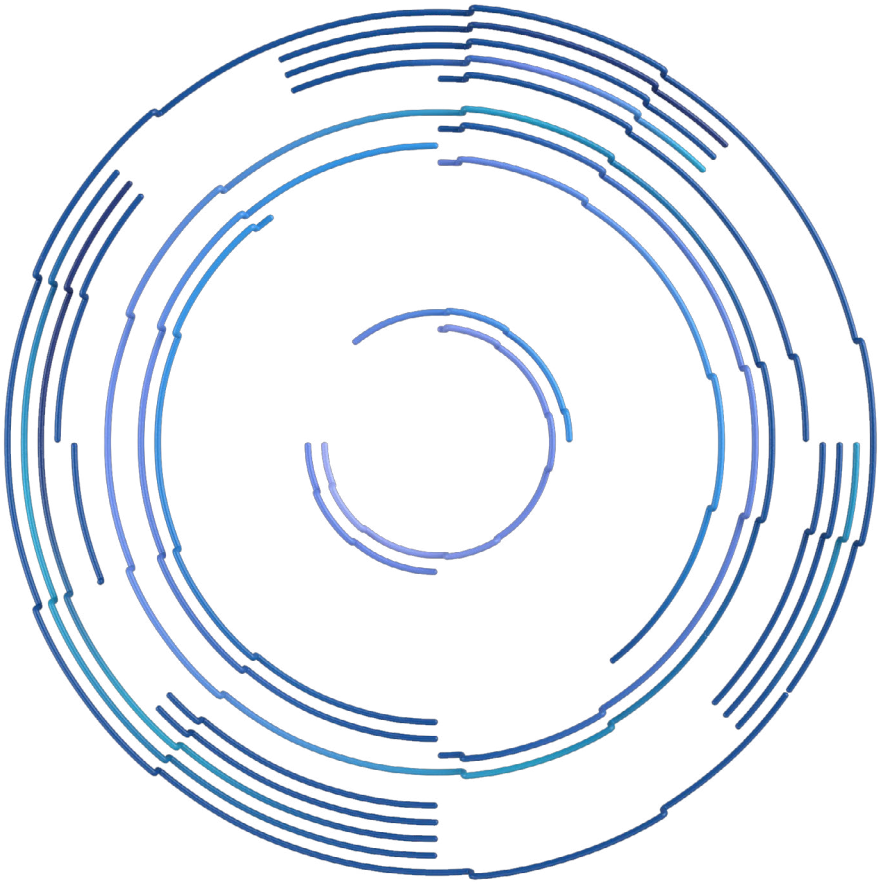

Digital Forensic Incident Response (DFIR)

Deloitte unterstützt und begleitet Sie weltweit im Fall von Cybercrime-Angriffen und Wirtschaftskriminalität. Wir helfen mit Cyber Incident Response, Krisenmanagement, der Wiederherstellung Ihrer Geschäftsprozesse und IT-Umgebung bis hin zur Aufklärung und Ursachenanalyse eines Cyber-Sicherheitsvorfalls.

Unternehmen aller Branchen und Größen sowie öffentliche Einrichtungen sind mit einer steigenden Zahl von Cybercrime-Angriffen konfrontiert, die sich schnell weiterentwickeln und immer professioneller und komplexer werden. Cybercrime-Angriffe wie Ransomware, Network Intrusion, Bankdatenbetrug und komplexe Malware sind oft erfolgreich und den betroffenen Unternehmen und Organisationen drohen Folgen wie Betriebsunterbrechungen, finanzielle Verluste, Vertragsstrafen, Reputationsschäden und der Verlust sensibler Unternehmensdaten.

Neben gezielten Angriffen auf Unternehmen und Organisationen stellen auch Straftaten in diesen, wie zum Beispiel Wirtschaftskriminalität in Form von Datendiebstahl, eine ernsthafte Bedrohung dar. Häufige sind sensible Unternehmensdaten betroffen und die Kompromittierung kann zu gravierenden Folgen für die Wirtschaftlichkeit führen.

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

Wir unterstützen Sie beim Umgang mit Cyber-Sicherheitsvorfällen 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.

MAKING AN IMPACT THAT MATTERS since 1845

Deloitte als zertifizierter Dienstleister für Advanced Persistent Threat (APT-) Response

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) hat Deloitte geprüft und empfiehlt uns als „qualifizierten Dienstleister für APT-Response“[1].

Unsere Services

Digital Forensic Incident Response

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

Im Rahmen unserer DFIR-Services bieten wir Ihnen eine 24x7-Erreichbarkeit 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 unseren erfahrenen Datenschutzanwälten begleitet.

Die digital-forensischen Labore und Forensic Data Centers von Deloitte erfüllen die höchsten Informationssicherheitsstandards und verfügen über eine skalierbare und hochverfügbare IT-Infrastruktur.

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 Cyber-Sicherheitsniveaus und eine nachhaltige Cyber-Prävention.

Cyber Compliance

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

Cyber Security

Wir unterstützen Sie bei der Identifikation bestehender Sicherheitslücken und Schwachstellen in Ihrer IT-Infrastruktur und geben Ihnen Empfehlungen, wie Sie diese beseitigen können.

Lieferkettenangriff mit Ransomware-Infektion

Durch einen sogenannten „Supply Chain Attack” (Lieferkettenangriff) können Unternehmen von Ransomware betroffen sein und sämtliche Systeme, inklusive des Backupsystems, verschlüsselt werden. Diese Situation zwingt Unternehmen dazu, sämtliche Geschäftsprozesse manuell abzubilden (u.a. Rechnungslegung, Lohnbuchhaltung) und die komplette IT-Infrastruktur neu aufzubauen.

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

Distributed Denial of Service (DDoS) Attack

Ein Distributed-Denial-of-Service-Angriff (DDoS) bezeichnet einen schwerwiegenden Sicherheitsvorfall, der die kritischen Geschäftsabläufe von Unternehmen beeinträchtigt.

Deloitte führt in diesem Fall eine Reihe von Untersuchungshandlungen durch, um Unternehmen dabei zu helfen, das volle Ausmaß des Angriffs zu verstehen, und bei der Schadensbegrenzung und den anschließenden Ermittlungsaktivitäten zu unterstützen.

Malware-Infektion

Durch Malware können globale Netzwerke von Unternehmen infiziert werden. Dadurch können mehrere bis alle relevanten operativen Prozesse lahmgelegt werden, was sich bis hin zu einem globalen Komplettausfall entwickeln kann.

Deloitte stellt innerhalb von wenigen Stunden ein internationales Expertenteam bereit, das in enger Zusammenarbeit mit betroffenen Unternehmen alle identifizierten Sofortmaßnahmen begleitet und den Vorfall erfolgreich eindämmt. Mit einer Teamstärke von über 130 erfahrenen Deloitte-Mitarbeitern können im Rahmen der Projekte IT-Systeme und Geschäftsprozesse wiederhergestellt und ein Reverse Engineering der Malware durchgeführt werden.

[1] Vgl. Bundesamt für Sicherheit in der Informationstechnologie (BSI): Qualifizierte APT-Response Dienstleister im Sinne § 3 BSIG. Stand: 16. Dezember 2021. [Online-Zugriff 06.01.2022].

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

Chris Lichtenthäler
Senior Manager
Forensic Technology
Tel: +49 151 54484140
clichtenthaeler@deloitte.de

Deloitte.

Stand 01/2022