



## Digital Forensic Incident Response (DFIR)

Deloitte unterstützt und begleitet Sie weltweit im Fall von Cybercrime-Angriffen und Wirtschaftskriminalität. Wir stehen Ihnen rund um die Uhr zur Seite – mit Incident Response und Krisenmanagement über die digital-forensische Aufklärung eines Cybersicherheitsvorfalls bis hin zur Wiederherstellung Ihrer Geschäftsprozesse und IT-Umgebung.

Unternehmen aller Branchen und Größen sowie öffentliche Einrichtungen sind mit einer steigenden Zahl von Cyberkriminalitätsfällen konfrontiert, die sich schnell weiterentwickeln und immer professioneller und komplexer werden. Cybercrime-Angriffe wie Ransomware, Network Intrusion, Bankdatenbetrug und Data Leakage sind oft erfolgreich, den betroffenen Unternehmen und Organisationen drohen schwerwiegende Folgen wie Betriebsunterbrechungen, finanzielle Verluste, Vertragsstrafen, Geldbußen, Reputationsschäden und Veröffentlichung oder Missbrauch sensibler Unternehmensdaten.

Neben gezielten Angriffen auf Unternehmen und Organisationen stellen auch Straftaten in diesen, wie zum Beispiel Datendiebstahl durch Innentäter\*, eine ernsthafte Bedrohung dar. Häufige sind sensible Unternehmensdaten betroffen und die Kompromittierung kann zu gravierenden Folgen für die Wirtschaftlichkeit oder zu Bußgeldern durch die Datenschutzbehörden führen.

Richtig auf solche Krisen und Internetkriminalität zu reagieren und diese zu überwinden wird im digitalen Zeitalter immer wichtiger und stellt eine Kompetenz dar, die entscheidend für den Geschäftserfolg ist.

Wir unterstützen Sie beim Umgang mit Cybersicherheitsvorfällen aller Art und beraten Sie von Beginn bis zum Abschluss des Vorfalls als Ihr kompetenter und verlässlicher Partner – und das weltweit. Durch die sofortige Schließung von Sicherheitslücken, die Rekonstruktion des Tathergangs sowie die Daten- und Systemwiederherstellung können wir dabei unterstützen, finanzielle und operative Schäden auf ein Minimum zu reduzieren und schnellstmöglich zum normalen Geschäftsbetrieb zurückzukehren. ➔

\* Aus Gründen der besseren Lesbarkeit gelten sämtliche Personenbezeichnungen gleichermaßen für alle Geschlechter

### Deloitte als zertifizierter Dienstleister

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) hat Deloitte geprüft und empfiehlt uns als „qualifizierten Dienstleister für APT-Response (Advanced Persistent Threat)“<sup>1</sup>.

### Unsere Services

#### Digital Forensic Incident Response

Unsere erfahrenen Experten für Digital Forensic Incident Response (DFIR) helfen Ihnen, optimal auf Cybercrime und potenzielle wirtschaftskriminelle Handlungen zu reagieren und diese anschließend digital-forensisch aufzuklären.

Im Rahmen unserer DFIR-Services bieten wir eine deutsch- und englischsprachige 24x7-Hotline für Cyber Incident Response sowie reaktive Lösungen für die forensische Datensicherung, Analyse und Berichterstattung, die jederzeit den aktuellen

forensischen Standards entsprechen. In der digital-forensischen Untersuchung ermitteln wir die Ursachen und Hintergründe des Vorfalls und unser Bericht kann zur Durchsetzung von Ansprüchen im Falle von zivil- oder strafrechtlichen Verfahren eingesetzt werden. Alle Untersuchungsschritte werden von erfahrenen Datenschutzanwälten begleitet.

#### Cyber-Prävention

Wir überprüfen Ihre Prozesse sowie technischen und organisatorischen Maßnahmen, bewerten diese und strukturieren sie nach ihrer Kritikalität.

Sie erhalten von uns klare Empfehlungen und einen auf Sie zugeschnittenen Maßnahmenplan für eine messbare Erhöhung Ihres IT-Sicherheitsniveaus und eine nachhaltige Cyberprävention. Durch unsere Erfahrung in der Untersuchung

von Cybercrime-Angriffen und häufig ausgenutzte Schwachstellen helfen wir Ihnen, schnell wirksame Maßnahmen ergreifen zu können.

#### Cyber Compliance/Risiko-Assessment

Wir bewerten die Einhaltung spezifischer gesetzlicher oder vertraglicher Anforderungen an die Cybersicherheit in Ihrer Organisation und unterstützen Sie bei der Implementierung und Weiterentwicklung Ihrer Maßnahmen.

#### Forensische Gutachten

Deloitte versteht sich als Full-Service-Provider, der im Falle eines Incident und gerichtlicher Auseinandersetzung sachkundige, unabhängige sowie gerichtsverwertbare Gutachten im Bereich der IT-Forensik für Sie anfertigt.

#### Lieferkettenangriff mit Ransomware-Infektion

Durch einen sogenannten „Supply Chain Attack“ (Lieferkettenangriff) war ein Unternehmen von Ransomware betroffen und sämtliche Systeme, inklusive des Backup-systems, waren von den Kriminellen verschlüsselt. Diese Situation zwang das Unternehmen dazu, sämtliche Geschäftsprozesse manuell abzubilden (u.a. Rechnungslegung, Lohnbuchhaltung) und die komplette IT-Infrastruktur neu aufzubauen.

Deloitte unterstützte das Unternehmen bei der Etablierung der temporären manuellen Prozesse sowie der Wiederherstellung aller geschäftsrelevanten Daten (Forensic Accounting). Zeitgleich wurde der (Wieder-)Aufbau der IT-Umgebung unterstützt und der Vorfall digital-forensisch untersucht. Ziele der Untersuchung war das Schließen von Sicherheitslücken und die digital-forensische Aufarbeitung des Vorfalls (Klärung des Angriffsvektors, der Kompromittierung und einer möglichen Datenausleitung).

#### Bankdatenbetrug

Bei Bankdatenbetrug (auch Payment Diversion Fraud) handelt es sich um ein weiteres, allgegenwärtiges Phänomen im Bereich Cybercrime. Betrüger spionieren E-Mail-Kommunikationen aus und teilen mit, dass sich die Bankverbindung geändert hätte und/oder erbeuten durch Phishing die Credentials des CFO des Unternehmens, was ohne ausreichende technische Absicherung zu Schäden in Millionenhöhe für die betroffenen Unternehmen aller Branchen führt.

DFIR macht für Sie den Unterschied, wenn es um die Identifizierung, Untersuchung und flächendeckende Behebung von IT-Sicherheitsvorfällen und Fällen von Wirtschaftskriminalität geht.

#### Betriebsunterbrechung durch Cyber Incidents

Lösegeldforderungen – beispielsweise im Zuge eines Ransomware-Angriffs – sind für Unternehmen nicht mehr zwangsläufig die größte Herausforderung. Erschwerender sind der Reputationsverlust und die Kosten, die durch Betriebsunterbrechungen oder Datenausleitungen entstehen. Nicht nur die Anzahl der Cyberattacken auf Unternehmen steigt wieder stetig, sondern auch die Dauer, bis sich die Betroffenen von einem solchen Angriff erholen und die kompromittierte IT-Infrastruktur wiederhergestellt werden konnte.

Das DFIR-Team von Deloitte übernimmt die Bewertung von Betriebsunterbrechungsschäden und Schadensermittlungen für betroffene Unternehmen und sorgt – neben der Beendigung des Angriffs – auch für eine Minimierung des Business Impact. Auch für die Themenbereiche Krisenmanagement, Krisenkommunikation und Vermittlung rechtlicher Beratung steht Ihnen unser Expertenteam rund um die Uhr zur Seite.

<sup>1</sup>Vgl. Bundesamt für Sicherheit in der Informationstechnologie (BSI): Qualifizierte APT-Response Dienstleister im Sinne § 3 BSIg. Stand: 16. Dezember 2021, Online-Zugriff 6.1.2022.

# Ihre Ansprechpartner



## **Thomas Fritzsche**

Partner  
Head of Forensic Technology  
und eDiscovery  
Tel: +49 151 58072802  
thfritzsche@deloitte.de



## **Helmut Brechtken**

Partner  
Head of Digital Forensic  
Incident Response  
Tel: +49 151 54484223  
hbrechtken@deloitte.de



## **Martin Bodenstein**

Director  
Forensic Technology  
Tel: +49 151 14880257  
mbodenstein@deloitte.de



Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited (DTTL), ihr weltweites Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen (zusammen die „Deloitte-Organisation“). DTTL (auch „Deloitte Global“ genannt) und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL-Mitgliedsunternehmen und verbundene Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen und nicht für die der anderen. DTTL erbringt selbst keine Leistungen gegenüber Kunden. Weitere Informationen finden Sie unter [www.deloitte.com/de/UeberUns](http://www.deloitte.com/de/UeberUns).

Deloitte bietet branchenführende Leistungen in den Bereichen Audit und Assurance, Steuerberatung, Consulting, Financial Advisory und Risk Advisory für nahezu 90% der Fortune Global 500®-Unternehmen und Tausende von privaten Unternehmen an. Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Unsere Mitarbeitenden liefern messbare und langfristig wirkende Ergebnisse, die dazu beitragen, das öffentliche Vertrauen in die Kapitalmärkte zu stärken, die unsere Kunden bei Wandel und Wachstum unterstützen und den Weg zu einer stärkeren Wirtschaft, einer gerechteren Gesellschaft und einer nachhaltigen Welt weisen. Deloitte baut auf eine über 175-jährige Geschichte auf und ist in mehr als 150 Ländern tätig. Erfahren Sie mehr darüber, wie die rund 457.000 Mitarbeitenden von Deloitte das Leitbild „making an impact that matters“ täglich leben: [www.deloitte.com/de](http://www.deloitte.com/de).

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen und weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited (DTTL), ihr weltweites Netzwerk von Mitgliedsunternehmen noch deren verbundene Unternehmen (zusammen die „Deloitte Organisation“) erbringen mit dieser Veröffentlichung eine professionelle Dienstleistung. Diese Veröffentlichung ist nicht geeignet, um geschäftliche oder finanzielle Entscheidungen zu treffen oder Handlungen vorzunehmen. Hierzu sollten Sie sich von einem qualifizierten Berater in Bezug auf den Einzelfall beraten lassen.

Es werden keine (ausdrücklichen oder stillschweigenden) Aussagen, Garantien oder Zusicherungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in dieser Veröffentlichung gemacht, und weder DTTL noch ihre Mitgliedsunternehmen, verbundene Unternehmen, Mitarbeiter oder Bevollmächtigten haften oder sind verantwortlich für Verluste oder Schäden jeglicher Art, die direkt oder indirekt im Zusammenhang mit Personen entstehen, die sich auf diese Veröffentlichung verlassen. DTTL und jede ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen.