.com

Aachen
Warth & Klein Grant Thornton AG
Wirtschaftsprüfungsgesellschaft
Laurentiusstraße 16-20
52072 Aachen
T +49 241 70508 50
F +49 241 70508 59

Dresden
Warth & Klein Grant Thornton AG
Wirtschaftsprüfungsgesellschaft
Schubertstraße 41
01307 Dresden
T +49 351 31821 0
F +49 351 31821 635

Düsseldorf
Warth & Klein Grant Thornton AG
Wirtschaftsprüfungsgesellschaft
Rosenstraße 47
40479 Düsseldorf
T +49 211 9524 0
F +49 211 9524 200

Frankfurt a.M.
Warth & Klein Grant Thornton GmbH & Co. KG
Wirtschaftsprüfungsgesellschaft
Ulmenstraße 22
60325 Frankfurt a. M.
T +49 69 905598 0
F +49 69 905598 677

Hamburg
Warth & Klein Grant Thornton AG
Wirtschaftsprüfungsgesellschaft
Kleiner Burstah 12
20457 Hamburg
T +49 40 4321862 0
F +49 40 4321862 49

Leipzig
Warth & Klein Grant Thornton AG
Wirtschaftsprüfungsgesellschaft
Springerstraße 11
04105 Leipzig
T +49 341 59083 0
F +49 341 59083 733

München
Warth & Klein Grant Thornton AG
Wirtschaftsprüfungsgesellschaft
Ganghoferstraße 31
80339 München
T +49 89 36849 0
F +49 89 36849 4299

Stuttgart
Warth & Klein Grant Thornton GmbH & Co. KG
Wirtschaftsprüfungsgesellschaft
Jahnstraße 6
70597 Stuttgart
T +49 711 16871 0
F +49 711 16871 40

Viersen
Warth & Klein Grant Thornton AG
Wirtschaftsprüfungsgesellschaft
Eindhovener Straße 37
41751 Viersen
T +49 2162 91811 0
F +49 2162 91811 60

Wiesbaden
Warth & Klein Grant Thornton GmbH & Co. KG
Wirtschaftsprüfungsgesellschaft
Hagenauer Straße 59
65203 Wiesbaden
T +49 611 18890 0
F +49 611 260133