Deloitte.
Legal

Umgang mit Cyberbedrohungen

Erkennen, Reagieren und Absichern

Deloitte Legal Webcast | 17. Januar 2024

MAKING AN IMPACT THAT MATTERS since 1845

Referent:innen

Helmut Brechtken
Financial Advisory
Partner | Head of Digital Forensic Incident Response
Deloitte GmbH

Tel.: +49 221 9732 4949
E-Mail: hbrechtken@deloitte.de

Nikola A. F. Werry, LL.M. (UK)
Digital Law | Head of Data and Data Protection Law
Partnerin, Rechtsanwältin
Deloitte Legal Rechtsanwaltsgesellschaft mbH

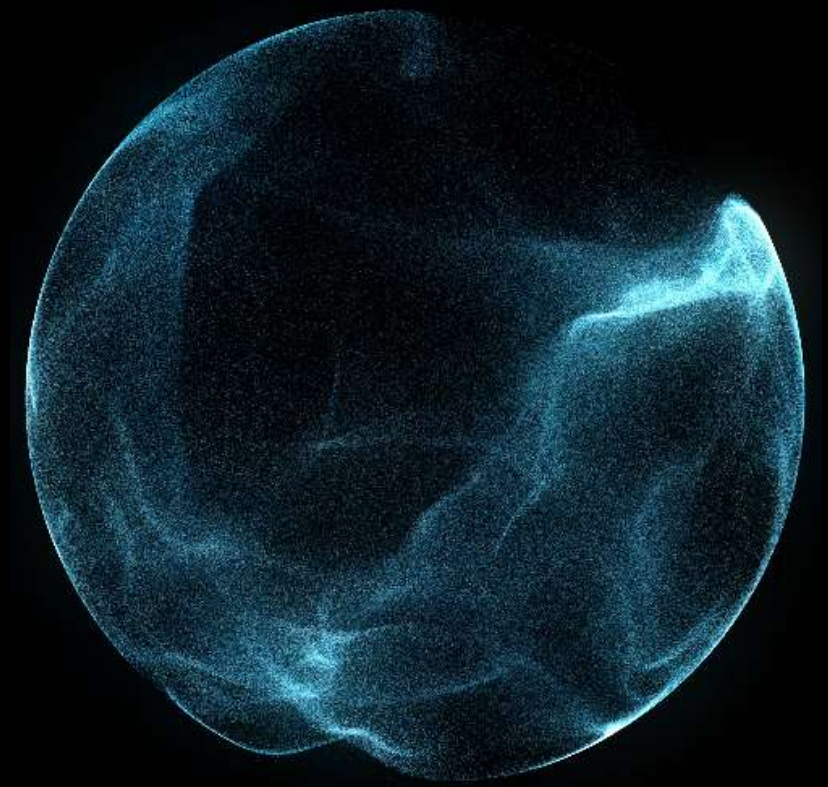
Tel.: +49 69 71918 8482
E-Mail: nwerry@deloitte.de

Frank Fischer, LL.M. (Univ. London)
Banking & Finance | Head of Insurance & Invest. Mgmt
Partner, Rechtsanwalt
Deloitte Legal Rechtsanwaltsgesellschaft mbH

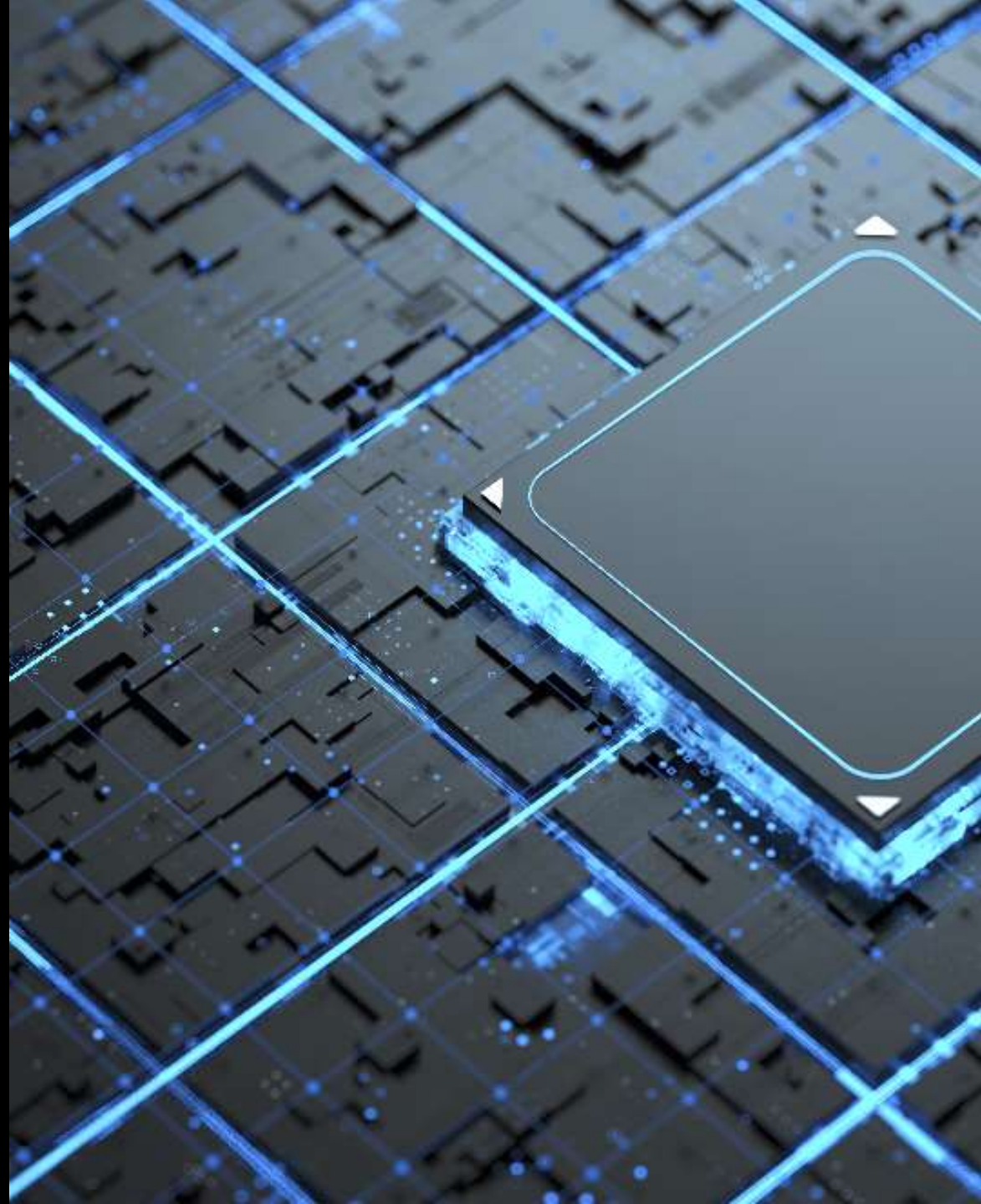
Tel.: +49 89 29036 5680
E-Mail: frankfischer@deloitte.de

AGENDA

1. Begrüßung / Vorstellung
2. Überblick über typische / heutige Angriffsszenarien
3. Reaktion auf Cyber-Angriffe aus rechtlicher Sicht
4. Versicherungsschutz und Regulierung von Ansprüchen
5. Q&A

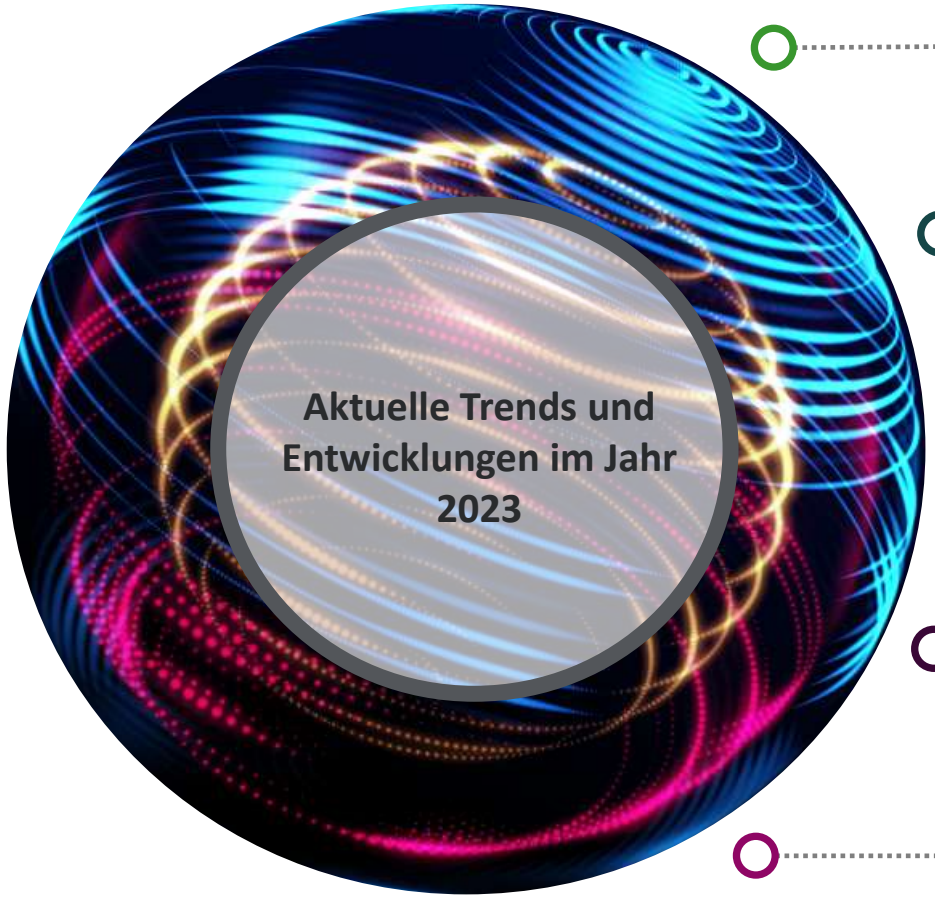


Überblick über typische / heutige Angriffsszenarien und ihre Auswirkung auf Unternehmen



Cybercrime Trends in 2024

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.*	→	€ - €€€

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

Reaktion auf Cyber-Angriffe aus rechtlicher Sicht

Abwicklung und Aufarbeitung von Cyber Incidents aus juristischer Sicht

Response. Recover. Thrive.

1

Response

- Identifizierung / initiale Dokumentation
- Schadensbegrenzung
- Evidenzsicherung
- Meldepflichten / Betroffenenrechte
- Ersatzbeschaffung
- Kommunikation

2

Recover

- Eingehende rechtliche Bewertung des Vorfalls
- Compliance Wiederherstellung
- (Weitere) Schadensbegrenzung

3

Thrive

- Umsetzung der Feststellungen
- Schulung und Sensibilisierung
- Zusammenarbeit mit den Behörden
- Versicherungsansprüche

Abwicklung und Aufarbeitung von Cyber Incidents aus juristischer Sicht

Response

Identifizierung und initiale Dokumentation

- Frühe Identifizierung des Vorfalls
- Dokumentation des Vorfalls (Sachverhalt und Maßnahmen)

Schadensbegrenzung

- Sofortmaßnahmen zur Schadensvermeidung und -begrenzung ergreifen

Evidenzsicherung

- Fortlaufende juristische Bewertung und Beweissicherung zur Vermeidung nachteiliger juristischer Konsequenzen

Meldepflichten und Betroffenenrechte

- Ergreifung der gesetzlich erforderlichen Sofortmaßnahmen (z.B. Meldung des Vorfalls)
- Erfüllung von Betroffenenanfragen

Ersatzbeschaffung

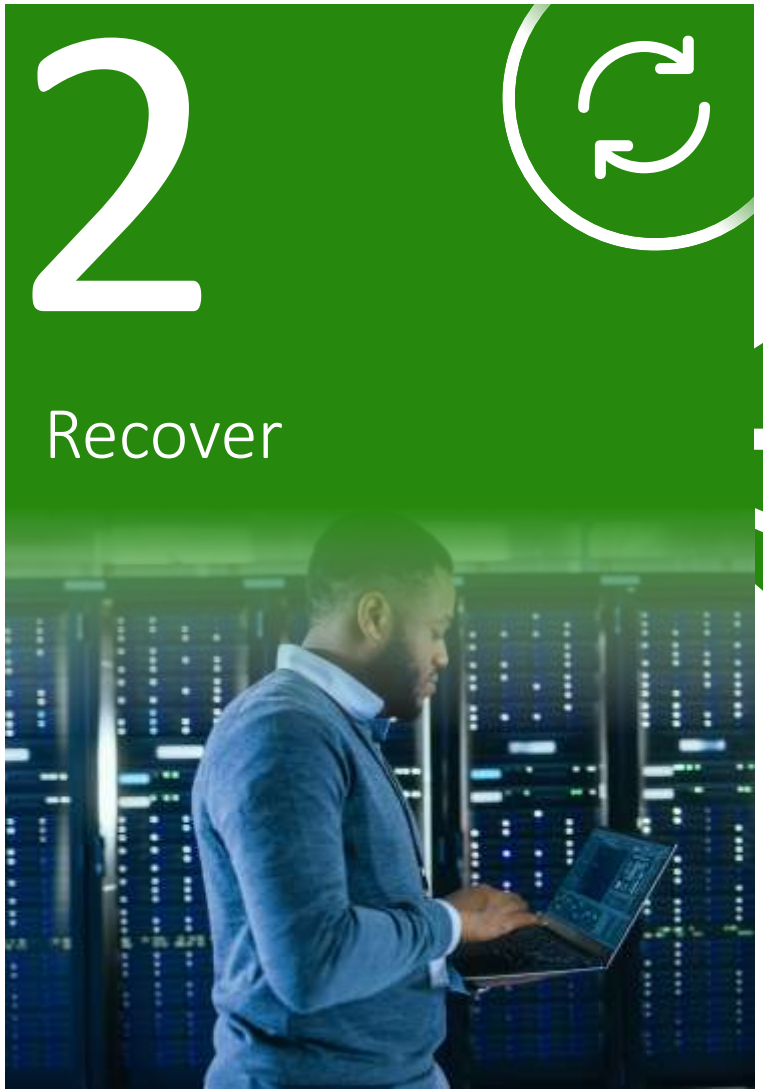
- Kurzfristige Ersatzbeschaffungen sorgfältig auswählen

Kommunikation

- Kommunikation mit Stakeholder zur Vermeidung von Risiken

Abwicklung und Aufarbeitung von Cyber Incidents aus juristischer Sicht

Recover



Eingehende rechtliche Bewertung des Vorfalls

Bericht darüber, was tatsächlich passiert ist, welche (rechtlichen) Konsequenzen der Vorfall hatte und was getan werden kann, um die Auswirkungen jetzt und in Zukunft zu beheben. Überprüfen Sie Ihre Verträge und Vereinbarungen mit Lieferanten, Kunden und Dienstleistern, um festzustellen, ob eine rechtliche Regress- oder Entschädigungs-verpflichtung besteht.

Compliance Wiederherstellung

Stellen Sie sicher, dass Sie die geltenden Datenschutz- und Sicherheitsvorschriften wieder einhalten und dokumentieren Sie Ihre Bemühungen zur Wiederherstellung der Compliance.

(Weitere) Schadensbegrenzung

Stellen Sie sicher, dass Sie Maßnahmen zur Schadensbegrenzung ergreifen, um mögliche rechtliche Folgen, wie Schadensersatzforderungen, zu minimieren.

Abwicklung und Aufarbeitung von Cyber Incidents aus juristischer Sicht

Thrive

3

Thrive

Umsetzung der Feststellungen

Die Ergebnisse der vorangegangen Phase (insb. die eingehende Analyse des Vorfalls und die ermittelten Verbesserungen der Compliance-Organisation) werden umgesetzt.

Schulung und Sensibilisierung

Einführung von Schulungen und Schulungsprogrammen, um das Bewusstsein für Cybersicherheit zu schärfen. Fokus: Einhaltung und Verstehen der regulatorischen Anforderungen.

Zusammenarbeit mit Behörden

Weiterhin Zusammenarbeit mit den zuständigen Strafermittlungs- / Datenschutzbehörden.

Versicherungsansprüche

Auseinandersetzung mit Versicherungen, insbesondere wenn der Anspruch (teilweise) bestritten wird. Dies kann insbesondere dann der Fall sein, wenn Sorgfaltspflichten angeblich nicht eingehalten wurden.

Versicherungsschutz und Regulierung von Ansprüchen

Versicherungsschutz und Regulierung von Ansprüchen

Effektiver Schutz im Bereich „Cyber“ bedarf einer strukturierten und langfristigen Betrachtung

1

Im Vorfeld des Versicherungsvertrags

- Risiko- und Bedarfsanalyse
- Beachtenswertes vor/bei Abschluss

2

Während der Vertragslaufzeit

- Kontinuierliche Beobachtung
- Vertragliche Obliegenheiten

3

Im konkreten Schadenfall

- Melde- und Mitigierungspflichten
- Anpassung des Risikomanagements

Versicherungsschutz und Regulierung von Ansprüchen

Im Vorfeld des Versicherungsvertrags

Risikoanalyse

- Identifizierung der angreifbaren IT-Infrastruktur
- Analyse des konkreten Geschäftsumfelds, mögliche Bedrohungsszenarien etc., auch unter Berücksichtigung regulatorischer Anforderungen z.B. FS, KRITIS

Bedarfsermittlung (Versicherungssumme)

- Bedarfsgerechte Ermittlung der relevanten Deckungssummen
- Drittschaden/Eigenschaden: Wesentliche Bausteine (Betriebsausfall, Wiederanlauf etc.)

Versicherungsschutz im Konzern

- Sicherstellung der Absicherung aller betroffenen Gesellschaften im Konzern
- Dynamische Einbindung auch künftiger Konzerngesellschaften

Abstimmung mit dem Versicherer

- Klare Benennung des Deckungsumfangs
- Abstimmung klarer Kommunikationswege und Zuständigkeiten auch für den Schadenfall

Anzeigepflichten

- Einhaltung vorvertraglicher Pflichten ggü. dem Versicherer
- Wahrheitsgemäße Beantwortung von Fragebögen zu IT-Security und Systemstandards

Versicherungsschutz und Regulierung von Ansprüchen

Während der Vertragslaufzeit

Fortwährende Risikoanalyse
- Identifikation neuer Risiken oder Änderung des Risikoumfangs

Aktualisierung der Versicherungssumme(n)
- Anpassung an Vermehrung oder Änderung der Risiken

Einhaltung etwaiger Obliegenheiten
- Durchführung regelmäßiger Softwareupdates, „Stand der Technik“

Versicherungsschutz im Konzern
- Regelmäßige Betrachtung (neuer) Gesellschaften und (neuer) Geschäftsmodelle

Interne Strukturen und Maßnahmen
- Dokumentation und Schulungen, Notfall-/Reaktionspläne/Schadenmanagement

Versicherungsvertragsmanagement
- Überblick und rechtzeitiges Handeln betreffend Verlängerung, Kündigung etc.

Versicherungsschutz und Regulierung von Ansprüchen

Im konkreten Schadenfall

Schadenmeldung

- Unverzügliche Meldung des Schadens an den Versicherer

Minimierung des Schadens

- Obliegenheit zur Schadensminderung, ggf. mit externer Beraterunterstützung
- Begrenzung von Datenschutz-Vorfällen, technische Eingrenzung etc.

Zusammenarbeit mit externen Dienstleistern

- Austausch mit z.B. Forensik zur schnellstmöglichen Wiederherstellung der IT
- Zusammenarbeit mit Gutachtern zur Feststellung möglicher (Eigen-)Schäden

Wiederherstellung der Arbeitsfähigkeit

- Schneller Wiederanlauf der wesentlichen IT, Nutzung interner Pläne/Kommunikation

Kommunikation mit Behörden/Geschädigten

- Stetige Gespräche mit (Datenschutz-)Behörden bzw. Geschädigten (Haftpflicht) führt zu Schadenminimierung und ggf. schnellerer Schadenregulierung durch Versicherer

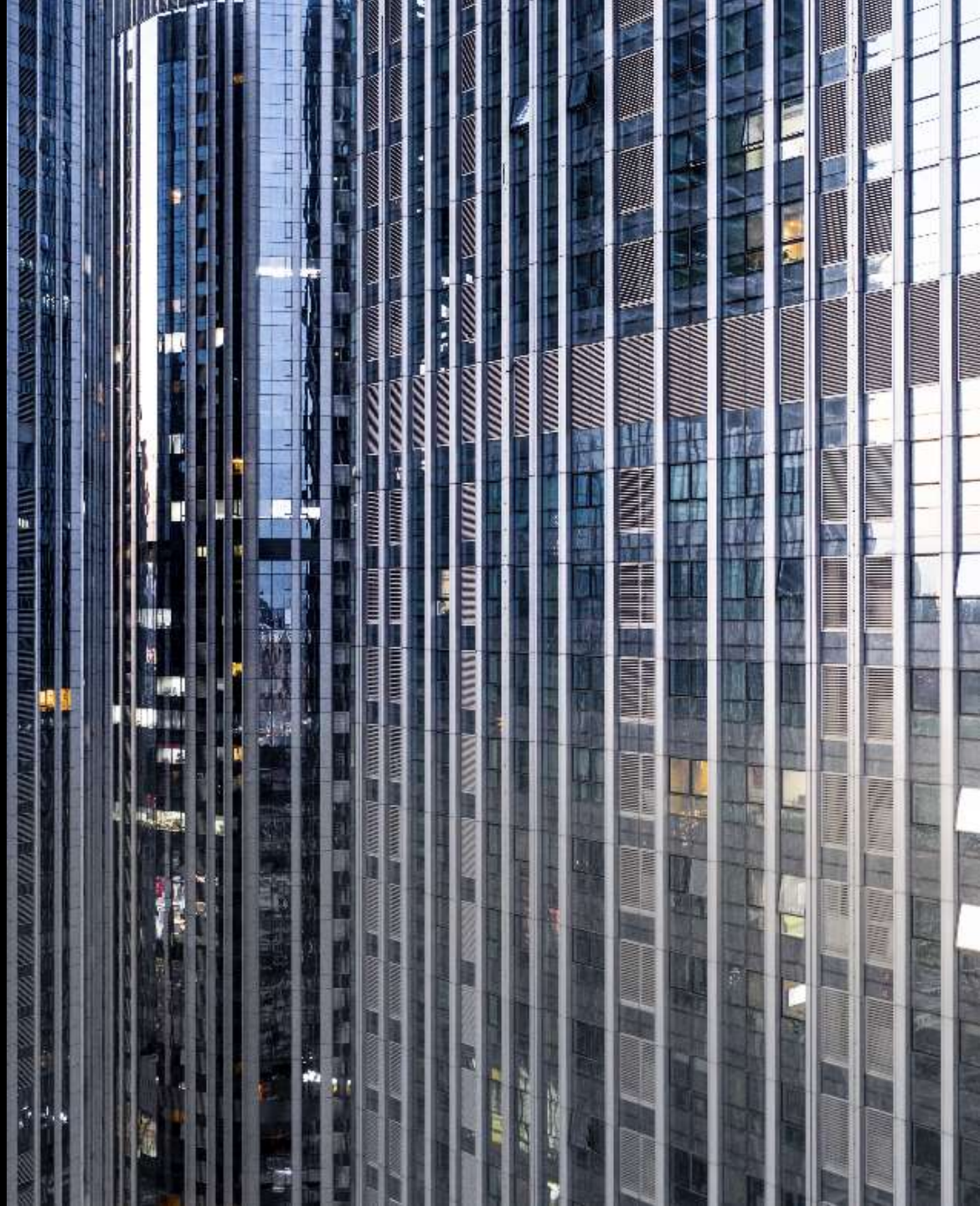
Interne Strukturen und Maßnahmen

- Optimierung der IT/Behebung von Sicherheitslücken zur Vermeidung künftiger Angriffe
- Anpassung der relevanten Dokumemtation, Lektionen aus dem Schadenfall (Abläufe)

Q&A

Vielen Dank für Ihre Aufmerksamkeit

Weitere Informationen



Ihr Kontakt

Helmut Brechtken
Financial Advisory
Partner | Head of Digital Forensic Incident Response
Deloitte GmbH

Tel.: +49 221 9732 4949
E-Mail: hbrechtken@deloitte.de

Nikola A. F. Werry, LL.M. (UK)
Digital Law | Head of Data and Data Protection Law
Partnerin, Rechtsanwältin
Deloitte Legal Rechtsanwaltsgesellschaft mbH

Tel.: +49 69 71918 8482
E-Mail: nwerry@deloitte.de

Frank Fischer, LL.M. (Univ. London)
Banking & Finance | Head of Insurance & Invest. Mgmt
Partner, Rechtsanwalt
Deloitte Legal Rechtsanwaltsgesellschaft mbH

Tel.: +49 89 29036 5680
E-Mail: frankfischer@deloitte.de

Ihr Ansprechpartner Helmut Brechtken

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).

Ihr Ansprechpartner Frank Fischer

Frank Fischer, LL.M. (Univ. London)

Partner
Banking & Finance | FSI | Head of Insurance & Investment Management

Rechtsanwalt

Frank Fischer ist seit über 15 Jahren als Rechtsanwalt im Bereich Legal Financial Services tätig und leitet als Partner den Versicherungsbereich sowie den Bereich Investment Management von Deloitte Legal in Deutschland.

Er berät Erst- und Rückversicherer, Versicherungsvermittler, EbAV, Banken, Finanzdienstleister und Asset Manager in allen Bereichen des Aufsichtsrechts und den Schnittstellen zum Gesellschaftsrecht und weiteren Gebieten. Regelmäßig steht er seinen Mandanten in Transaktionen, in Transformationsprojekten und in Verfahren gegenüber der BaFin zur Seite.

Frank war vor seiner Tätigkeit bei Deloitte Legal u.a. Rechtsanwalt in einer anderen Big4-Rechtsanwaltsgesellschaft und Assistant General Counsel eines führenden Asset Managers für institutionelle Investoren. Er hat umfassende Erfahrung bei der Lösung rechtsgebietsübergreifender Problemstellungen im Konzern sowie der Geschäftsleiter-Beratung zu Haftungs-, Struktur- und Organisationsthemen (Corporate Governance & Compliance).

Ihre Ansprechpartnerin Nikola Werry

Nikola A. F. Werry, LL.M. (UK)

Partnerin
Digital Law | Head of Data & Data Protection Law

Rechtsanwältin

Nikola Werry ist Partnerin bei Deloitte Legal am Standort Frankfurt am Main und in der Service Line Digital Law tätig. Nikos fachlicher Fokus liegt auf dem IT- und Datenschutzrecht und rechtlichen Fragen rund um Digitalisierung. Sie verfügt über eine breite Erfahrung im Hinblick auf die Begleitung und Beratung nationaler und internationaler Unternehmen zu Aspekten im Zusammenhang mit der rechtssicheren Konzeptionierung und Implementierung digitaler Produkte, Strategien und Geschäftsmodelle. Durch ihre Erfahrung im Markt sowie ihre Expertise bei der Führung multidisziplinärer Teams im Rahmen von komplexen Beratungsprojekten unterstützt Niko ihre Mandanten nicht nur bei den rechtlichen Herausforderungen eines Projekts, sondern berät auch bei der Bewältigung der zahlreichen organisatorischen, wirtschaftlichen und prozessualen Herausforderungen, mit denen diese im Laufe eines Projekts konfrontiert sind.

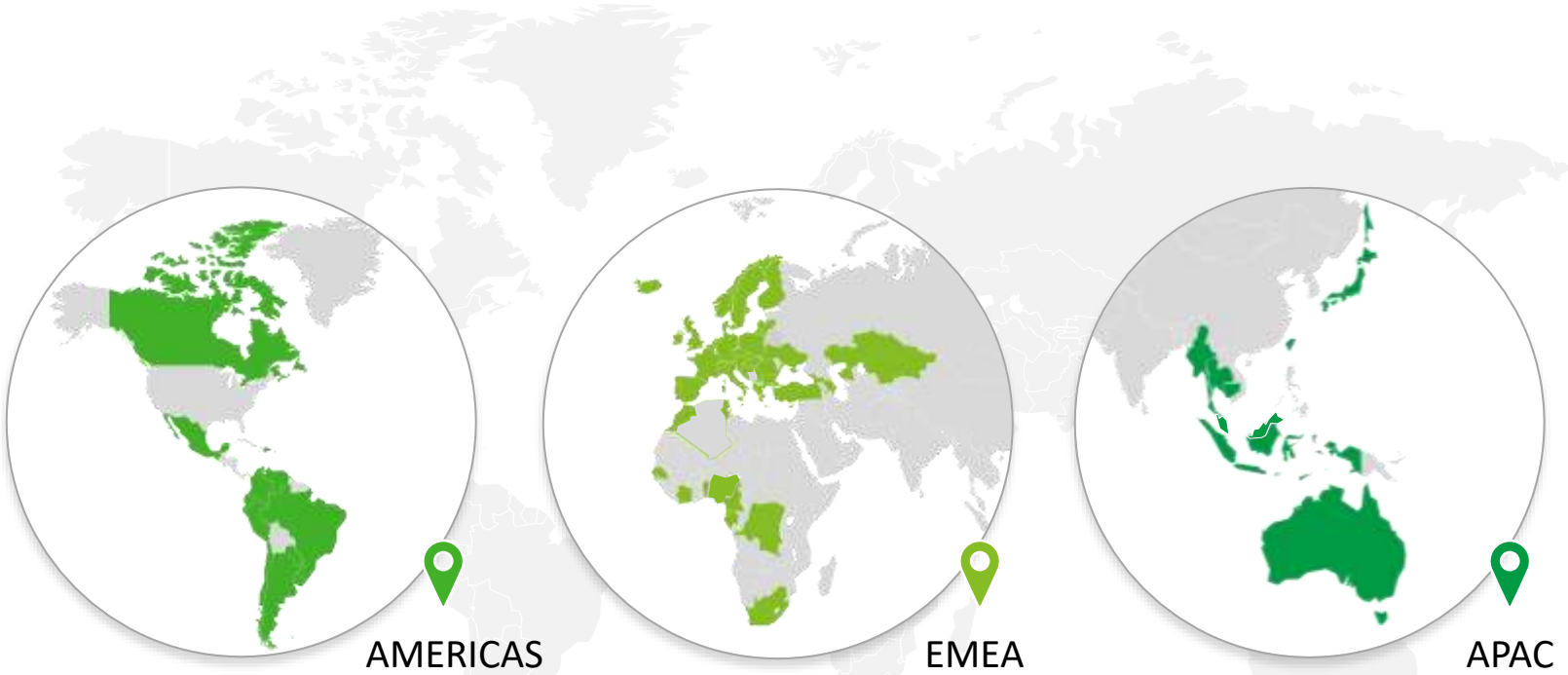
Niko hält regelmäßig Vorträge, Workshops und Webinare zu verschiedenen Themen im Bereich Digitalisierung und veröffentlicht regelmäßig Fachartikel. Sie ist daneben Herausgeberin und Autorin des Handbuchs „Datenrecht in der Digitalisierung“, welches das Datenrecht erstmals in seinen einzelnen Facetten beleuchtet und definiert. Daneben ist Niko u.a. Gründerin eines Fachnetzwerks für Datenrecht und Digitalisierung sowie Vorstandsmitglied der Forschungsstelle für Rechtsfragen neuer Technologien und Datenrecht (ForTech) an der Universität Bonn.

Sie wird im Best-Lawyers-Ranking im Bereich Data Security und Privacy Law unter den "Ones to Watch 2024" gelistet.

Deloitte Legal ist weltweit stark aufgestellt

Es kann sehr herausfordernd sein, eine Vielzahl von Rechtsberatern rund um die Welt zu koordinieren, ohne dabei einzelne Aspekte aus den Augen zu verlieren.

Als eine der weltweit führenden Rechtsberatungen unterstützt Deloitte Legal Sie bei der Bewältigung von Herausforderungen und der Verwirklichung Ihrer Vision; dabei ist Deloitte Legal Ihr zentraler Kontakt für Ihren weltweiten juristischen Beratungsbedarf.



Deloitte Legal practices

AMERICAS

1. Argentina
2. Brazil
3. Canada
4. Chile
5. Colombia
6. Costa Rica
7. Dominican Republic
8. Ecuador
9. El Salvador
10. Guatemala
11. Honduras
12. Mexico
13. Nicaragua
14. Paraguay
15. Peru
16. Uruguay
17. Venezuela

EMEA

1. Albania
2. Austria
3. Azerbaijan
4. Belgium
5. Benin
6. Bosnia and Herzegovina
7. Bulgaria
8. Cameroon
9. Croatia
10. Cyprus
11. Czech Republic
12. Dem. Rep. of Congo
13. Denmark
14. Equatorial Guinea
15. Finland
16. France
17. Gabon
18. Georgia
19. Germany
20. Greece
21. Hungary
22. Iceland
23. Ireland
24. Italy
25. Ivory Coast
26. Kazakhstan
27. Kosovo
28. Latvia
29. Lithuania
30. Malta
31. Morocco
32. Nigeria
33. Norway
34. Poland
35. Portugal
36. Romania
37. Senegal
38. Serbia
39. Slovakia
40. Slovenia
41. South Africa
42. Spain
43. Sweden
44. Switzerland
45. The Netherlands
46. Tunisia
47. Turkey
48. Ukraine
49. United Kingdom

APAC

1. Australia
2. Cambodia
3. Hong Kong SAR, China
4. Indonesia
5. Japan
6. Malaysia
7. Myanmar
8. Singapore
9. Taiwan
10. Thailand

Erleben Sie die Zukunft der Rechtsberatung schon jetzt

Deloitte Legal, das sind

mehr als **2.500** Rechtsanwälte

in **75+** Ländern

die eng zusammenarbeiten
über nationale Grenzen hinweg und gemeinsam mit anderen Deloitte-Geschäftsbereichen

Services von Deloitte Legal

Unsere drei sich überschneidenden Servicebereiche ermöglichen es uns, unsere Mandanten wann und wo benötigt und in der jeweils optimal geeigneten Form bei der Realisierung ihrer Visionen zu beraten.

Rechtsberatung

Modelle, Konzepte und Systeme zur Effizienzsteigerung

Outsourcing und Legal Managed Services

Wir schaffen (Mehr)Werte

Als Teil des weltweiten Deloitte-Netzwerks arbeitet Deloitte Legal mit einer Vielzahl anderer Fachrichtungen zusammen und bietet multinationale juristische Lösungen und weltweit integrierten Service:

in Einklang
mit Ihrer unternehmensweiten Vision

maßgeschneidert
für Ihre Geschäftsbereiche und Niederlassungen

technologiegestützt
für verbesserte Zusammenarbeit und Transparenz

abgestimmt
auf Ihre regulatorischen Anforderungen

Deloitte Legal