Deloitte.

Aktuelle Trends im Cybercrime mit Fallbeispielen aus der digitalen Forensic

Deloitte GRC Espresso – 18. Oktober 2023

Agenda

- Vorstellung des Referenten
- Aktuelle Trends & hybride Bedrohungslage
- Ein Blick in die Praxis: Fallbeispiele aus forensischen Untersuchungen
- Empfehlungen

Vorstellung des Referenten

Vorstellung des Referenten

Helmut Brechtken

Partner
Head of Digital Forensic Incident Response

Diplom-Physiker
Certified ISO/IEC 27001 Lead Auditor

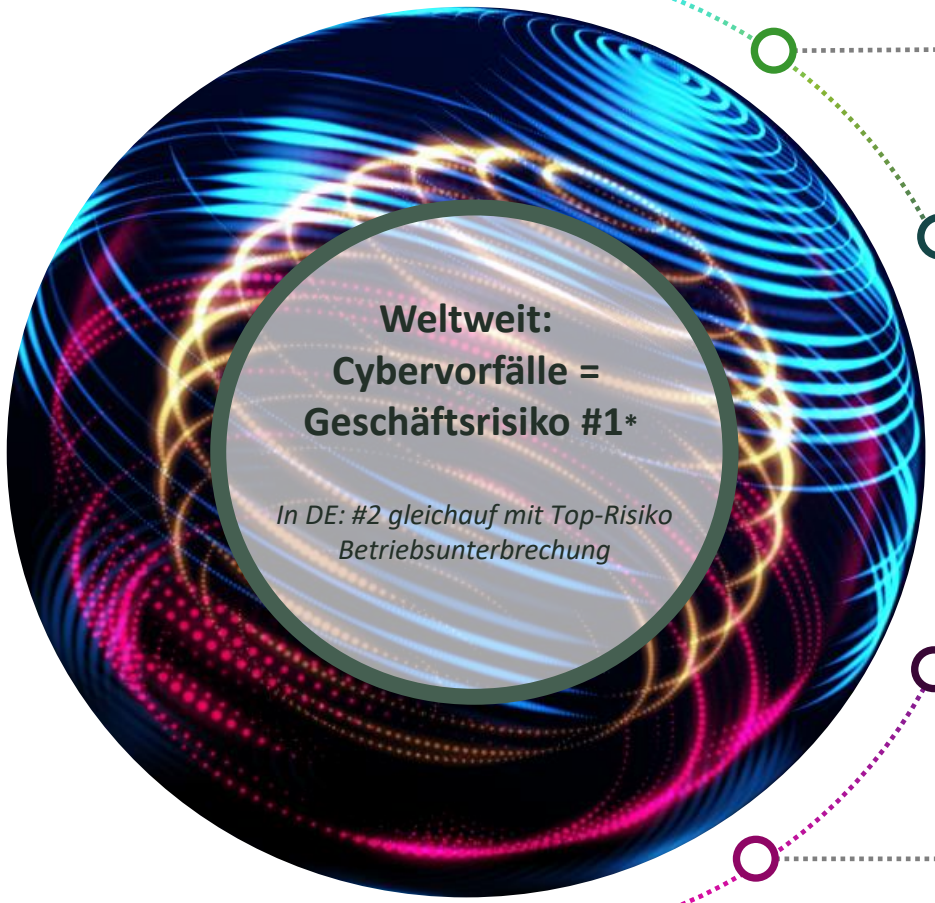
Helmut Brechtken ist Partner in der Service Line Forensic bei Deloitte und verfügt über mehr als 25 Jahre Berufserfahrung in der Beratung und der chemischen Industrie.

Er hat bereits über 300 Untersuchungen und Projekte zur digitalen Forensik und Cyber Incident Response geleitet.
Er verfügt über umfangreiche Erfahrung bei der Durchführung von komplexen eDiscovery-Verfahren aus nationalen und internationalen Investigationen, wie bspw. Investigations des US-Department of Justice (DoJ) und der US Securities and Exchange Commission (SEC).

Aktuelle Trends im Cybercrime

Aktuelle Trends

Gefährdung durch Cybercrime in Deutschland



Zero Day Exploits

z. B. Microsoft Exchange Exploit, Log4J Exploit

Innovative Ransomware

Ausweitung cyberkrimineller Erpressungsstrategien, neue Gruppierungen, Rebranding

Cybercrime: Ransomware V5

Data Leakage Investigation

Bankdatenbetrug

z. B. Phishing, Man in the Middle-Angriffe, Fake Invoices

Gefährdung durch Cyber-Warfare

*Allianz Risk Barometer 2023: *Quelle: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html*

Aktuelle Trends

Gefährdung durch Cybercrime in Deutschland

Innovative Ransomware

Die Evolution der Cybererpressung

Die Evolution der Cybererpressung seit ca. 2018

Traditionell (V1)	Erpressung durch **Verschlüsselung der Daten**
V2	+ Zerstörung der Backups
V3	+ Datenausleitung
V4	**Datenausleitung OHNE** Verschlüsselung, Erpressung **durch Drohen mit Datenveröffentlichung**
V5 - aktuell	**Datenausleitung OHNE** Verschlüsselung, Erpressung **des Target UND der Datenowner mit Datenveröffentlichung**
V6 - ???	

Zu beachten:

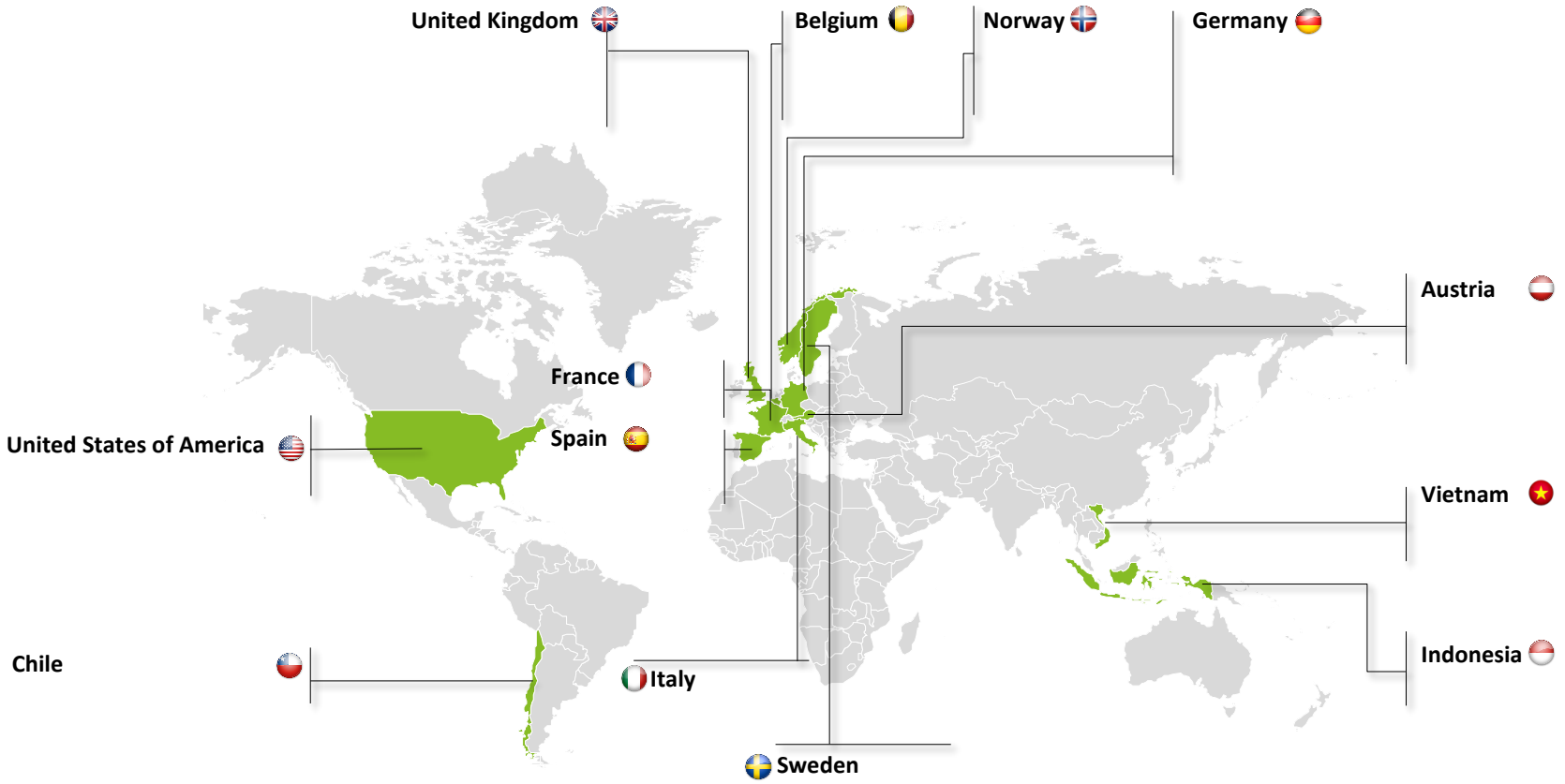
- Ggf. Strafanzeige
- Risiko Straftatbestand / ggf. Strafen bei Lösegeldzahlung

Ein Blick in die Praxis: Erfahrungsberichte aus aktuellen Investigations Data Leakage Investigation

Erfahrungsberichte aus aktuellen Investigations

Data leakage Investigation

- A total of over **1 TB** of data was exfiltrated from 20+ servers.
- Around **700 GB (~ 700.000 Files)** were published on the Darknet.
- The criminals provided a list of the published data („File-Listing“).
- In Data Leakage scenarios legal requirements demand the notification of all people whose personal data was affected.
- To that end, a review of the leaked data is necessary to be able to identify the concerned persons and their published information.



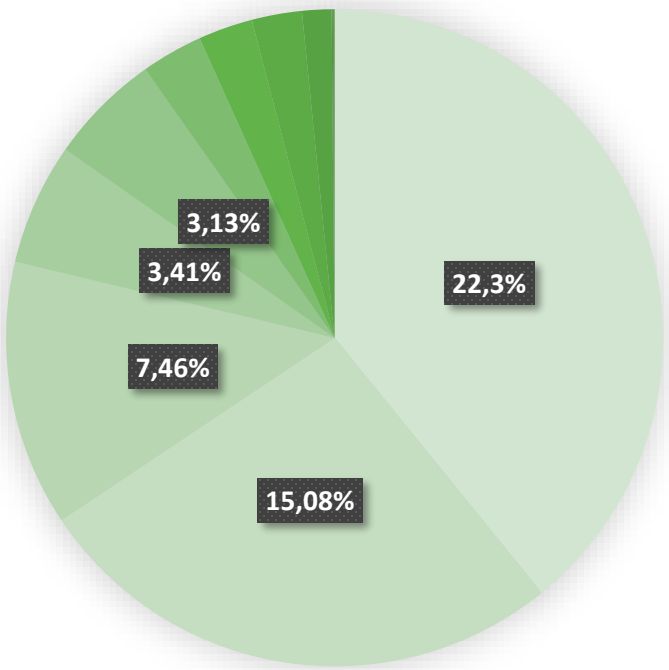
Overview

Data distribution per Risk category distribution and languages

As several servers from different countries were affected the review demanded for several languages.

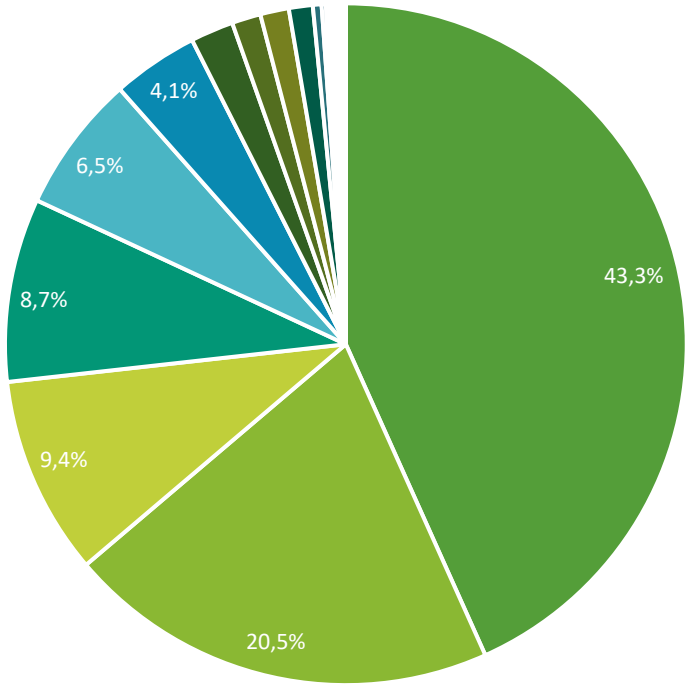
Thus, for the top 10 languages of the documents PII search terms had to be created. Additionally, reviewers for all concerned languages had to be contracted.

Distribution of Top Risk Categories



- Other Personal Data
- Core employment-related Documents (without CV)
- Identity Data of Individuals
- Health Data of Individuals
- Identity Misuse Data
- Bank/Financial Data of Individuals
- Other Personal Data – Minors
- Full Resume/CV
- Labour Union Affiliation
- Religious, Political or Philosophical Data
- Criminal Background Data
- Ethnicity Data
- Data on Sexuality and Sexual Identity

Language Distribution Top 10



- English
- German
- Other
- Italian
- French
- Spanish
- Dutch
- Swedish
- Norwegian
- Catalan
- Danish

Ein Blick in die Praxis: Erfahrungsberichte aus aktuellen Investigations Bankdatenbetrug

Erfahrungsberichte aus aktuellen Investigations

Ein falscher Klick führt zu einer ungewollten Datenausleitung und Geldtransaktion

Risiko Mensch

Risiko von außen

Der Fall

- Wir erklären anhand eines **Phishing-Angriffs**, den ein Unternehmen aus dem Bereich Wirtschaftsprüfung/Steuerberatung erlitt, wie der initiale Angriff zu einer **Datenausleitung von E-Mail-Daten** sowie zu einer **unautorisierten Transaktion i. H. v. 450.000 EUR** führte.

Die Betrugsstrategie

Phishing E-Mail

Ein Mitarbeiter gibt sein Passwort auf einer Website ein:

Es folgt eine Fehlermeldung

Nach Rücksprache mit dem vermeintlichen Absender erfolgt ein Reset des Passworts

Der IT-Dienstleister führt einen Scan mit der Antivirenlösung durch:

Keine Auffälligkeiten

Man-In-The-Middle-Attack

6 Monate später

Dem Mitarbeiter fallen unerklärliche Antwortmails auf:

Zustellfehler-meldungen

Die Analyse ergibt:

In dem E-Mail-Postfach ist eine **Weiterleitungs-regel** aktiv

Die Detailanalyse zeigt:

In 6 Monaten wurden ca. **20.000 E-Mails ausgeleitet**

Meldung an die Datenschutzbehörde

Transaktion: 450.000 EUR

Erfahrungsberichte aus aktuellen Investigations

Unzureichende technische Absicherung ermöglicht Durchführung eines Bankdatenbetrugs

Risiko System

Der Fall

- Wir zeigen anhand eines **Bankdatenbetrugs in der Finanzbrache**, wie eine unzureichende technische Absicherung zu einer zweifachen Wiederholung eines Angriffsmusters und einem **Gesamtschaden von knapp 3 Millionen EUR** führte.

Die Betrugsstrategie

Ein Unternehmen nutzt Cloud-Services, die durch einen Faktor (Credentials) abgesichert sind

Angreifer erbeuten durch Phishing die **Credentials des CFO** des Unternehmens

Gemäß IKS müssen Zahlungen ab 1 Mio. EUR durch CFO-Approval freigegeben werden

Angreifer schleusen manipulierte Rechnungen per E-Mail ein, u.a. eine **Rechnung über 1.6 Mio. EUR**

Aus dem O365-Account des CFO wird die Rechnung von den Angreifern freigegeben

Erste Transaktion (USA): 1.6 Mio. EUR

Die Freigabe ist für die Beteiligten des Unternehmens nicht als Betrug zu erkennen.

Es erfolgt eine Wiederholung des Angriffs, eine Rechnung i. H. v. 1.2 Mio. EUR wird freigegeben.

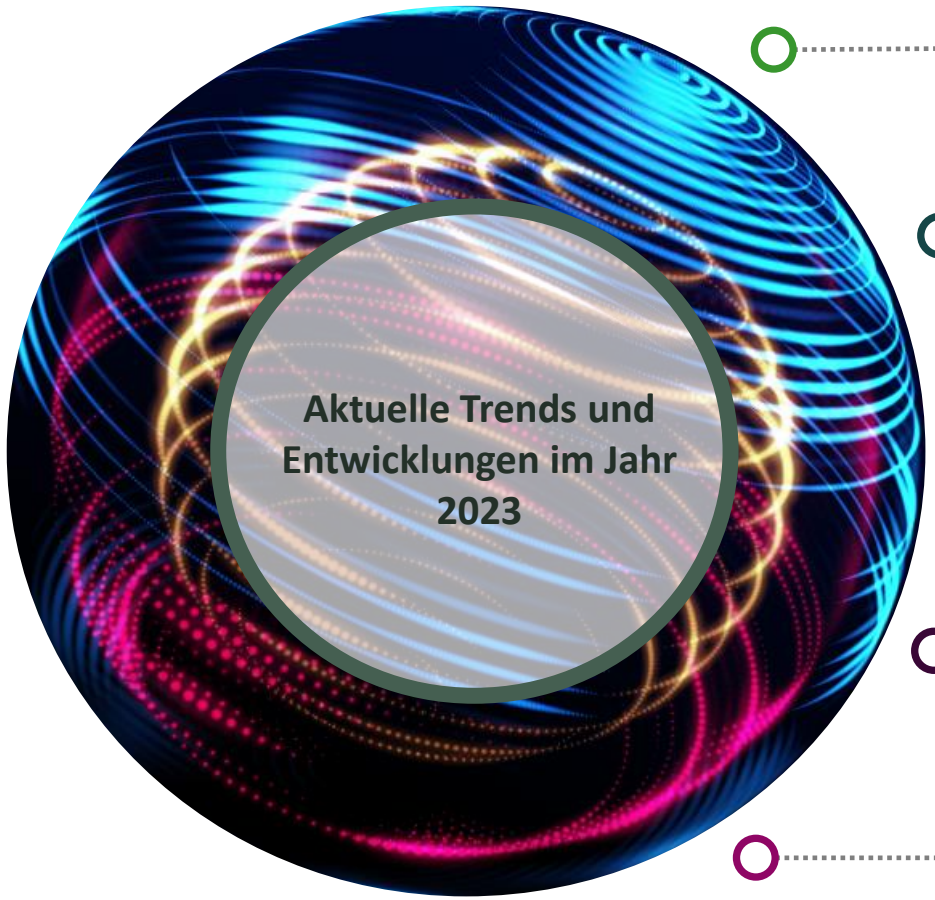
Zweite Transaktion (Asien): 1.2 Mio. EUR

Betrug fällt auf & wird gemeldet

Empfehlungen

Financial Fraud und Cybercrime Trends in 2023

Unsere Wahrnehmung



	Trend	Costs
Payment Diversion Fraud ***(Bankdatenbetrug)*** *Betrüger spionieren E-Mail-Kommunikationen aus und teilen mit, dass sich die Bankverbindung geändert hat.*	→	€€€
CEO Fraud ***(Fake President Fraud, „Chef-Masche“)*** *Ein Betrüger gibt sich als Chef aus und fordert Mitarbeiter zu Handlungen auf (z. B. Überweisung)*	↘	€€€
Ransomware ***(Verschlüsselungs-/Erpressungstrojaner)*** *Angreifer erpressen, indem sie zur Entschlüsselung bzw. Nichtveröffentlichung von Daten ein Lösegeld fordern.*	↘ ↗	€ - €€€
Advanced Persistent Threat **(Komplexe Malware)** *Angreifer führen ausgefeilte, zielgerichtete Angriffe durch (z. B. um Daten und Zugangsdaten zu stehlen).*	→	€€€
Insider Fraud ***(Bedrohung von innen)*** *Ein Betrüger mit autorisiertem Zugriff in einer Organisation missbraucht diesen, um wichtige Informationen oder Systeme negativ zu beeinflussen.*	→	€ - €€€

Empfehlungen zur wirksamen Cybercrime-Prävention
Ganzheitlicher, unabhangiger & nachhaltiger Ansatz

1

Häufig ähnliche Angriffsvektoren und Schwachstellen

Bei der forensischen Untersuchung von Cybercrime-Angriffen werden häufig die gleichen ~5 Schwachstellen ausgenutzt (fehlende Cyber Awareness, kein MFA, ungepachte OS + Altsysteme, keine Offline-Backup, IKS-Schwächen).

2

Prävention: Durchführung von Cyber Security Assessments

1. Ganzheitliches & unabhängiges Cyber Security Assessment: Mensch + Organisation, Prozesse, Technik
2. Nachhaltige Beseitigung von Schwachstellen

3

Schutz durch Cyber Incident Response CIR & Digital-Forensische Incident Response DFIR

1. Cyberversicherung oder Rahmenverträge für CIR & DFIR sichern sehr kurzfristige Unterstützung im Angriffsfall (24x7 global, 2h)
2. Schnelle Beendigung des Angriffs, Minimierung des Business Impact, Digital-Forensische Aufklärung und Frage Datenausleitung
3. Inkl. Krisenmanagement, Krisenkommunikation, Vermittlung rechtlicher Beratung

Kontakt

Helmut Brechtken

Partner - Forensic Technology

Helmut Brechtken
- Partner - Financial Advisory
- Head of Digital Forensic Incident Response Köln/Düsseldorf
- Phone +49 221 9732 4949
- Mobile +49 1515 4484 223
- Mail hbrechtken@deloitte.de

Helmut Brechtken ist Partner im Bereich Financial Advisory von Deloitte Deutschland und verfügt über 25 Jahre Berufserfahrung.

Ausbildung und Berufsabschlüsse

- Diplom-Physiker – Julius-Maximilians-Universität Würzburg
- Certified ISO/IEC 27001 Lead Auditor

Sprachkenntnisse

- Deutsch – Muttersprache
- Englisch – verhandlungssicher

Relevante Berufserfahrung

Als Head of Digital Forensic Incident Response (DFIR) ist er verantwortlich für Projekte zur forensischen Aufklärung von Cybercrime-Angriffen und dem Einsatz von Digitaler Forensik in forensischen Sonderuntersuchungen. Zudem hat er Mandanten zur Cyber-Security-Prävention und der Einführung bzw. Weiterentwicklung von ISMS betreut. Er verfügt über Erfahrung bei der Durchführung von komplexen eDiscovery-Verfahren aus nationalen und internationalen Investigations. Helmut Brechtken besitzt neben seiner langjährigen Tätigkeit in der Beratung/Wirtschaftsprüfung über Berufserfahrung im Management von IT-Operations und IT-Security in der chemischen Industrie.

Relevante Projekterfahrung

- Beratung von Mandanten aus verschiedenen Branchen im Zusammenhang mit Cybercrime-Angriffen (Ransomware, Netzwerkausfälle, Bankdatenbetrug, Sabotage etc.) und Leitung der digital-forensischen Untersuchung
- Implementierung der digitalen Forensik im Rahmen von forensischen Ermittlungen
- Beratung von Mandanten bei der Planung und Umsetzung von eDiscovery in forensischen Ermittlungen, kartellrechtlichen Ermittlungen oder anderen Gerichtsverfahren
- Beratung von Mandanten bei Cybercrime-Attacken und Beratung zur präventiven Cybersicherheit zur Vermeidung von Cyber-Vorfällen
- Beratung von Mandanten bei der Einführung von Informationssicherheits-Managementsystemen (ISMS, z.B. ISO 27001)

Lena Gehrig

Managerin - Forensic Technology

Lena Gehrig
- Managerin Financial Advisory - Digital Forensic Incident Response (Köln/Düsseldorf)
- Phone +49 221 97324103
- Mobile +49 160 90396411
- Mail lgehrig@deloitte.de

Lena Gehrig ist seit September 2023 Managerin im Bereich Financial Advisory bei Deloitte Deutschland mit >3 Jahren Berufserfahrung im Business Development und internationalen Projektmanagement.

Ausbildung und Berufsabschlüsse

- M. A. – International Management and Marketing, RFH Köln
- Certified Incident Handler (ECIH)

Sprachkenntnisse

- Deutsch – Muttersprache
- Englisch – verhandlungssicher
- Spanisch – Grundkenntnisse

Relevante Berufserfahrung

Lena Gehrig unterstützt Mandanten im Kontext komplexer Digitalforensik und vollumfänglicher Präventionsservices. Sie widmet sich Projekten zur forensischen Aufklärung von Cybercrime-Angriffen (Hackerangriffen) und dem Einsatz von digitaler Forensik in forensischen Sonderuntersuchungen einschließlich des notwendigen Krisenmanagements und der Krisenkommunikation. Lena Gehrig verfügt über mehrjährige Berufserfahrung im Business Development im Umfeld von E-Health-Unternehmen und ist spezialisiert auf das Gesundheitswesen. Darüber hinaus war sie mit Prozess- und Anforderungsmanagement in diversen übergreifenden sowie internationalen Projekten betraut.

Deloitte.