
KPMG
ALLES
IM BLICK
FORENSIC. EINEN
SPRUNG VORAUS.
www.kpmg.de/forensic

FORENSIC. EINEN SPRUNG VORAUS.

Wir meinen, dass Sie in unerwarteten und herausfordernden Situationen schnell Klarheit brauchen – damit Sie immer einen Schritt voraus sind und die richtigen Entscheidungen für Ihr Unternehmen treffen können.

IHR GESCHÄFT IM FOKUS

Private Unternehmen und öffentliche Verwaltungen müssen sich im Rahmen der Auseinandersetzung mit Wirtschaftskriminalität zunehmend einem neuen Phänomen stellen: Cybercrime und Data Leakage. Sie bedrohen Unternehmen von innen und außen und bergen ein enormes wirtschaftliches Risiko. Zudem bedrohen sie die wohlerworbene Reputation eines Unternehmens. Jedes Managementmitglied und jeder Entscheider steht somit vor großen Herausforderungen. Wir unterstützen Sie bei der Eindämmung dieser Gefahren, damit Sie Ihren Fokus unverändert auf Ihr Geschäft und dessen erfolgreiche Weiterentwicklung setzen können.

SCHNELLE AUFKLÄRUNG

Rasante Digitalisierung und globale Vernetzung schaffen neue und unbegrenzte Entwicklungsmöglichkeiten für Unternehmen, aber auch neue Risiken und Bedrohungen: Das virtuelle Verbrechen ist so global wie Ihr Business. Wer zum Ziel oder Opfer wird, muss entschieden und schnell reagieren. Voraussetzung dafür ist die umfassende und umgehende Kenntnis der Situation.

KLARE ENTSCHEIDUNGEN

Eine heikle Situation wird beherrschbar, wenn alle Fakten aufbereitet, geordnet und bewertet sind. Nur wer die Fakten kennt und einen ungetrübten Blick hat, kann klare Entscheidungen treffen.

SICHER IN DIE ZUKUNFT

Ebenso wichtig ist es, frühzeitig zu erkennen, wo Bedrohungen und Risiken lauern, um diese zu eliminieren, bevor sie sich realisieren.

ALLES IM BLICK

Forensic. Einen Sprung voraus.

HERAUSFORDERUNG VERSTEHEN: ES KANN JEDEN TREFFEN!

Cybercrime und Data Leakage sind für alle Unternehmen eine große Herausforderung: Wer davor die Augen verschließt, den trifft es im Ernstfall unvorbereitet. Ausweislich der Ergebnisse der von KPMG veröffentlichten e-Crime-Studie waren in den vergangenen zwei Jahren 40 Prozent der befragten Unternehmen Opfer von Computerkriminalität. Der erste Schock kann gleich zu Beginn wesentliche Entscheidungen behindern, Aktionismus und Überreaktion können die Situation sogar verschlimmern.

EIN RISIKO VON VIELEN

Cybercrime und Data Leakage werden oft stiefmütterlich behandelt: Ob aus Unkenntnis oder Fahrlässigkeit, allzu häufig wird nichts oder wenig unternommen, um das Risiko eines Schadensfalls proaktiv einzudämmen. Allein der IT-Abteilung die Verantwortung zu geben, wird der Herausforderung nicht gerecht und kann das Risiko vergrößern. Cybercrime- und Data Leakage-Prävention verlangen Einsatz aus allen Bereichen eines Unternehmens.

Dabei handelt es sich bei der elektronischen Bedrohung genaugenommen auch nur um ein Risiko von vielen. Daher stellt sich die Frage, warum sicherheitsbezogene beziehungsweise datenschutzrechtliche Verpflichtungen eines IT-Dienstleisters in der Praxis nicht genauso aktiv verfolgt und überwacht werden wie zum Beispiel die Verfügbarkeitszeiten von IT-Systemen, die in Service-Level-Agreements vereinbart werden.

Cybercrime und Data Leakage gehören in das Risikomanagement eines Unternehmens. Es ist kein Zeichen von Schwäche, sondern Ausdruck von verantwortungsvollem und zukunftsgerichtetem unternehmerischen Handeln, sich diesen Herausforderungen zu stellen.

FORENSIC. EINEN SPRUNG VORAUS.

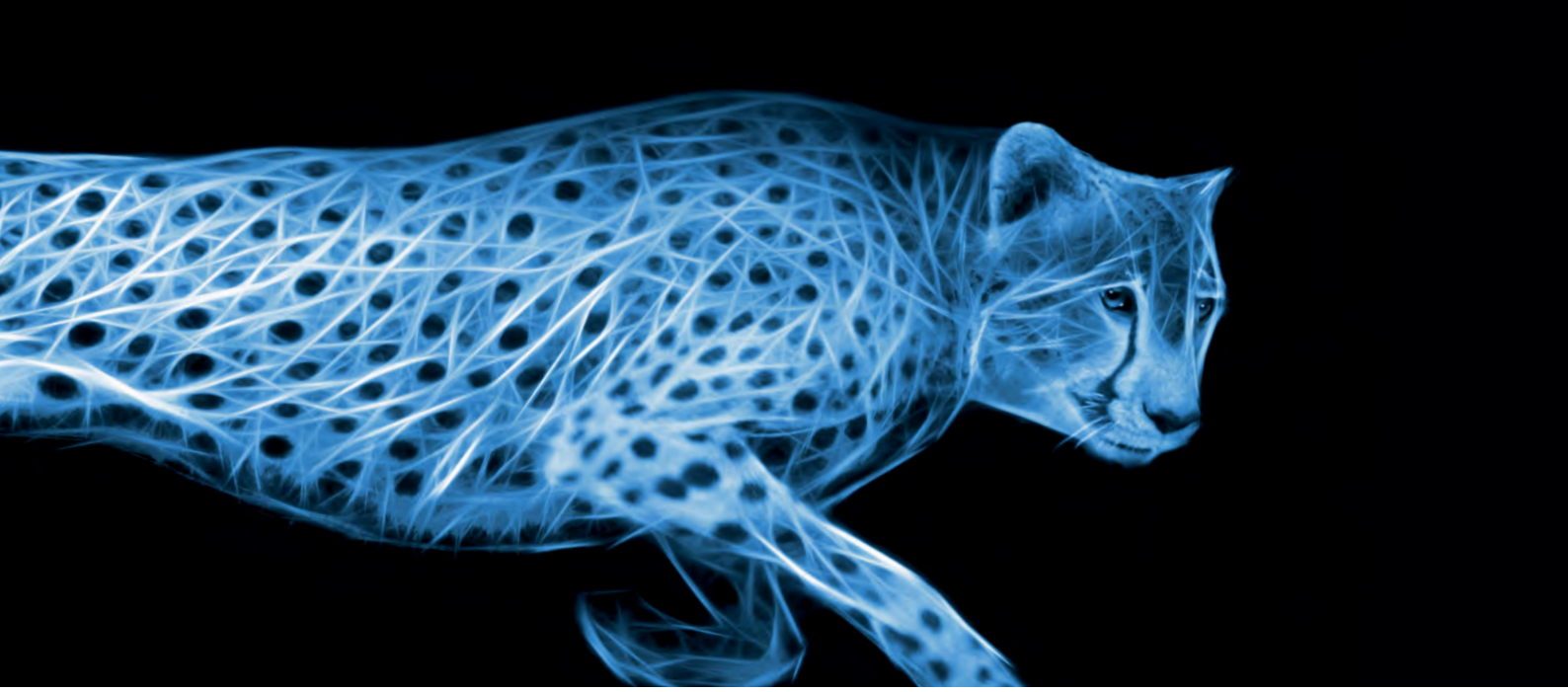
EIN RISIKO, DAS SICH VERÄNDERT

Die Bedrohungslandschaft ändert sich nahezu täglich. Über 80 Prozent der von KPMG in der e-Crime-Studie Befragten sind der Ansicht, dass die virtuellen Attacken internationaler, das regulatorische Umfeld komplexer und die Täter professioneller werden. Die Vernetzung von IT-Systemen, die unternehmerischen Erfolg vorantreibt, eröffnet Tätern neue Möglichkeiten. Kaum ein Tag vergeht, an dem nicht über neue Vorfälle und Ermittlungsverfahren berichtet wird. Aus dem allgegenwärtigen Risiko kann sich ein diffuses Gefühl der Verwundbarkeit entwickeln, das die Fokussierung auf das Wesentliche – die Geschäftsentwicklung – verhindert, notwendige unternehmerische Entscheidungen verzögert und den unternehmerischen Mut, der geschäftlichen Erfolg erst ermöglicht, immer weiter einschränkt.

RISIKO KONKRETISIEREN

Doch das diffuse Gefühl der Verwundbarkeit lässt sich konkretisieren. Für jedes Unternehmen bestehen unterschiedliche Risiken, Opfer von Cybercrime und Data Leakage zu werden. Je nach Geschäftsmodell liegen Angriffe von Cyberkriminellen, die es insbesondere auf den eigenen finanziellen Vorteil abgesehen haben, näher als Attacken, bei denen das betroffene Unternehmen in das virtuelle Schlachtfeld von zwischenstaatlichen Auseinandersetzungen gezogen wird.

Je nach Produkt- und Dienstleistungsangebot können Risiken in einer IT-Infrastruktur angesiedelt sein, die bis zu Tausende von Kunden umfasst, oder auf wenige, besonders sensible Daten zielen, die nur in einzelnen Rechenzentren gespeichert und verarbeitet werden.



UNSERE ERFAHRUNG ZEIGT: RISIKO UND AUSWIRKUNGEN VON CYBERCRIME UND DATA LEAKAGE WERDEN UNTERSCHÄTZT – BIS DER ERNSTFALL EINTRITT.

Jedes Unternehmen hat seine ganz eigene Risikoexposition. Nur wer sie kennt, kann sein konkretes Bedrohungspotenzial verstehen und angemessene Vorkehrungen treffen.

VORBEREITET SEIN

Unternehmen müssen deshalb Vorkehrungen treffen, die zum einen das Risiko eines Schadensfalls reduzieren und zum anderen, im Falle des Falles, die schnelle, klare und entschiedene Reaktion auf Cybercrime oder einen Data Leakage-Vorfall ermöglichen.

WIR UNTERSTÜTZEN SIE

Wir unterstützen Sie, die entscheidenden Vorkehrungen zu treffen, um im Zweifel richtig vorbereitet zu sein und schnell und entschieden reagieren zu können. Außerdem entwickeln wir gemeinsam mit Ihnen Maßnahmen, die das Risiko eindämmen, zukünftig Opfer von Cybercrime und Data Leakage zu werden.

SCHNELLE AUFKLÄRUNG – KLARE ENTSCHEIDUNG

SITUATION VERSTEHEN, RICHTIGE ENTSCHEIDUNGEN TREFFEN

Cybercrime und Data Leakage werden niemals gänzlich zu verhindern sein. Und es wird niemals alltäglich sein, einen konkreten Sachverhalt aufzuklären – unabhängig davon, ob es sich um einen laufenden oder bereits beendeten Vorfall handelt, und unabhängig davon, ob der Angriff von außen oder von innen erfolgt. Die betroffenen Entscheidungsträger werden in der Regel alles daran setzen, die Situation so schnell wie möglich aufzuklären. Möglicherweise auch getrieben von verständlicher Enttäuschung und Überraschung, wenn der Täter im Kollegenkreis vermutet werden muss.

Wenn eine Cybercrime-Attacke oder ein Data Leakage-Vorfall in einem Unternehmen entdeckt wird, ist die größte Herausforderung, schnell einen klaren Überblick über die Situation zu gewinnen. Nur so können richtige Entscheidungen getroffen werden. Je nachdem, um welchen Vorfall es sich handelt, kann es darum gehen,

- den konkreten Vorfall abzustellen und die betroffenen Daten, Informationen und Strukturen zu schützen,
- einen entstehenden Schaden zu begrenzen und finanzielle Risiken zu verringern,
- die Notwendigkeit oder Vorteilhaftigkeit der Zusammenarbeit mit Verfolgungsbehörden, beispielsweise mit Blick auf eine mögliche Bußgeldreduzierung, beurteilen zu können,
- geeignete Maßnahmen zur Wahrung der Unternehmensreputation und des Kundenvertrauens zu ergreifen.

UNSERE ERFAHRUNG ZEIGT, DASS VIELE UNTERNEHMEN SCHON BEI DER KLÄRUNG VON ZUSTÄNDIGKEITEN UND DER SUCHE NACH ANSPRECHPARTNERN WERTVOLLE ZEIT VERLIEREN.

DIE ERSTEN STUNDEN ZÄHLEN

Die Weichen einer erfolgreichen Aufarbeitung werden in den ersten Stunden gestellt. Doch häufig reagieren die Betroffenen auf einen Cyberangriff nach dem gleichen – schädlichen – Muster: Im Bemühen, den Sachverhalt aufzuklären, versuchen alle Verantwortlichen im Unternehmen nach Kräften zu helfen. Ihre Aktivitäten sind nicht abgestimmt, notwendige Schritte werden gleich mehrfach initiiert, andere unterbleiben, ein umfassender Überblick über die Situation fehlt oder entsteht erst mit erheblicher Verzögerung. Wenn alle in unterschiedliche Richtungen laufen, kommt niemand weit. Das belegen auch die Ergebnisse der e-Crime-Studie von KPMG. Versäumnisse im Rahmen des Incident Managements, wie eine unklare Informationslage, unklare Verantwortlichkeiten oder das Fehlen entsprechender Sofortmaßnahmen bzw. ihre mangelhafte Umsetzung, sind in dieser Hinsicht die meist genannten Risiken.

Dabei erwartet niemand, dass ein Vertriebschef zugleich Experte für den Kundendatenschutz ist oder der Leiter der IT-Abteilung ein Experte für IT-forensische Maßnahmen.

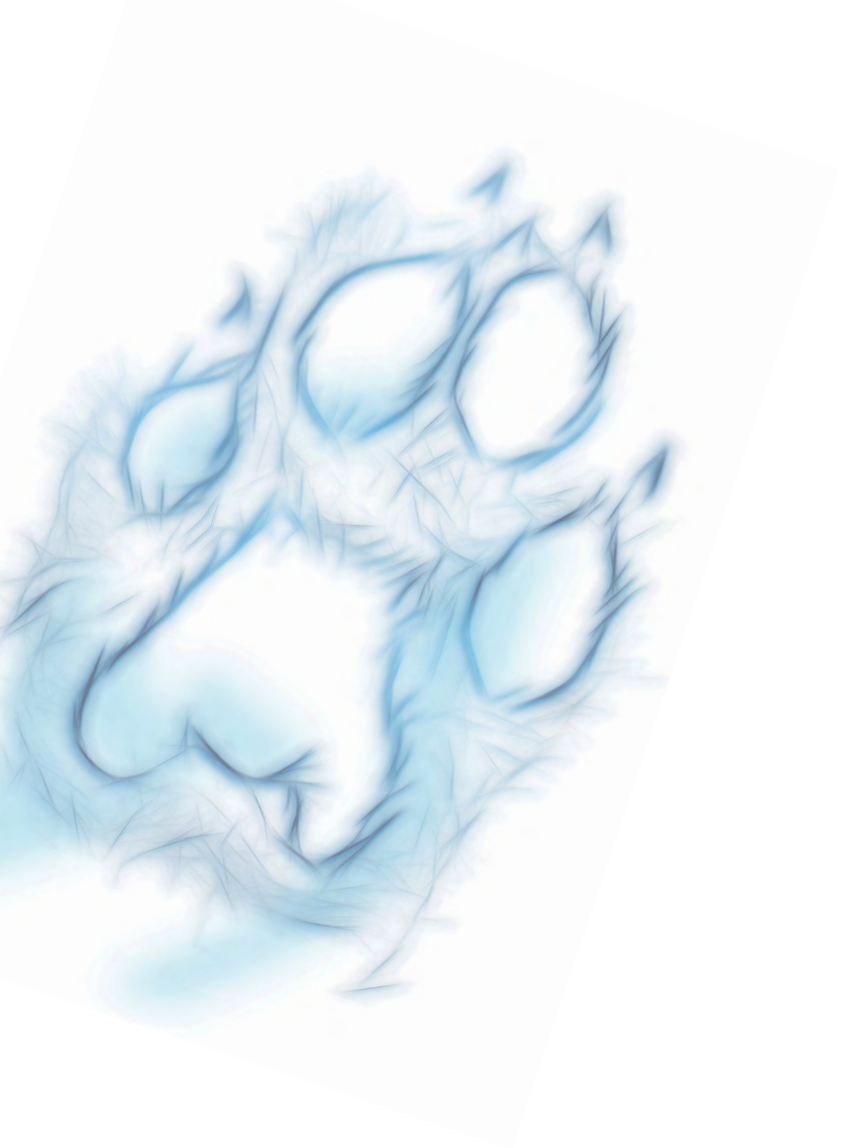
Von einem Unternehmen wird erwartet, wirksame Schritte einzuleiten, damit die richtigen Stellen im Unternehmen zeitnah und umfassend informiert werden, der Informationsfluss koordiniert sowie die notwendige externe Unterstützung aktiviert wird. So kann das Chaos der ersten Stunden schnellstmöglich über ein geordnetes und fest vereinbartes Verfahren in eine beherrschbare Situation geführt werden (Cyber Incident Response Readiness). Das ist die notwendige Voraussetzung, um eine gerichtsverwertbare Sachverhaltsdokumentation erstellen zu können.

Sie als verantwortlicher Entscheider müssen schnell einen klaren Überblick über die Situation erlangen, um die notwendigen Entscheidungen für die Zukunft des Unternehmens treffen zu können.

WIR UNTERSTÜTZEN SIE

Wir unterstützen Sie bei der Implementierung eines maßgeschneiderten Cyber Incident Response-Systems in Ihrem Unternehmen, damit Sie im Falle von Cybercrime oder eines Data Leakage-Vorfalls schnellstmöglich die richtigen Maßnahmen ergreifen.

Außerdem begleiten wir Sie bei der schnellen, diskreten und professionellen Aufklärung von Cybercrime und Data Leakage-Vorfällen, gegebenenfalls auch in Kooperation mit Ermittlungsbehörden. So erhalten Sie die Informationsgrundlage, die Sie benötigen, um die richtigen Konsequenzen für Ihr Unternehmen zu ziehen.



SICHER IN DIE ZUKUNFT

PHÄNOMEN CYBERCRIME AKTIV AUFGREIFEN

Virtuelle Wirtschaftskriminalität ist kein Mysterium, aber die fehlende Auseinandersetzung mit menschlichem Fehlverhalten – vor allem in der eigenen Belegschaft – sowie fehlendes Hintergrundwissen führen häufig zu einer Verdrängung des Problems. Schnell sieht man sich auch dem Vorwurf des Generalverdachts oder der Dramatisierung ausgesetzt. Aber Nichtbeschäftigung mit dem Thema führt zur Unkenntnis und zu Unvorbereitetsein. Das erleichtert es den hochprofessionellen Tätern allzu oft, Schwachstellen auszunutzen und großen Schaden anzurichten. 88 Prozent der Teilnehmer an der e-Crime-Studie von KPMG sehen in der Unachtsamkeit der Beschäftigten einen entscheidenden, Cybercrime begünstigenden Faktor.

INDIVIDUELLE RISIKOEXPOSITION ERMITTELN

Dabei sind die Verhaltensmuster der virtuellen Angriffe und die typischen Täter längst bekannt und schon über Jahre hinweg aus den verschiedensten Blickwinkeln untersucht – nach Ländern und Regionen, nach Deliktstypen, nach Branchen und nach Kunden- und Wettbewerberstruktur. Mit diesem Wissen lässt sich, angewendet auf die individuelle Situation Ihres Unternehmens, eine präzise Landkarte Ihrer Cybercrime-Risiken zeichnen, die dokumentiert, in welchen Unternehmensbereichen welche Bedrohung lauert und wie hoch ihre Eintrittswahrscheinlichkeit ist.

UNSERE ERFAHRUNG ZEIGT, DASS DIE KOSTEN DER BEWÄLTIGUNG EINER ERFOLGREICHEN CYBERCRIME-ATTACKE DIE KOSTEN VON PRÄVENTIVEN MASSNAHMEN UM EIN VIELFACHES ÜBERSTEIGEN.

PASSGENAUE MASSNAHMEN ERGREIFEN

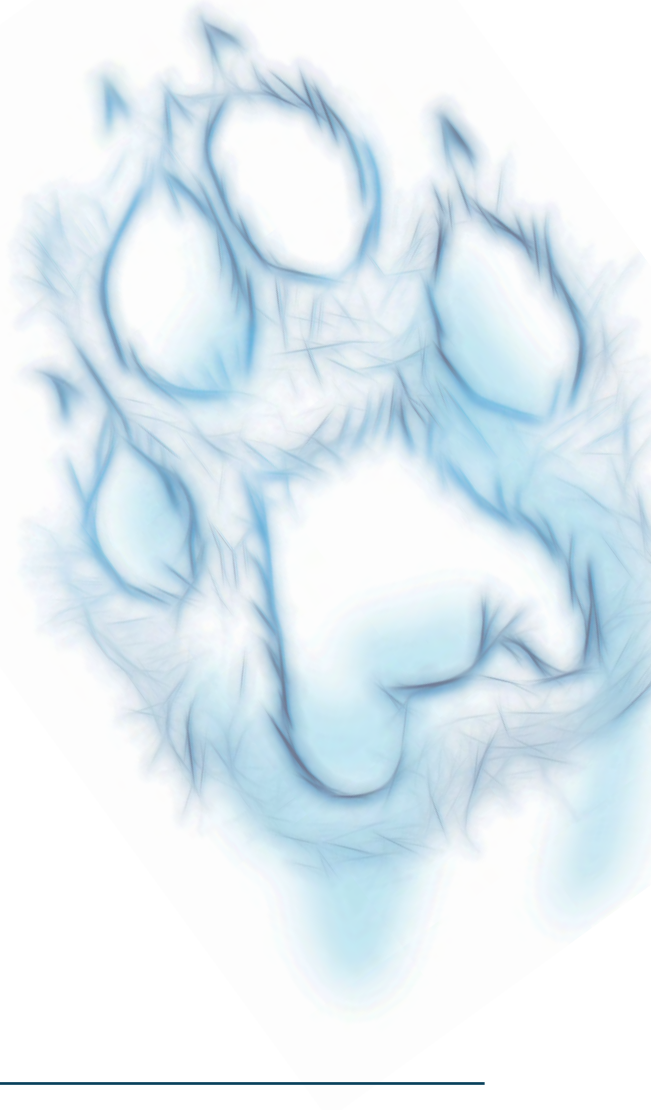
Auf dieser Basis können Sie notwendige und angemessene Maßnahmen punktgenau dort veranlassen, wo das Risiko von Cybercrime und Data Leakage am größten ist. Punktgenau heißt kostenbewusst und ist gleichzeitig darauf ausgerichtet, für Verständnis in der Belegschaft zu sorgen, weil Sie erklären können, aus welchem Grund die eine Maßnahme hier und die andere Maßnahme dort umgesetzt wird. Eine Belegschaft, die Verständnis für risikoverringernde Maßnahmen entwickelt und diese verinnerlicht, bildet das notwendige Fundament für den Erfolg einer jeden Compliance- und Sicherheitsmaßnahme.

SICHER IN DIE ZUKUNFT

Mit der Umsetzung dieser Schritte sind Sie und Ihr Unternehmen gut vorbereitet. Den Fall der Fälle werden Sie nicht verhindern können. Aber Sie können das Risiko, dass es zu Cybercrime oder Data Leakage kommt, reduzieren und schnell reagieren. Damit wird das Risiko beherrschbar und kalkulierbar und Sie können sich auf die Weiterentwicklung Ihrer geschäftlichen Aktivitäten und den Ausbau Ihres geschäftlichen Erfolgs fokussieren.

WIR UNTERSTÜTZEN SIE

Wir unterstützen Sie, eine unternehmensindividuelle Risikolandkarte der Cybercrime- und Data Leakage-Sachverhalte zu erstellen, die Ihre Geschäftstätigkeit, Wettbewerberstruktur, regionalen Tätigkeitsschwerpunkte und weitere wesentliche Gesichtspunkte berücksichtigt. Außerdem stehen wir Ihnen mit unserer Erfahrung zur Seite, aus dieser unternehmensindividuellen Risikolandkarte maßgeschneiderte Maßnahmen abzuleiten und diese schonend in Ihre Geschäftsprozesse zu implementieren.



ALLES IM BLICK

Der Bereich Forensic von KPMG verfügt über umfassende Erfahrung und Praxisorientierung bei der Prävention, Aufdeckung und Aufklärung wirtschaftskrimineller Sachverhalte in Unternehmen und Behörden, insbesondere auch im Bereich von Cybercrime und Data Leakage. Wir arbeiten dabei eng mit juristischen Beratern zusammen und erstellen gerichtsverwertbare Berichte für zivil-, straf- und arbeitsrechtliche Auseinandersetzungen unter strikter Wahrung (datenschutz-)rechtlicher Grenzen.

Drei Kernaspekte stehen im Zentrum unserer Tätigkeit:

- Zeitnahe Sachverhaltsaufklärung zur Ermittlung des Tatgeschehens und der Schadenshöhe
- Angemessene Projektsteuerung
- Wirksame Prävention

Das erreichen wir im Zusammenspiel unserer verschiedenen Services.

FORENSIC INVESTIGATIONS

Aufdeckung und Untersuchung von wirtschaftskriminellen Sachverhalten sowie strafbaren Handlungen in und gegen Unternehmen beziehungsweise Behörden

FORENSIC TECHNOLOGY

Sicherung und Wiederherstellung digitaler Beweismittel sowie systematische Analyse und Auswertung von strukturierten und unstrukturierten Datenbeständen. Die Ermittlung von Cybercrime-Vorfällen sowie die Krisenbetreuung während eines Vorfalls gehören ebenfalls zu unserem Leistungsspektrum.

FORENSIC DUE DILIGENCE

Erweiterung klassischer Due Diligences um die Perspektive der Risiken aus Fraud und sonstigen dolosen Handlungen

FRAUD RISK MANAGEMENT

Analyse des Designs und der Funktionsfähigkeit von Prozessabläufen sowie interner Kontrollen im Hinblick auf forensische Risiken

CORPORATE INTELLIGENCE

Fachspezifische Recherchen und Analysen sowie zielgerichtete Aufbereitung von Hintergrundinformationen zu Unternehmen, Personen und Vermögenswerten

DATENSCHUTZ

Prävention von und Reaktion auf Datenabfluss/-diebstahl sowie Konzeption datenschutzkonformer Revisions- und Compliance-Maßnahmen

Das Forensic-Team von KPMG steht Ihnen mit interdisziplinären Spezialisten für Wirtschaftskriminalität an den Standorten Berlin, Frankfurt am Main, Hamburg, Köln und München bundesweit zur Verfügung.

Bei internationalen Sachverhalten können wir über Landesgrenzen hinweg auf unser globales KPMG-Netzwerk mit 2.500 Forensic-Spezialisten in den KPMG-Ländergesellschaften zurückgreifen. Denn: Cybercrime und Data Leakage sind kein nationales, sondern ein weltweites Phänomen.

BEI VERDACHT AUF WIRTSCHAFTS-KRIMINALITÄT UND CYBERCRIME

Wir sind für Sie da. 24 Stunden am Tag, 365 Tage im Jahr.

24/7 Notruf-Hotline* 0180 KPMG FOR
(+49 1805 764367)

E-Mail forsupport@kpmg.com

* Telefonkosten: Festnetz 14 ct/min; Mobilfunknetze 42 ct/min

KONTAKT

KPMG AG Wirtschaftsprüfungsgesellschaft

Für Forensic Investigation & Cyber Response:
Alexander Geschonneck
Partner, Leiter Forensic Deutschland
T +49 30 2068-1520
ageschonneck@kpmg.com

Für Datenschutz:
Barbara Scheben
Partner, Forensic
T +49 69 9587-3737
bscheben@kpmg.com

Uwe Bernd-Striebeck
Partner, Security Consulting
T +49 201 455-6870
uberndstriebeck@kpmg.com

www.kpmg.de/forensic

Folgen Sie uns auf Twitter:

@KPMG_DE_FOR
https://twitter.com/KPMG_DE_For

Mehr Informationen finden Sie auch im App Store:

KPMG-Forensic-Krisenmanager

KPMG-DilemmApp

Haben Sie Interesse am KPMG-Forensic-Newsletter?
Dann melden Sie sich hier kostenlos an:
https://www.kpmg.de/newsletter/subscribe.aspx?defaultnewsletter=forensic-newsletter