HEUKING KÜHN LÜER WOJTEK

Cybersecurity

Themen und Aufgaben
in der Rechtsberatung

RECHTSANWÄLTE UND STEUERBERATER

Vorderstes Ziel unserer juristischen Beratung im Bereich Cybersecurity ist die Schaffung oder Wiederherstellung sicherer Prozesse und Abläufe innerhalb des Geschäftsbereichs unserer Mandanten. Da die Ursachen für fehlende Sicherheit bei der Verarbeitung von Daten oder in der IT-Sicherheitsinfrastruktur vielfältig sein können, kommt auch unser Beratungsansatz unterschiedlich, in jedem Fall aber angepasst auf die spezifischen Bedürfnisse unserer Mandanten daher.

Sie profitieren von unserer Expertise in allen relevanten Bereichen des IT- und Datenschutzrechts. Von der Implementierung eines umfassenden Informationssicherheits- oder Datenschutzmanagementsystems bis zum schnellen Eingreifen im Falle eines Cyberangriffs auf Ihre Systeme. Unsere Berater arbeiten standortübergreifend in schnell handlungsfähigen Tasks-Forces zusammen und sorgen dafür, dass Ihr Unternehmen schnell wieder einsatzfähig wird und dies langfristig auch weiterhin bleibt.

Auf den nachfolgenden Seiten geben wir Ihnen einen Überblick über die Schwerpunkte unserer IT-sicherheitsrechtlichen Praxis.

Datenschutzrecht

Die Bedeutung des Datenschutzes und der Datenschutz-Compliance nimmt nicht nur vor dem Hintergrund immer neuer Meldungen zu Bußgeld- und Schadensersatzprozessen stetig zu. Daher ist ein mit den datenschutzrechtlichen Vorgaben zu vereinbarendes Vorgehen bei der Verarbeitung personenbezogener Daten unerlässlich. In der Praxis stellen diese Vorgaben die Verantwortlichen immer wieder vor neue, komplexe Aufgaben, deren Bewältigung mit einem immensen Zeit- und Kostenaufwand verbunden sein kann.

Unser standortübergreifendes Team marktbekannter und ausgezeichneter Experten unterstützt Sie dabei, sowohl Einzelfragen zu beantworten, als auch umfangreiche Prozesse datenschutzkonform auszugestalten und die damit einhergehenden Risiken zu minimieren.

Beratung bei Datenschutz- und IT-Sicherheitsverstößen, insbesondere Cyber-Angriffen

In den vergangenen Jahren hat sich das Risiko für Unternehmen, Opfer von Cyberangriffen zu werden, dramatisch erhöht. Sollte es Angreifern gelingen, in interne Systeme einzudringen, sehen sich Unternehmen regelmäßig beträchtlichen Lösegeldforderungen, Bußgeldern und/oder erheblichem Reputationsverlust ausgesetzt.

Wir unterstützen Sie dabei, präventiv IT- und datenschutzrechtliche Schwachstellen Ihrer Infrastruktur zu erkennen und zu beheben. Sollten Sie Opfer eines Cyberangriffs werden, so helfen wir Ihnen mit unserem Netzwerk technischer IT-Sicherheitsberater bei der Incident and Emergency Response. Wir übernehmen für Sie die Kommunikation mit Ermittlungs- und Aufsichtsbehörden und unterstützen Sie dabei, die interne und externe Kommunikation zum Vorfall vorzubereiten und durchzuführen.

Emergency Response Plan

Im Falle eines Cyber-Angriffs gilt es vor allem, zügig zu handeln. Mit jeder Stunde, in der Geschäftsprozesse unterbrochen sind, entstehen weitere Schäden für betroffene Unternehmen. Daher sollten umgehend die erforderlichen Sofortmaßnahmen eingeleitet und ein Krisenstab gebildet werden, um das weitere Vorgehen zu koordinieren. Bei der Implementierung eines umfassenden Emergency Response Plans helfen wir Ihnen gerne und unterstützen Sie dabei, ein für Sie maßgeschneidertes Konzept zu entwickeln, mit dem Sie auf den Ernstfall vorbereitet sind.

Beratung bei der Einführung von Informationssicherheits- und Datenschutzmanagement-systemen (ISMS und DSMS)

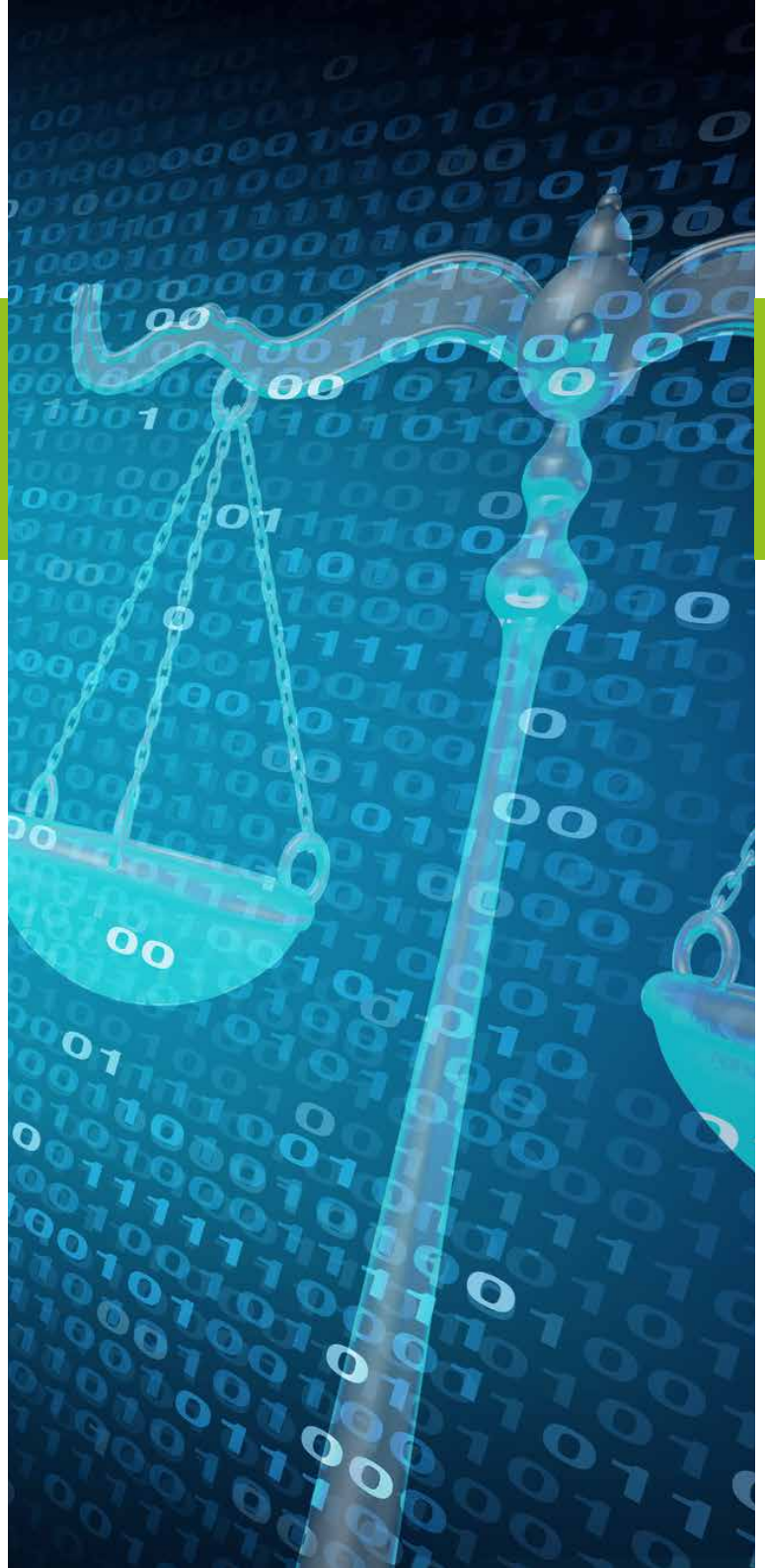
Moderne Sicherheitsstandards setzen eine Vielzahl wirkungsvoller, synergetisch wirkender Maßnahmen zum Schutz der IT-Infrastruktur voraus. Ein Informationssicherheitsmanagementsystem hilft Ihnen dabei, Verfahren und Regeln innerhalb Ihrer Organisation aufzustellen, um die Sicherheit, der von Ihnen verarbeiteten Informationen, dauerhaft zu gewährleisten und fortlaufend zu verbessern. Um die Einhaltung der besonderen Anforderungen der Verarbeitung personenbezogener Daten zu organisieren und dauerhaft zu gewährleisten, sollte daneben auch ein Datenschutzmanagementsystem eingeführt und betrieben werden.

Wir beraten Sie gerne dabei, Datenschutz- und Informationssicherheitsmanagementsysteme einzuführen und dafür zu sorgen, dass diese ineinandergreifen. Falls Sie dies wünschen, unterstützen wir Sie auch bei der Zertifizierung.

Prüfung von Rechtsfragen zum Stand der Technik

Der zentrale Begriff des IT-Sicherheitsrechts ist der des „Stands der Technik". Nicht nur im Bereich kritischer Infrastrukturen, sondern auch bei Anbietern von Telemedien, dem Einsatz von IT-Systemen bei Kreditinstituten, der Einführung technischer und organisatorischer Maßnahmen im Bereich des Datenschutzes, Policen von Cyber-Versicherungen und vielem mehr ist die Auslegung dieses Begriffs von zentraler Bedeutung und gleichzeitig rechtlich hochkomplex.

Auch die Abgrenzung zu „allgemein anerkannten Regeln der Technik" oder dem „Stand der Wissenschaft und Technik" stellen rechtlich eine nicht zu verkennende Anforderung dar. Nicht zuletzt aufgrund der technischen Expertise unserer auf IT-Sicherheitsrecht spezialisierten Rechtsanwälte beraten wir Sie gerne zum Fragen des Stands der Technik in allen für Sie relevanten Bereichen.



Managed Service und Service Level Agreements mit IT-Dienstleistern

Jedes Unternehmen steht vor der Frage, ob und in welchem Maße es sich bei der Verwaltung seiner IT-Infrastruktur der Unterstützung externer Dienstleister bedient. Die Inanspruchnahme solcher Managed Services, die in Abgrenzung zu anderen Arten des IT-Outsourcings regelmäßig wiederkehrende Leistungen betreffen, kann für Unternehmen lohnend sein, da eigene Ressourcen eingespart werden. Der Umfang der zu erbringenden Dienstleistung sollte jedoch in beiderseitigem Interesse vorher klar definiert und vertraglich festgehalten werden.

Die Schaffung von Transparenz über das erworbene Leistungsspektrum erfolgt durch den Abschluss eines Service Level Agreements, in dem vertraglich festgehalten wird, welche Leistungen das externe Unternehmen zu erbringen hat. Die Verhandlung dieses Vertrags erfordert im Einzelnen eine hohe Beratungs- und Verhandlungskompetenz, um Ihren Interessen optimal zur Geltung zu verhelfen.

Hierbei unterstützen wir Sie gerne.

Pflichten der Gesellschaftsorgane und Organhaftung

Cybersecurity ist Chefsache. Daher ist die angemessene Berücksichtigung IT-sicherheitsrechtlicher Anforderungen und die Einhaltung datenschutzrechtlicher Vorschriften für Unternehmen, unabhängig von ihrer Größe, unerlässlich. Unternehmen, die diesen Pflichten nicht nachkommen und unter Umständen auch ihren Organen drohen die Inanspruchnahme durch Vertragspartner oder eine Haftung gegenüber der Gesellschaft. Bei gravierenden Verstößen gegen solche Pflichten können im Übrigen empfindliche Bußgelder verhängt werden.

Mithilfe unseres ganzheitlichen Beratungsansatzes, können Sie ihre Haftungs- und Prozessrisiken bewerten und minimieren. Gerne unterstützen Sie unsere auf IT-Sicherheits-, Gesellschafts-, Versicherungsrecht und Compliance spezialisierten Rechtsanwälte bei der Implementierung und Durchsetzung geeigneter Maßnahmen, dem Abschluss einer D&O-Versicherung und notfalls der gerichtlichen Verteidigung gegen geltend gemachte Ansprüche.

KRITIS Betreiber und regulierte Industrien

Betreiber kritischer Infrastrukturen haben neben den allgemeinen IT-sicherheitsrechtlichen Anforderungen im Übrigen auch die Vorgaben des BSI-Gesetzes einzuhalten. Hierdurch haben Betreiber kritischer Infrastrukturen in besonderem Maße Sorge dafür zu tragen, dass die von ihnen betriebenen kritischen Infrastrukturen funktionsfähig sind und bleiben. Denn der Ausfall oder die Störung einer kritischen Infrastruktur hat erhebliche Folgen für eine Vielzahl von Personen.

Die erhöhten Anforderungen an Betreiber kritischer Infrastrukturen gelten sowohl hinsichtlich der eingesetzten Elemente, Komponenten und Bestandteile, als auch hinsichtlich der eingesetzten Software.

Produktsicherheit und Lieferketten bei IT- und Softwareprodukten

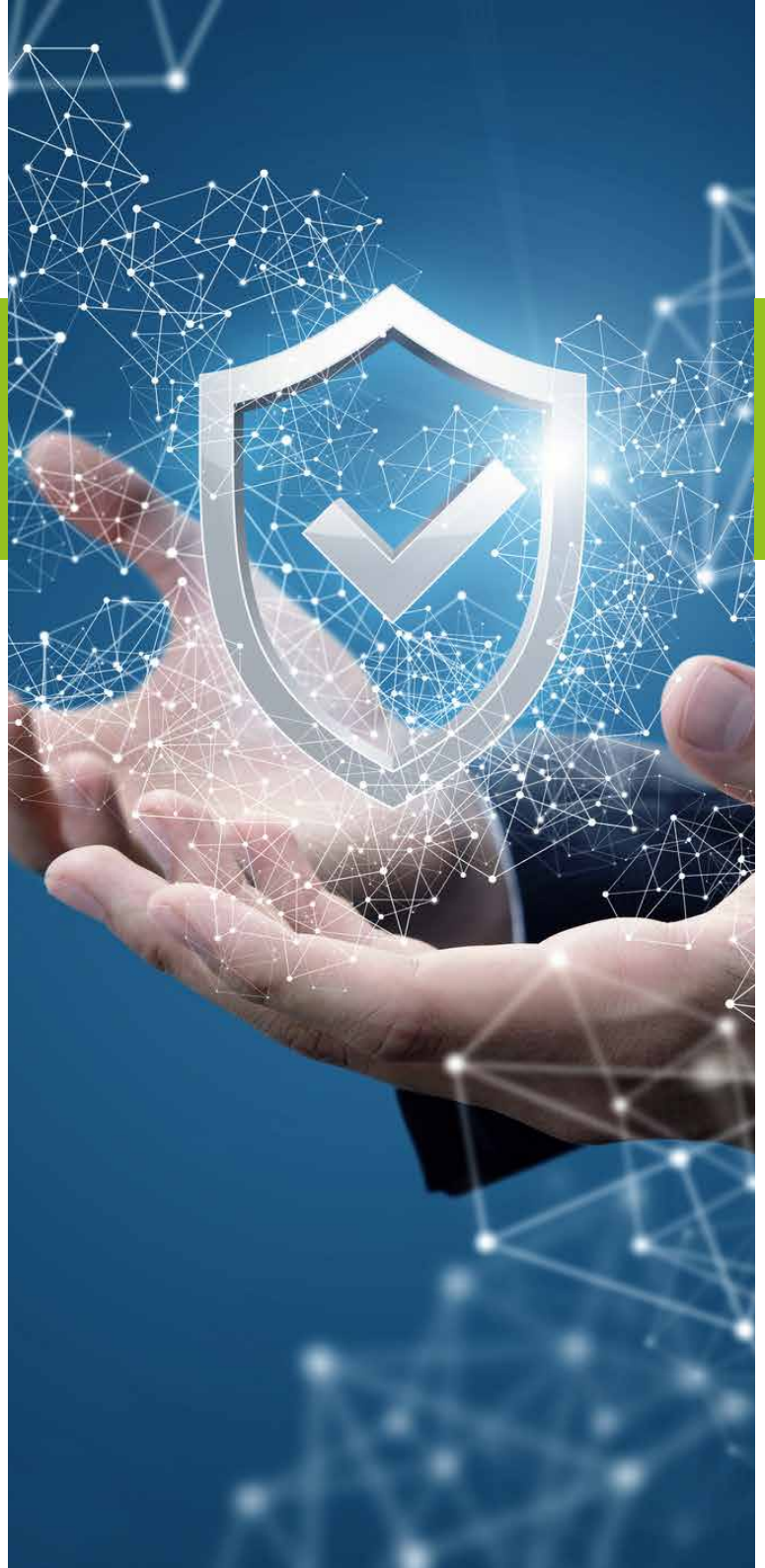
Immer häufiger erfolgen Cyberangriffe auch indirekt über externe Dienstleister. Wie bei jedem Cyberangriff, besteht auch im Falle eines indirekten Angriffs, also in Form eines Angriffs auf ein anderes Unternehmen innerhalb der Lieferkette ein herausragendes Haftungsrisiko für die betroffenen Unternehmen. Gerade vor dem Hintergrund immer neuer gesetzlicher und europarechtlicher Vorgaben, stehen Unternehmen beim Einsatz und Vertrieb von digitalen Produkten und digitalen Inhalten vor vielfältigen rechtlichen Fragestellungen.

Wir beraten Sie bei der Implementierung einer Strategie, welche unterschiedliche, synergetisch wirkende Maßnahmen zur Sicherung der Lieferkette verzahnt.

Cyber-Versicherung

Im Nachgang an einen IT-Sicherheitsvorfall können unter Umständen auch Gesellschaftsorgane, etwa handelnde Vorstände oder Geschäftsführer in Anspruch genommen werden. Wenn vorherige Schutzmechanismen nicht gewirkt haben, so sollte für den äußersten Fall eine Cyber-Versicherung greifen, um Verantwortungsträger wirksam abzusichern. Der Abschluss einer solchen erscheint vor allem deshalb ratsam, da die entstandenen Schäden in der Regel nicht von der D&O Versicherung berücksichtigt werden.

Insgesamt sollte das Leistungsspektrum sämtlicher Versicherungen im Hinblick auf Schäden durch IT-Sicherheitsvorfälle unbedingt an die jeweilige Unternehmenssituation sowie das individuelle Haftungsrisiko angepasst werden. **Hier hilft die juristische Expertise unserer Berater dabei zu erkennen, welche Leistungen wirklich abrufbar sein sollten.**



Kontakt

Berlin
Kurfürstendamm 32
10719 Berlin
T +49 30 88 00 97-0
F +49 30 88 00 97-99

Chemnitz
Weststraße 16
09112 Chemnitz
T +49 371 38 203-0
F +49 371 38 203-100

Düsseldorf
Georg-Glock-Straße 4
40474 Düsseldorf
T +49 211 600 55-00
F +49 211 600 55-050

Frankfurt
Goetheplatz 5-7
60313 Frankfurt am Main
T +49 69 975 61-0
F +49 69 975 61-200

Hamburg
Neuer Wall 63
20354 Hamburg
T +49 40 35 52 80-0
F +49 40 35 52 80-80

Köln
Magnusstraße 13
50672 Köln
T +49 221 20 52-0
F +49 221 20 52-1

München
Prinzregentenstraße 48
80538 München
T +49 89 540 31-0
F +49 89 540 31-540

Stuttgart
Königstraße 45
70173 Stuttgart
T +49 711 22 04 579-0
F +49 711 22 04 579-44

Zürich
Bahnhofstrasse 69
8001 Zürich/Schweiz
T +41 44 200 71-00
F +41 44 200 7101