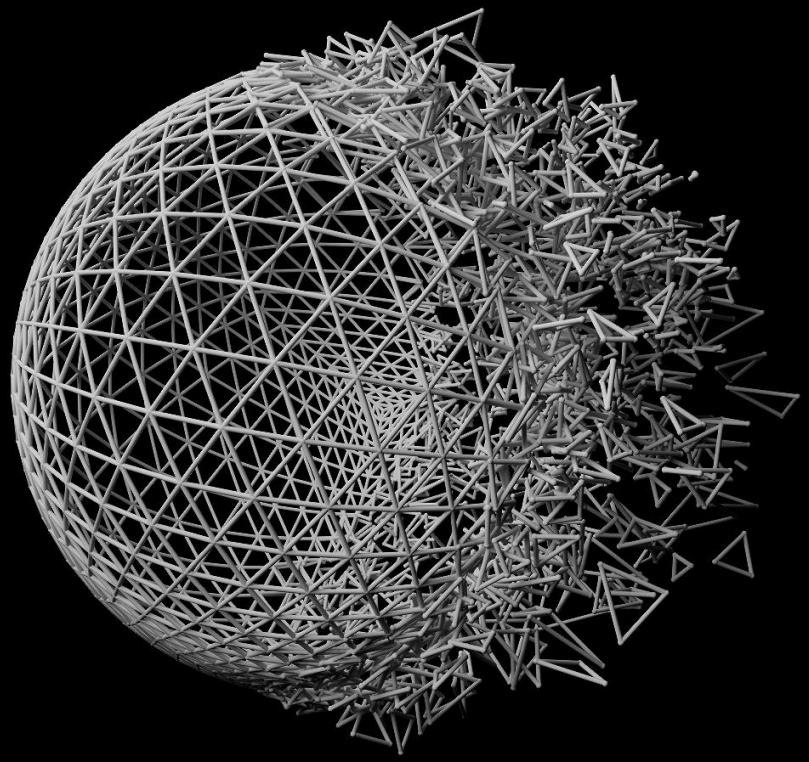
Deloitte.
Legal



Cyber Security im kommunalen Sektor – wie sichern wir die Kommunen? Aktuelle Herausforderungen und Entwicklungen der Cyber-Sicherheit

Deloitte Legal Webcast | 12. Oktober 2022, 11.00 - 11.45 Uhr

Vorstellung & Gliederung

Referenten

Deloitte Legal

Danny Essing
Government & Public Sector
Rechtsanwalt
Partner

Tel.: +49 211 877201
E-Mail: dessing@deloitte.de

Rafael Sarlak
Government & Public Sector
Rechtsanwalt
Associate

Tel.: +49 211 877201
E-Mail: rsarlak@deloitte.de

Deloitte – Risk Advisory

Michael Müller
Risk Advisory | Crisis & Resilience
Partner

Tel.: +49 30 2546 85225
E-Mail: micmueller@deloitte.de

André Roosen
Risk Advisory | Cyber Strategy
Government and Public Services
Director

Tel.: +49 30 254 68327
E-Mail: aroosen@deloitte.de

Agenda

Wie sieht die aktuelle Cyber-Sicherheitslage in Deutschland aus?

Welche rechtlichen Pflichten treffen kommunale Entscheidungsträger, Geschäftsführer und Aufsichtsräte im Bereich Cyber-Sicherheit?

Wer haftet wie für die Folgen eines Cyber-Angriffs?

Welche Maßnahmen zur Vermeidung von IT-Sicherheitsvorfällen sind im kommunalen Bereich unbedingt vorzunehmen?

Wie sieht eine Incident Response im Falle von erfolgreichen IT-Angriffen aus?

Was zeichnet ein erfolgreiches Krisenmanagement aus? Welche Besonderheiten sind im kommunalen Bereich zu beachten?

Beantwortung Ihrer Fragen (Q&A)

Prolog:

Cyber-Sicherheitslage in Deutschland

Cyber-Sicherheitslage in Deutschland

Aktuelle Presseberichterstattung

Anhalt-Bitterfeld

Landkreis erhält Lösegeldforderung nach Cyberattacke

IT-Sicherheit

Bochum erleidet Cyber-Angriff 400 Mitarbeiter tappen in Phishing-Falle

Informationstechnologie

Cyberangriff auf IT-Systeme von Schwerin zieht Kreise

IM NOTBETRIEB

Cyberangriff auf Stadtwerke Pirna

von MDR SACHSEN

Stand: 06. Dezember 2021, 20:15 Uhr

Kriminelle haben vergangene Woche die Computer der Stadtwerke Pirna angegriffen. Ein Zugriff auf einen Teil der Systeme ist nicht möglich, so das Unternehmen, die Versorgungssicherheit sei jedoch gewährleistet.

LANDKREIS LIEGT LAHM

Erster Cyber-Katastrophenfall in Deutschland

Hacker veröffentlichen Daten nach Angriff auf Stadt Witten

Nach dem Angriff auf die Stadt Witten ist nicht nur die Verwaltung offline. Es sind wohl auch Daten abgeflossen, die nun veröffentlicht wurden.

Katastrophenfall in Sachsen-Anhalt

Hacker stellen persönliche Daten von Abgeordneten ins Darknet

Russischer Cyberangriff

FSB-Hacker spionierten deutsches Stromnetz aus

28.07.2022, 14:32 Uhr

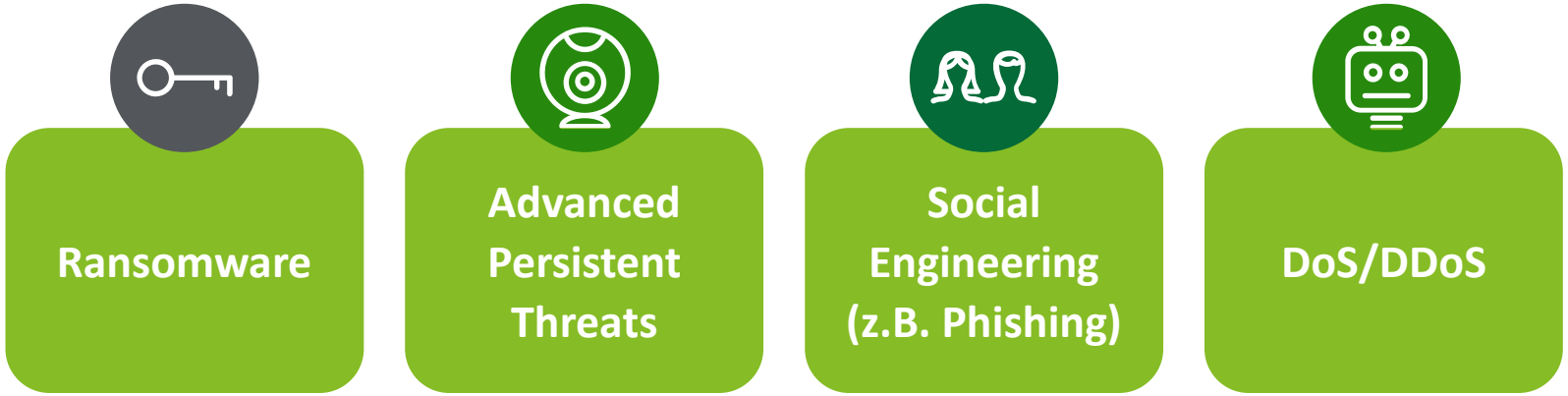
ENTEGA, FES & STADTWERKE

Cyberangriff hat Auswirkungen auf Mainzer Mobilität

Ein Hackerangriff auf einen IT-Dienstleister betrifft auch den öffentlichen Nahverkehr in Mainz und Umgebung. Beispielsweise können Fahrten ausfallen.

Update zur Cyber-Sicherheitslage in Deutschland

- Lage der IT-Sicherheit in Deutschland ist insgesamt angespannt bis kritisch*
- Im Kontext des Krieges in der Ukraine: weiter erhöhte Bedrohungslage*
- Hohe Anzahl der IT-Systeme im Homeoffice, ihre Verbindung mit dem Unternehmensnetz und die verstärkte Nutzung von Kollaborationstools bieten eine vergrößerte Angriffsfläche gegenüber Cyber-Angriffen**
- Häufigste Methoden der Cyber-Angriffe:



* BSI, Update vom 3. August 2022 zum Bericht zur Lage der IT-Sicherheit in Deutschland 2021
** Deloitte, Cyber Security Report 2021

Die rechtliche Perspektive:

Organpflichten in Unternehmen und Verwaltungen zur Abwehr von Cyber-Angriffen

Im kommunalen Sektor besteht regelmäßig eine besondere Verantwortung zum Schutz von IT-Infrastruktur

- Funktionierende IT-Infrastruktur hat für Unternehmen & Verwaltung herausragende Bedeutung
- Verantwortliche im kommunalen Bereich (Geschäftsleiter/Verwaltungsleiter) sind in besonderem Maße dazu verpflichtet, organisatorische Maßnahmen zum Schutz der IT-Systeme zu treffen

- Kommunen und kommunale Unternehmen sind regelmäßig **Betreiber von KRITIS**

- **§ 8a BSIG:** Pflicht zum Treffen von organisatorischen und technischen Vorkehrungen zum Schutz informationstechnischer Systeme, Komponenten oder Prozesse

- Kommunen und kommunale Unternehmen sowie deren Geschäfts-/ Behördenleitung sind **Verantwortliche** i.S.d. DSGVO

- **§ 32 DSGVO:** Pflicht zum Treffen geeigneter technischer und organisatorischer Maßnahmen, um ein angemessenes Schutzniveau vor dem Risiko einer Datenschutzverletzung zu gewährleisten

Die Geschäfts-/Behördenleitung und das Aufsichtsgremium sorgen jeweils als Kollegialorgane für ein angemessenes Schutzniveau der IT

- Aufbau, Ausstattung und Kontrolle einer geeigneten IT-(Sicherheits-)Struktur ist Teil der Pflicht zum Aufbau einer funktionsfähigen IT-Compliance als Teil der Organisationsverantwortung

Schutzziel der IT-Compliance-Maßnahmen

- IT-Compliance Maßnahmen dienen dem **Schutz von Hardware, Software** und **Daten**
- Zu treffenden Maßnahmen sind abhängig vom **Risikograd**, der **Höhe eines möglichen Schadens** sowie dessen **Eintritts-wahrscheinlichkeit**

Zuständigkeiten in der Geschäfts-/Verwaltungsleitung

- IT-Sicherheit ist Aufgabe des **(Gesamt-)Organs**
- **Delegation** an einzelnes Mitglied ist möglich
- Überwachungsverantwortung bleibt beim Gesamtvorstand

Zuständigkeiten des Aufsichtsrates

- **Aufsichtsrat** trägt als Gesamt-organ die Verantwortung für eine ordnungsgemäße Überwachung
- Art, Umfang, Häufigkeit der Berichterstattung an AR in Abhängigkeit der individuellen Verhältnisse
- Einrichtung eines IT-Ausschusses des AR möglich

IT-Sicherheit ist ein dauerhafter Prozess und kann im Rahmen eines ISMS gesteuert werden

- Informationssicherheit ist eine **Daueraufgabe** in einem dynamischen Risikoumfeld
- Der Schlüssel zur Informationssicherheit ist ein übergreifendes und systematisches Managementsystem für Informationssicherheit (ISMS).
  - **ISO 27001** ist der internationale Standard – aber für kleine Einheiten ggf. überfordernd
  - **CISIS12** insbesondere **für KMU und Behörden** gedacht
- ISMS beinhalten ein Plan-Do-Check-Act-Modell (**PDCA**), um IT-Sicherheit als fortlaufenden Prozess zu implementieren
- Wichtig: Dokumentation zu Nachweiszwecken

Spezialisierte Einheiten auf Landesebene bieten Kommunen und ihren Unternehmen Unterstützung bei der Abwehr von Cyber-Gefahren an:

CYBER COMPETENCE CENTER HESSEN

SAX.CERT Computer Emergency Response Team des Freistaates Sachsen

CERT Nord Bremen Schleswig-Holstein Hamburg Sachsen-Anhalt

Bayern-CERT

Haftungsfragen bei Pflichtverletzungen

Durch Cyber-Attacken ausgelöste Schäden können existenz-bedrohende Haftungsfolgen auslösen

- **Schäden & Kosten**, die durch erfolgreiche Cyber-Angriffe verursacht werden, sind vielfältig:

Kosten für Systemwieder-herstellung

Schadenersatz-ansprüche

Umsatz-einbußen

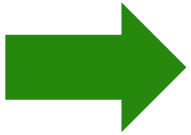
Beraterkosten

Reputations-schäden

Geldbußen (nicht gegen Behörden & öff. Stellen)

Schadenersatzanspruch nach § 82 DSGVO (auch direkt gegen Geschäfts-/ Behördenleitung als „Verantwortliche" i.S.d. DSGVO)

- **Haftungsbeschränkungen** für Cyberrisiken gegenüber den Kunden und Lieferanten sind **kaum zulässig**
- Verantwortliche für die Cyber-Angriffe können in der Regel nicht ausgemacht werden



Letzte Möglichkeit für Unternehmen/Behörde, um Schadensersatz zu erlangen: Haftung der Geschäfts-/Behördenleitung

Eine Innenhaftung kann nur vermieden werden, wenn der Geschäfts-/Behördenleiter seine (Amts-)Pflichten erfüllt

Haftung der Geschäftsleitung

- Nach § 93 Abs. 2 AktG (bzw. § 43 Abs. 2 GmbHG) mit **gesamten Privatvermögen** für Pflicht-verletzungen bei Ausübung der Geschäftsführung
- Geschäftsleitung kommt ihren **Organisationspflichten** nur dann nach, wenn „sie eine auf Schadens-prävention und Risikokontrolle angelegte Compliance-Organisation einrichtet“ (vgl. „Neubürger-Urteil“)

Haftung der Aufsichtsräte

- Nach §§ 116, 93 Abs. 2 AktG mit **gesamten Privatvermögen** für Pflichtverletzungen bei Ausübung der Aufsicht über Geschäftsführung
- Bei **fakultativen AR** einer GmbH Haftung über Verweis von § 52 GmbHG ins Aktiengesetz, soweit im Gesellschaftsvertrag nicht anders festgelegt

Haftung des HVB

- HVB haften gem. der jeweiligen Landesgesetze in entsprechender Anwendung der **allg. beamtenrechtlichen Regeln** (vgl. § 118 LBG NRW, § 92 LBG BaWÜ)
- Nach § 48 BeamtStG (und der Landesbeamtengesetze) Haftung des Beamten **für Vorsatz und grobe Fahrlässigkeit**
- **Organisationsverschuldens** kann haftungsbegründende Amtspflichtverletzung sein

- Zusätzlich zur Haftung für Pflichtverletzung ggü. Unternehmen/Behörde aus Organstellung: **persönliche Haftung des Verantwortlichen aus § 82 DSGVO** ggü. der verletzten Person
- Nur wenn das Mitglied der Geschäftsführung / des Aufsichtsrates / der HVB beweisen kann, dass es seine (Amts-)Pflichten erfüllt hat kommt eine Haftungserleichterung nach den Grundsätze der **Business Judgement Rule** in Frage (Safe Harbour)

Key take aways

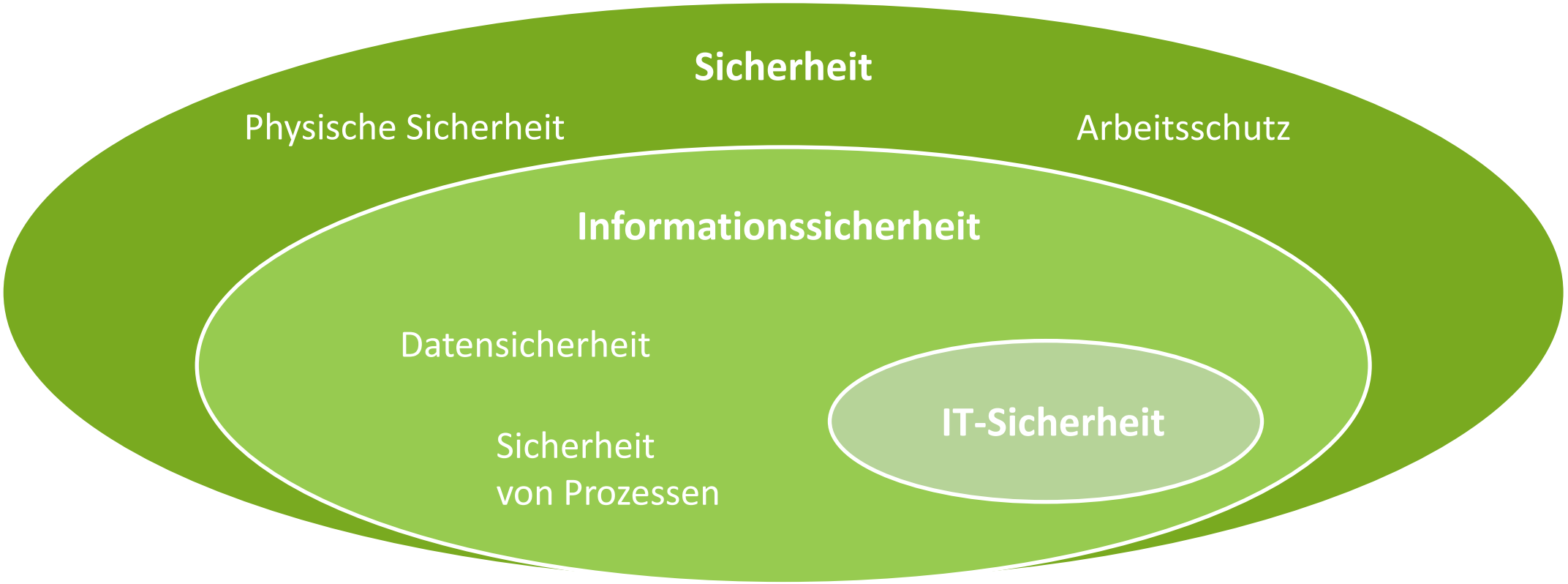
Key take aways

- Kommunen stehen verstärkt im Fadenkreuz von Cyberangriffen
- IT-Sicherheit ist als Organsationspflicht Chefsache
- Die Einrichtung eines (anerkannten) ISMS ist unbedingt zu empfehlen
- Gesetzesverstöße oder Verstöße gegen Organisationspflichten können zu persönlicher Haftung führen
- Spezialgesetzliche Haftungsnormen wie z.B. § 82 DSGVO geraten mit zunehmenden Cyber-Attacken stärker in den Fokus, verbunden mit erheblichen Rechtsrisiken
- Berücksichtigung von Angeboten der Länder (CERT und Co.) und/oder Einbindung von Beratern

Cyber Security & Resilience

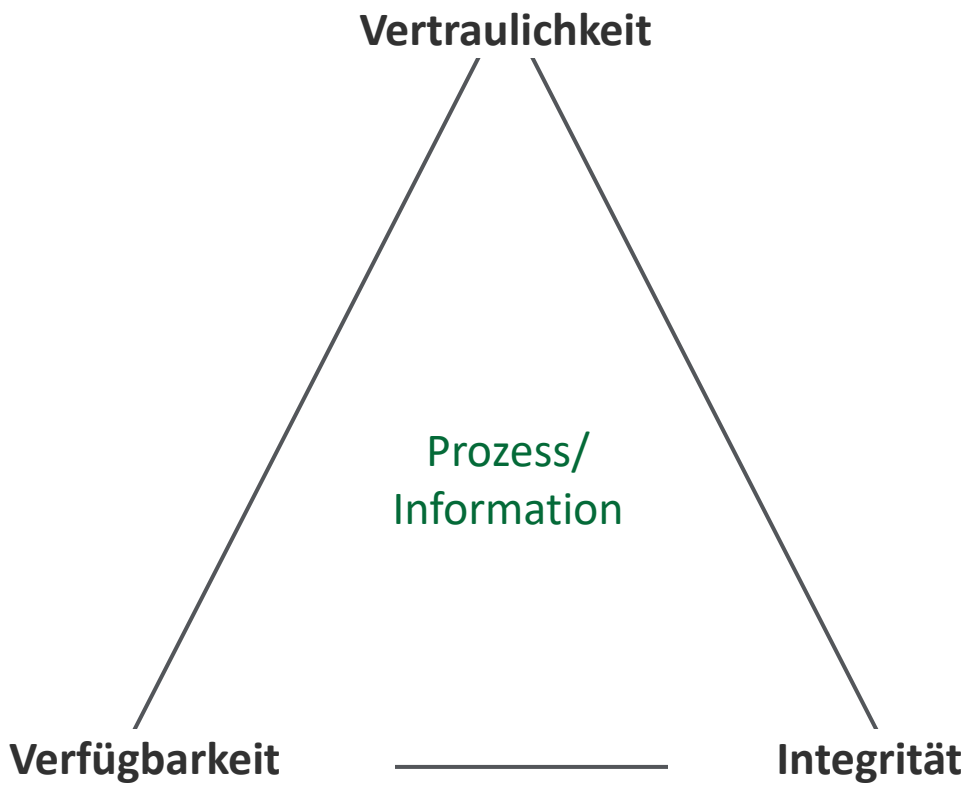
Grundlagen der Informationssicherheit

Was ist „Informationssicherheit“ und was ist „IT-Sicherheit“ ?



Grundlagen der Informationssicherheit

Was bedeutet es, Informationen zielorientiert zu schützen?



BESCHREIBUNG

Vertraulichkeit (Confidentiality) – C:

Gewährleistung des Zugangs zu Informationen nur für Zugangsberechtigte

Integrität (Integrity) – I:

Sicherstellung der Richtigkeit und Vollständigkeit von Informationen/Verarbeitungsmethoden

Verfügbarkeit (Availability) – A:

Gewährleistung des bedarfsorientierten Zugangs zu Informationen für berechtigte Benutzer

Grundlagen der Informationssicherheit

Es sollten stets Sicherheitsmaßnahmen ergriffen werden, die dem Stand der Technik entsprechen

Stand von Wissenschaft und Technik

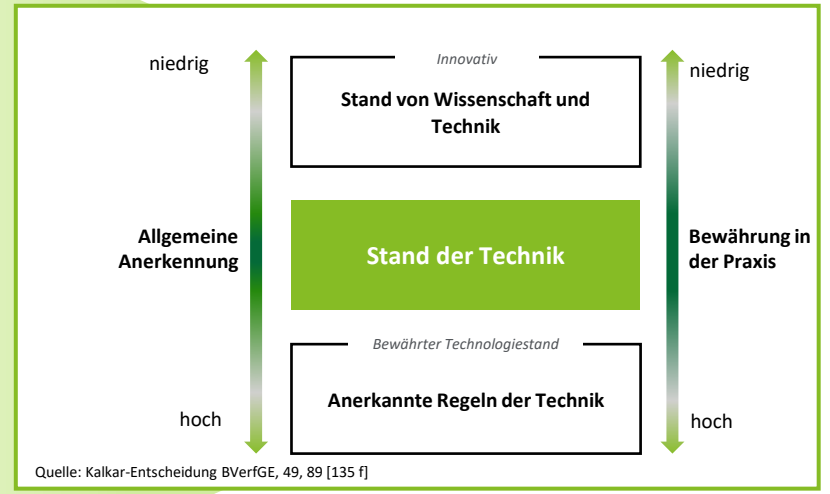
- Die neuesten technischen und wissenschaftlichen Erkenntnisse sind meist noch in der Entwicklung und gehen erst mit Erreichung der Marktreife in das Stadium „Stand der Technik“ über.

Stand der Technik

- Der Stand der Technik bezeichnet die am Markt verfügbare Bestleistung einer Sicherheitsmaßnahme zur Erreichung der vorgegebenen regulatorischen Ziele (bspw. DSGVO, BSI).
- Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die Erreichung eines allgemein hohen Schutzniveaus gesichert erscheinen lässt. Der rechtliche Maßstab für das Erlaubte oder Gebotene wird hierdurch an die Front der technischen Entwicklung verlagert.

Anerkannte Regeln der Technik

- Minimal-Standard, den man mindestens erwarten kann (Baurecht, z. B. § 319 StGB zur Baugefährdung)
- Die herrschende Auffassung unter den technischen Praktikern
- Bereits in der Praxis bewährt (z.B. DIN-Normen)



Quelle: Kalkar-Entscheidung BVerfGE, 49, 89 [135 f]

Die eingesetzte Technik sollte stets verhältnismäßig sein. Das heißt, sie müssen den tatsächlichen Bedürfnissen der Institution entsprechen und angemessen ausgewählt werden.

Grundlagen der Informationssicherheit

Auswahl an ISMS Standard in der Übersicht

Kriterien	ISIS12	ISO 27000-Reihe	BSI IT-Grundschutz
Herausgeber	Netzwerk Informationssicherheit für den Mittelstand[9]	International Standards Organisation[10]	Bundesamt für Sicherheit in der Informationstechnik[11]
Zielgruppe	Kleine und mittlere Unternehmen	Organisationen jeder Größenordnungen	Organisationen jeder Größenordnungen und öffentliche Verwaltung
Dokumentation	ca. 170 Seiten	ca. 400 Seiten	ca. 4.500 Seiten
Detaillierung	Mittel	Minimalistisch abstrakt	Maximal detailliert
Aufbau	Selektierte Bausteine + Maßnahmen	Maßnahmenempfehlungen	Umfassende Bausteine, Gefährdungen + Maßnahmen
Umfang des Maßnahmenkataloges	ca. 400 Maßnahmen	ca. 150 Maßnahmen	ca. 1.100 Maßnahmen
Risikoanalyse	indirekt	grundsätzlich	ergänzend
Umsetzung	konkret formulierte Maßnahmen umsetzen	allgemeingültig formulierte Maßnahmen umsetzen	konkret formulierte Maßnahmen umsetzen
Mögliche Zertifizierung	DQS-Zertifizierung	ISO-Zertifizierung	ISO-Zertifizierung nach IT-Grundschutz

Tabelle 1: Gegenüberstellung ausgewählter ISMS-Standards

Quelle: Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen

Die BSI Standards & IT-Grundschutz Kompendium

Übersicht über die aktuell verfügbaren BSI Standards

Die BSI-Standards zur Informationssicherheit

BSI-Standard 200-1:
Managementsysteme für Informationssicherheit (ISMS)

BSI-Standard 200-2:
IT-Grundschutz-Methodik

BSI-Standard 200-3:
Risikoanalyse auf der Basis von IT-Grundschutz

BSI-Standard 200-4:
Business Continuity Management

- Die BSI-Standards der Reihe 200-x, lösen seit Oktober 2017 die Reihe 100-x ab
- Zur erfolgreichen Migration auf den modernisierten IT-Grundschutz stellt das BSI eine „Anleitung zur Migration von Sicherheitskonzepten“ zur Verfügung
- Der BSI-Standard 200-4 befindet sich derzeit noch in der Finalisierung

Die BSI Standards & IT-Grundschutz Kompendium

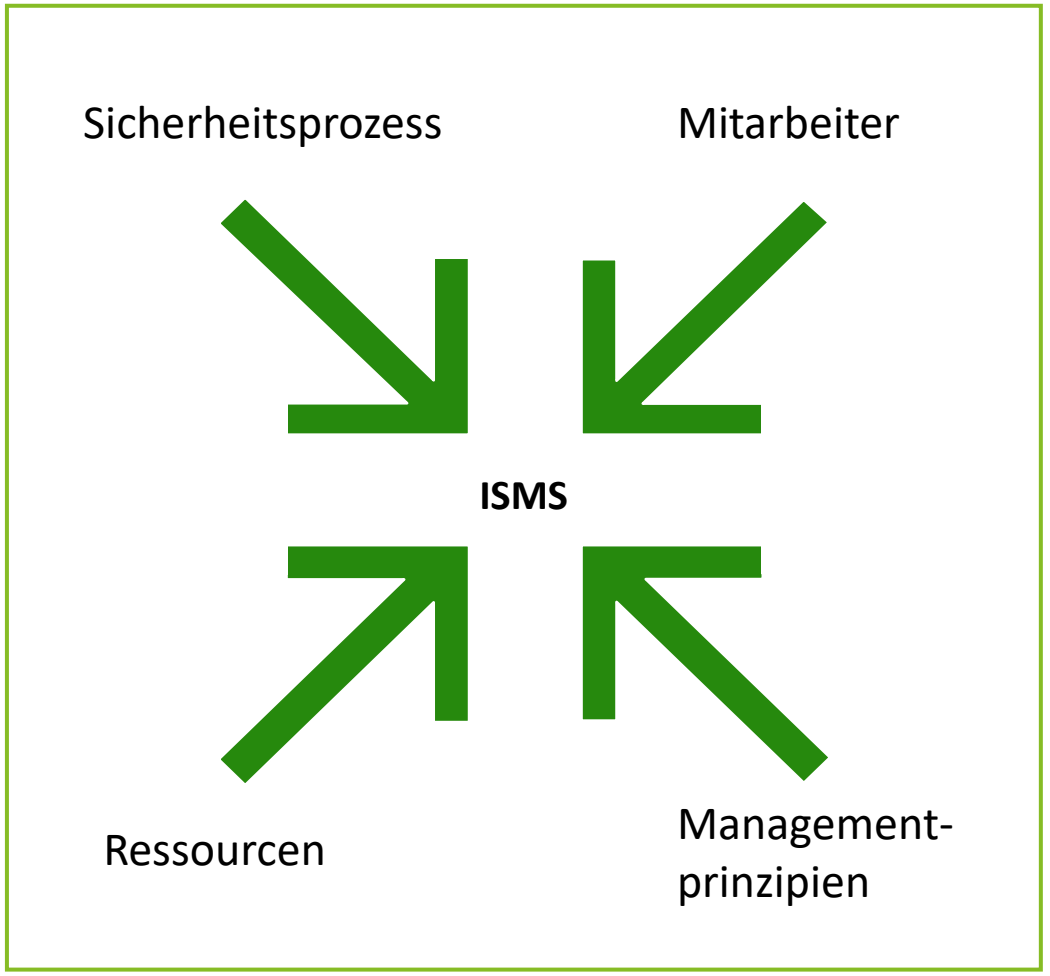
Was ist ein Informationssicherheitsmanagementsystem (ISMS)?

I nformation

S ecurity

M anagement

S ystem



Definition „ISMS“:

Ein ISMS ist die Aufstellung von Instrumenten, Methoden und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Die BSI Standards & IT-Grundschutz Kompendium

Management-Prinzipien

Aufgaben und Pflichten

Kommunikation und Wissen

Erfolgskontrolle im Sicherheitsprozess

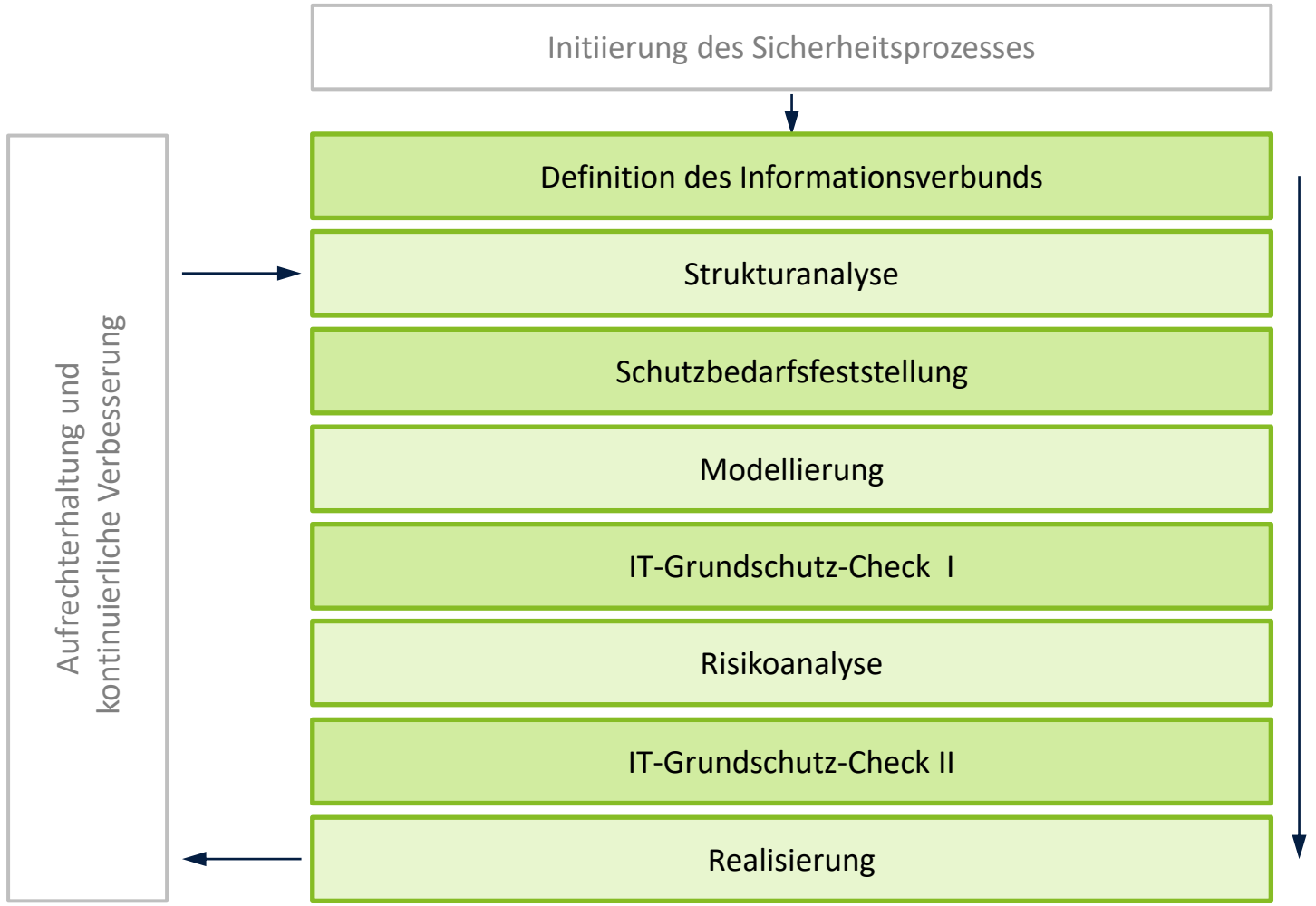
Kontinuierliche Verbesserung des Sicherheitsprozesses

Aufgaben und Pflichten

- Übernahme der Gesamtverantwortung für Informationssicherheit
- Informationssicherheit initiieren, steuern und kontrollieren
- Informationssicherheit integrieren
- Erreichbare Ziele setzen
- Sicherheitskosten gegen Nutzen abwägen
- Vorbildfunktion

Aufbau eines ISMS gem. BSI IT-Grundschutz

Vorgehensweise der IT-Grundschutz-Methodik



Cyber Security & Resilience

Verschiedene Krisenszenarien stellen unterschiedliche Herausforderungen an das Krisenmanagement. Gerade Cyber Krisen benötigen Führungsstärke und eingeübte Verfahren zur Bewältigung.

Eine Krise ist ein außergewöhnliches Ereignis mit einem hohen Maß an Unsicherheit, das die materiellen (Leistungserbringung, Eigentum, Gesundheit oder Sicherheit der Mitarbeiter und Kunden) und immateriellen Werte (Vertrauen, Ruf und Image) einer Organisation existentiell bedroht.

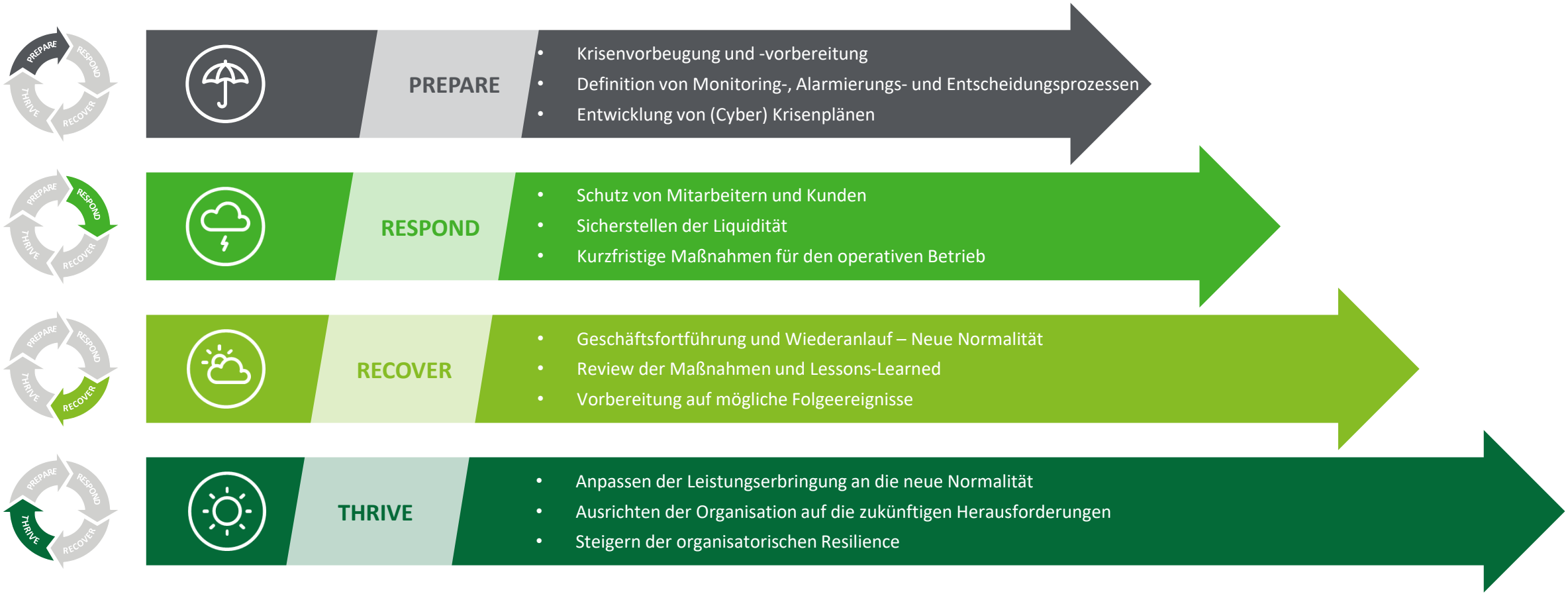
	COVID-19-PANDEMIE	Cyber Krisen
Risiko	**Unvorhersehbarkeit (Zeit); hohe Unsicherheit**	
Einfluss	"Kontinuierliche" Auswirkungen	Direkte (ad-hoc)Auswirkungen
Aufgabe	„Strategisch Folgen"	„Strategisch Führen"
Verantwortung	Verantwortung der Organe	Rechenschaftspflicht
Haftung	Haftung hat keine Priorität	Haftung von Anfang an ein zentrales Thema
Überwindung	Regierung/Regulierungsbehörden führen; ext. Entsch.	Management ist führend; meist interne Entscheidungen
Vertrauen	„Verständnisvolle" Stakeholder	Vertrauensverlust - keine "verzeihenden" Beteiligten

BEDEUTUNG DER EINBINDUNG DER OGANE

- Wenn eine Krise eintritt, **stehen die Verantwortlichen unter großem Druck**, die Krise zu lösen. Außerdem müssen sie unter Umständen ihre Handlungen und Entscheidungen verteidigen, während sie von der **Öffentlichkeit und den Medien beobachtet und bewertet** werden.
- Bei erfolgreicher Bewältigung kann die Führung die **positiven Eigenschaften einer Organisation demonstrieren** und ihre **Reputation verbessern**.
- Dies bedeutet, dass ***Leadership* in der Lage sein muss, in von Unsicherheit und Stress geprägten Situationen umsichtig zu agieren.** Dazu sind Situationsbewusstsein, Führungsstärke und **schnelle Entscheidungsfindung essentiell.**

Krisenmanagement als Stabilisator in einer Krise

Effektives Notfall- und Krisenmanagement verringert Ausmaß und Wahrscheinlichkeit negativer Auswirkungen auf die Leistungserbringung in Krisensituationen und ist Voraussetzung für einen souveränen Umgang mit einer Krise



Krisenmanagement als Stabilisator in einer Krise

Was zeichnet ein effektives Krisenmanagement aus?

Unternehmen

- **Resilience Kultur**
- Reputation des Krisenmanagements

Führung

- **Klare Verantwortungen**
- Kommunikation und Stakeholder-Management

Organisation

- **Lageanalyse und Entscheidungsfindung**
- Definierte Entscheidungs-kompetenzen

Wissen

- **Fähigkeiten der Organisation kennen**
- Explizites vs. Implizites Wissen

Krisenmanagement als Stabilisator in einer Krise

In Krisensituationen muss das Krisenmanagement drei essentielle Aufgaben erfüllen: schnelle Eskalation von Ereignissen, klare Führung sowie zielgerichtete Kommunikation an alle relevanten Stakeholder.

Eskalation

Schnelle, **konsequente** und **zielgerichtete** Alarmierung sowie Eskalation von Ereignissen

Führung

Klare Feststellung:

- **Wer führt?**
- Welche **anderen Rollen** existieren?

Planung

Rückgriff auf vorbereitete **Krisenpläne** und **Strukturen** zur **Kommunikation** mit Stakeholdern

Fragen & Antworten

Vielen Dank für Ihre Aufmerksamkeit!

Ihre Ansprechpartner

Deloitte Legal

Danny Essing
Government & Public Sector
Rechtsanwalt
Partner

Tel.: +49 211 877201
E-Mail: dessing@deloitte.de

Rafael Sarlak
Government & Public Sector
Rechtsanwalt
Associate

Tel.: +49 211 877201
E-Mail: rsarlak@deloitte.de

Deloitte – Risk Advisory

Michael Müller
Risk Advisory | Crisis & Resilience
Partner

Tel.: +49 30 2546 85225
E-Mail: micmueller@deloitte.de

André Roosen
Risk Advisory | Cyber Strategy
Government and Public Services
Director

Tel.: +49 30 254 68327
E-Mail: aroosen@deloitte.de

Experience the future of law, today

Mehr als
2,500
Anwälte

in
75+
Ländern

Nahtlose Zusammenarbeit

Grenzüberschreitend und mit andern Deloitte Business Lines

Als Teil des weltweiten Deloitte Professional Services Netzwerks, arbeitet Deloitte Legal eng mit Kollegen weltweit zusammen, um Mandanten eine integrierte Beratung und multinationale Lösungen zu bieten, die:

- **Konsistent** mit ihrer Unternehmensvision
- **Technologie-basiert** für eine bessere Zusammenarbeit und mehr Transparenz
- **Maßgeschneidert** auf die Unternehmensform und den lokalen Markt
- **Sensibilisiert** für die jeweiligen regulatorischen Bestimmungen

Deloitte Legal