TaylorWessing

Versteckte Gefahr: Cybersicherheits-Angriffe

Schützen Sie Ihr Unternehmen vor Bedrohungen, Haftung und künftigen Risiken – all das aus einer Hand, mit einem Partner für rechtliche Cybersicherheit.

Unser ganzheitlicher Ansatz: Schützen, bewältigen und zurück zur Normalität!

Von der Einhaltung gesetzlicher Vorschriften über die proaktive Reaktion auf Vorfälle bis hin zur Zukunftssicherung Ihres Unternehmens - Taylor Wessing unterstützt Sie umfassend, damit Sie den auch neuen Bedrohungen stets einen Schritt voraus sind.

Mit einer bewährten Kombination aus Cyber-, Daten-, IT- und Dispute Resolution-Expertise unterstützen wir Unternehmen dabei,

- Risiken proaktiv zu mindern,
- effektiv auf Vorfälle zu reagieren und
- ihre Widerstandskraft für die Zukunft zu stärken.

Darüber hinaus verfügen wir über ein Netzwerk aus erfahrenen IT-Spezialist:innen, PR-Teams und Verhandlungs-Expert:innen, um eine umfassende Reaktion auf Vorfälle zu ermöglichen und sicherzustellen, dass Ihr Unternehmen bestmöglich unterstützt wird.

TaylorWessing

Unsere Leistungen im Überblick

1. Schützen – Risiken minimieren, bevor sie entstehen

- **Überprüfung von Richtlinien und Dokumentation:** Wir stellen sicher, dass Ihre internen Richtlinien, Verträge und Dokumentationsstandards regulatorischen Anforderungen, wie z.B. NIS2, entsprechen.
- **Optimierung des Cyber Security Frameworks:** Wir evaluieren und optimieren vorhandene Prozesse zum Risikomanagement in Ihrer gesamten Organisation.
- **Beratung der Unternehmensleitung:** Wir beraten zu Haftungsrisiken im Zusammenhang mit unzureichenden Cyber-sicherheitsmaßnahmen.
- **Verträge mit Lieferant:innen und Partner:innen:** Wir überprüfen, entwerfen und verhandeln Vereinbarungen zur Cybersicherheit (etwa Vertragsklauseln, die Haftungsrisiken reduzieren sollen).
- **Überprüfung des Versicherungsschutzes:** Wir bewerten die Angemessenheit Ihres Cyber-Haftpflichtversicherungsschutzes in Bezug auf die Deckung kritischer Bereiche wie drohende Strafen, „incident response costs" und drohende Betriebsunterbrechungen.

TaylorWessing

2. Bewältigen – Schnelles Handeln, wenn jeder Moment zählt

- **Sofortige rechtliche Unterstützung:** Rechtliche Vertretung Ihres Unternehmens während eines laufenden Vorfalls und Übernahme der erforderlichen Verhandlungen.
- **Unterstützung beim Krisenmanagement:** Wir unterstützen Sie, die Folgen von Betrug, Erpressung, Ransomware und Betriebsunterbrechung so weit als möglich zu reduzieren.
- **Regulatorische Meldungen:** Wir kümmern uns um Meldepflichten und die Kommunikation mit Behörden, einschließlich der Meldung von Datenschutz- und Sicherheitsverletzungen
- **Forderungsmanagement:** Wir unterstützen Sie bei der Abwehr von Ansprüchen gegen Ihr Unternehmen und bei der Verfolgung von Ansprüchen, die Ihnen durch Fehler Dritter entstehen.

3. Zurück zur Normalität – Aus Cyber-Vorfällen lernen, sich anpassen und gestärkt daraus hervorgehen

- **Lessons learned:** Gemeinsam mit Ihnen überprüfen wir den Vorfall im Nachgang, um Schwachstellen in Ihren Systemen, Verträgen und Verfahren zu identifizieren.
- **Für die Zukunft vorsorgen:** Wir setzen zusammen mit Ihnen unsere Empfehlungen zur Verbesserung Ihres Sicherheitsrahmens und zur Vermeidung von neuerlichen Vorfällen um.
- **Schulungen:** Wir helfen Ihrem Team, Bedrohungen zu erkennen und wirksam auf diese zu reagieren.

Unsere “lessons learned” nach Cyber-Sicherheitsvorfällen

1. Ransomware-Angriff:

„Wir haben einen Klienten bei der Abwehr eines groß angelegten Ransomware-Angriffs, der seinen Geschäftsbetrieb beeinträchtigte, beraten. Dank unserer schnellen Unterstützung bei der Einhaltung der gesetzlichen Vorgaben sowie unserer Hilfe bei der Wiederherstellung wichtiger Daten, konnte der Mandant erhebliche Geldstrafen vermeiden.“

Lessons learned: Je früher ein Angriff erkannt und darauf reagiert wird, desto weniger Schaden kann er anrichten. Eine Task Force mit Spezialist:innen aus den Bereichen Versicherungen, Recht, Forensik und Öffentlichkeitsarbeit ist der Schlüssel, um bei einem Cyberangriff Zeit und Geld zu sparen. Das richtige Team, das bereit ist, sofort zu handeln, macht den Unterschied.

2. Verantwortlichkeit des Managements für Versäumnisse im Bereich der Cybersicherheit:

„Nach einem gravierenden Cyberangriff stellten wir fest, dass die Geschäftsleitung es versäumt hatte, angemessene Cybersicherheitsmaßnahmen zu implementieren, sodass das Unternehmen nicht ausreichend vorbereitet war. Wir leiteten rechtliche Schritte gegen die Führungskräfte ein, da sie ihrer Verantwortung, das Unternehmen vor Cyberrisiken zu schützen, nicht nachgekommen waren.“

Lessons learned: Die Sicherstellung von Cybersicherheit ist eine wesentliche Aufgabe der obersten Führungsebene. Führungskräfte müssen dafür sorgen, dass ihre Unternehmen entsprechend vorbereitet sind.

3. Ermittlung von Versicherungslücken:

„Durch unsere Prüfungsprozesse konnten wir Lücken in der Cyber-Haftpflichtversicherung eines Klienten identifizieren und so einen umfassenden Versicherungsschutz gegen drohende Bußgelder und Betriebsunterbrechungen sicherstellen.“

Lessons learned: Cyber-Bedrohungen entwickeln sich rasant weiter. Es ist von entscheidender Bedeutung, dass Unternehmen ihre Cyber-Versicherungspolizzen regelmäßig überprüfen lassen, um sicherzustellen, dass sie angemessen versichert sind.

TaylorWessing

Schon gewusst?

1. 2024 erreichten die **Verluste durch Cyberkriminalität** in Europa **10 Milliarden Euro**. Das ist doppelt so viel wie im Jahr davor.

2. Allein im zweiten Halbjahr 2024 **stieg die Zahl der Phishing-Nachrichten um 202%** und die Zahl der Phishing-Angriffe auf Zugangsdaten um 703% - Experten führen diese Trends auf KI-gestützte Taktiken zurück.

3. Die **NIS2-Richtlinie** führt EU-weit **strengere Pflichten** für Unternehmen ein, auch für die Unternehmensleitung. Die **Nichteinhaltung** dieser Anforderungen kann zu einer **persönlichen Haftung** des Managements, **hohen Bußgeldern** und **Reputationsschäden** führen.

4. Trotz zunehmender Bedrohungen gaben **74%** der Unternehmen in der EU im Rahmen einer Befragung im Jahr 2024 an, ihren Mitarbeitern **keine Schulungen** oder **Sensibilisierungsprogramme** zu Cybersecurity anzubieten.

Ein Wort von unseren Experten

Angesichts der zunehmenden KI-gestützten Bedrohungen ist Cybersecurity nicht mehr nur eine Option, sondern eine geschäftliche Notwendigkeit. Unternehmen, die jetzt in die Vorbereitung investieren, werden morgen die Gewinner sein.

Partner Mag. Andreas Schütz, LL.M., CEE Head of IT & Datenschutz

Das Management ist für Cybersecurity verantwortlich. In Anbetracht der ständigen Verschärfung der gesetzlichen Vorgaben müssen Führungskräfte sicherstellen, dass Cyber-Sicherheit nicht nur ein IT-Thema bleibt, sondern unternehmensweit Priorität genießt.

Partner Dr. Philipp Zumbo, CEE Head of Dispute Resolution

TaylorWessing

Lassen Sie uns gemeinsam Ihre unternehmerische Zukunft sichern

Wir bieten Ihnen maßgeschneiderte Workshops und Beratung:

SCHÜTZEN - Risikobewertung, Compliance und interne Dokumentation

BEWÄLTIGEN - Step-by-step-Aktionspläne zur Abfederung der unmittelbaren Auswirkungen von Zwischenfällen

ZURÜCK ZUR NORMALITÄT - Analyse nach einem Vorfall und Verbesserung der Widerstandskraft

Kontaktieren Sie uns noch heute, um mehr über unsere maßgeschneiderten Lösungen zu erfahren oder einen Workshop zum Thema Cybersecurity zu planen.

Mag. Andreas Schütz, LL.M.
Partner, IT / Datenschutz
Wien
+43 1 716 55
a.schuetz@taylorwessing.com

Dr. Philipp Zumbo
Partner, Dispute Resolution
Wien
+43 1 716 55
p.zumbo@taylorwessing.com

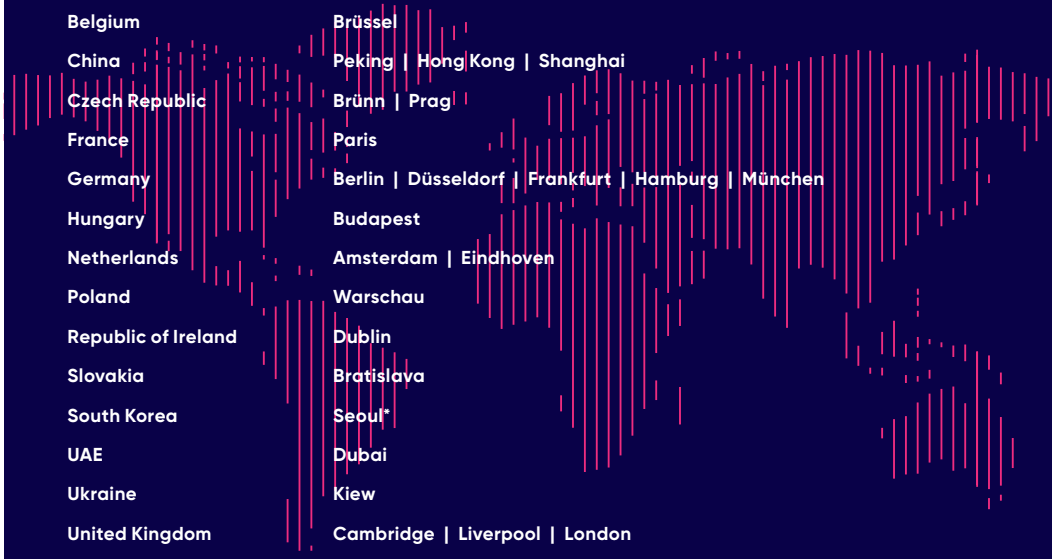
Mag. Ivo Deskovic
Partner, Dispute Resolution
Wien
+43 1 716 55
i.deskovic@taylorwessing.com

Mag. Christopher Bakier
Senior Assoicate, IT
Wien
+43 1 716 55
c.bakier@taylorwessing.com

Mag. Erik Steiner
Senior Assoicate, IT
Wien
+43 1 716 55
e.steiner@taylorwessing.com

TaylorWessing

1200+ Jurist:innen
300+ Partner:innen
28 Offices
17 Jurisdiktionen



Austria	Wien
Belgium	Brüssel
China	Peking | Hong Kong | Shanghai
Czech Republic	Brünn | Prag
France	Paris
Germany	Berlin | Düsseldorf | Frankfurt | Hamburg | München
Hungary	Budapest
Netherlands	Amsterdam | Eindhoven
Poland	Warschau
Republic of Ireland	Dublin
Slovakia	Bratislava
South Korea	Seoul*
UAE	Dubai
Ukraine	Kiew
United Kingdom	Cambridge | Liverpool | London
USA	New York | Silicon Valley

* In association with DR & AJU LLC

© Taylor Wessing 2025

Diese Publikation stellt keine Rechtsberatung dar. Die unter der Bezeichnung Taylor Wessing tätigen Einheiten handeln unter einem gemeinsamen Markennamen, sind jedoch rechtlich unabhängig voneinander; sie sind Mitglieder des Taylor Wessing Vereins bzw. mit einem solchen Mitglied verbunden. Der Taylor Wessing Verein selbst erbringt keine rechtlichen Dienstleistungen. Weiterführende Informationen sind in unserem Impressum unter taylorwessing.com/de/legal/regulatory-information zu finden

TaylorWessing