TaylorWessing

Haftung bei IT-Sicherheitsvorfällen

Wie Security-Budgets den richtigen Stellenwert bekommen

10. April 2024 | Mag. Andreas Schütz, LL.M.

Überblick

Gefahrenquellen:

- ! Phishing über E-Mails
- ! Unsicherer Umgang mit Daten (z.B. unbeaufsichtigt liegende Dokumente, unzureichende Entsorgung, Verwendung unbekannter USB-Sticks)
- ! Unsicherer Umgang mit Daten auf Reisen oder im Home-Office
- ! Unverschlüsselte Passwörter und fehlende Passwort-Policy
- ! Verwendung von Software aus unbekannten Quellen
- ! Verwendung von Open Source Software mit Sicherheitslücken
- ! Browsen im Internet ohne https-Verschlüsselung

Akteure:

- Staatliche Akteure
- Finanzkriminalität
- Industriespionage
- Insider-Bedrohungen
- Computerspieler (für Spielgewinn)
- „Hacktivists“ (politisch, moralisch etc. motiviert)
- Einzelkämpfer

IT-Sicherheit in Zahlen

Cyber Security Studie 2023:

- Anstieg von Cyberangriffen zwischenjährlich um 201 %
- Mehr als die Hälfte der befragten Unternehmen durch die Angriffe in ihrem Fortbestehen bedroht
- Betriebsunterbrechung von mehreren Wochen bei 14 % der Unternehmen
- Schaden bis zu 100.000 EUR bei knapp der Hälfte der Unternehmen
- Häufigste Angriffe (in % der befragten Unternehmen):
  - 100 % erlebten **Phishing**
  - 57 % erlebten eine **Social-Engineering-Attacke**
  - 33 % erlebten einen **Ransomware-Angriff**
  - 22 % musste sich mit einem **Deep-Fake** auseinandersetzen

KPMG und Kompetenzzentrum Sicheres Österreich: Cyber Security Studie 2023 (https://kompetenzzentrum-sicheres-oesterreich.at/studienpaesentation-cybersecurity-in-oesterreich-2023/)

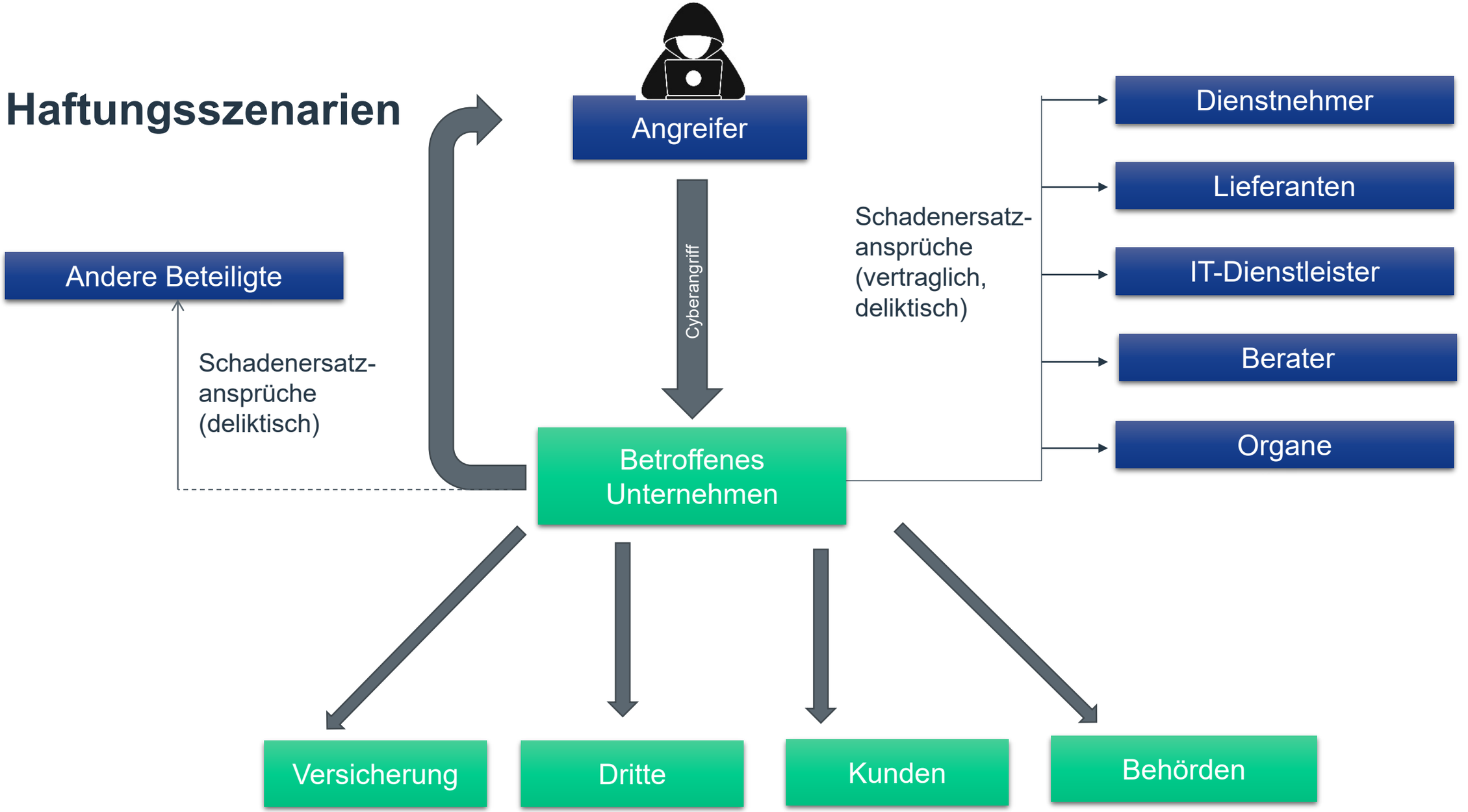
Datenschutzbericht 2022 der DSB:

- **818 nationale Meldungen** von Datenschutzverletzungen nach Art 33 DSGVO
- Zudem 15 Meldungen von grenzüberschreitenden Sicherheitsverletzungen
- Häufigste Vorfälle:
  - Ungewollte **Verschlüsselung von Daten** und Verlangen von Lösegeld für die Entschlüsselung
  - Übertragung von **Schadsoftware** auf Systeme des Verantwortlichen (über E-Mail oder Internet)

https://www.dsb.gv.at/download-links/dokumente.html

Was passiert, wenn‘s passiert ist?

Haftungsszenarien



Ansprüche und potenzielle Schäden

- **Vertragliche Ansprüche:**
  - Gewährleistung / Schadenersatz
  - Unmöglichkeit der Leistung, Verzug
  - Vertragliche (Neben-)Pflichtverletzungen
- **Deliktische Ansprüche:**
  - Verletzungen des Persönlichkeitsrechts
  - Allgemeine deliktische Ansprüche
  - Schutzgesetzverletzung
- **Ansprüche nach DSGVO**
- **Eigenschäden:**
  - Kosten aufgrund von verhängten Verwaltungsstrafen
  - Wiederherstellung von Daten, Programmen, Systemen
  - Stillstandskosten, Umsatzeinbußen
  - Ursachenbehebung
  - Kosten für technische und juristische Beratung (Forensiker, Sachverständige, Berater)
  - Lösegeld
  - Reputationsschäden
- **Fremdschäden:**
  - Verletzung der Vertraulichkeit und des Rechts auf Datenschutz
  - Verletzung von Immaterialgüterrechten
  - Verletzung von Betriebs- und Geschäftsgeheimnissen
  - Entgangener Gewinn

Haftung des Unternehmens

Gegenüber den Kunden:

- **Lieferausfall**
  - Verzug und Verzugsschaden
- **Datenleaks**
  - Nach allgemeinen Bestimmungen
  - Nach Art 82 DSGVO
- **Vertragliche Haftung**
  - Beweislastumkehr
  - Sorgfaltsverstoß
  - Stand der Technik
  - Haftung für Erfüllungsgehilfen nach § 1313a ABGB (Fehler von Mitarbeitern)
  - Pönalen

Gegenüber den Lieferanten:

- **Gläubigerverzug und Gefahrenübergang**
- **Datenleaks**
  - Nach allgemeinen Bestimmungen
  - Nach Art 82 DSGVO

Gegenüber jedermann:

- N**ach Art 82 DSGVO**
  - Beweislastumkehr
  - Immaterieller Schaden
  - EuGH 04.05.2023, C-300/21 (*Sinus-Geo-Milieus II*): der bloße Verstoß gegen die Bestimmungen der DSGVO reicht nicht aus

Haftung der Geschäftsführung / des Vorstands

Gegenüber dem Unternehmen

- **§ 25 GmbHG**
  - Sorgfalt eines ordentlichen Geschäftsmannes
  - keine Erfolgshaftung (nur eigenes Verschulden, nicht für Mitarbeiter)
  - Organisations- und Überwachungspflicht
  - branchen-, größen- und situationsadäquate Bemühungen
  - „Business Judgement Rule“
  - Beiziehung von Experten
- **§ 84 AktG**
  - Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters
  - „Business Judgement Rule“
- **§ 22 GmbHG / § 82 AktG**
  - den Anforderungen des Unternehmens entsprechendes IKS

Gegenüber Dritten:

- Deliktische Haftung → keine Beweislastumkehr
  - Vorsätzlich sittenwidrige Schädigen
  - Eingriff in absolut geschützte Rechtsgüter
  - Schutzgesetzverletzung
  - keine Beweislastumkehr
- Haftung und Schadenersatz nach Art 82 DSGVO

Strafen

- **§ 188 TKG 2021:**
  - Verwaltungsstrafen bis zu 75.000 EUR
    - bei mangelnden Maßnahmen zur Sicherung der Netzintegrität und Netzsicherheit
    - bei Verletzung der Informationspflichten

- **§ 26 NISG:**
  - Verwaltungsstrafen bis zu 50.000 EUR (im Wiederholungsfall 100.000 EUR)
    - bei mangelnden technischen und organisatorischen Sicherheitsvorkehrungen
  - Außerdem sind **Meldepflichten** nach NISG bei Risiken und Sicherheitsvorfällen zu beachten

- **Nach DSG:**
  - Verwaltungsstrafe bis zu 50.000 EUR gemäß § 62 DSG:
    - bei Verschaffung eines widerrechtlichen Zugangs zu einer Datenverarbeitung
    - bei Übermittlung von Daten in Verletzung eines Datengeheimnisses
    - bei einer widerrechtlichen Bildverarbeitung
  - Geldbußen gegen juristische Personen nach § 30 DSG

Neue EU-Vorgaben

Cybersicherheits-Richtlinie (NIS2)

- Ziel: europaweite Anhebung des Cybersicherheitsniveaus durch Einführung von geeigneten **Risikomanagementmaßnahmen** für die IT-Systemlandschaft betroffener Unternehmen
- Ausgenommen sind kleine Unternehmen mit < 50 Mitarbeiter und < 10 Mio. Umsatz (Achtung: bestimmte Unternehmen sind unabhängig von der Größe erfasst)
- Umsetzung der Richtlinie in Österreich bis **17. Oktober 2024**
  - Netz- und Informationssystemsicherheitsgesetz 2024 (aktueller Stand: Begutachtungsverfahren bis 01.05.2024 offen)

- Aktuelle Verwaltungsstrafen für Verletzungen von Meldepflichten und Pflichtverletzungen bei Sicherheitsvorkehrungen bis zu 100k EUR (nach NISG) → Höchstbeträge nach NIS2 bis zu **10 Mio. EUR** oder **2 % des weltweiten Umsatzes**
- Leitungsorgane haben Umsetzung der Maßnahmen zu überwachen → Haftung für Verstöße wird einzelstaatlich ausgestaltet

Cyber Resilience Act (CRA)

- Ziel: Anhebung des Sicherheitsniveaus bei **Produkten mit digitalen Elementen**
- Wichtigste Neuerungen:
  - Meldepflichten
  - Updatepflichten
  - Dokumentationspflichten
  - Durchführung von Konformitätsverfahren
- Außerdem sieht die NIS2 konkrete Verpflichtungen für die **Leitungsorgane** betroffener Unternehmen in Zusammenhang mit **Risikomanagementmaßnahmen** und **Berichtspflichten** vor
- Betroffen sind **Wirtschaftsteilnehmer entlang der Lieferkette** – Hersteller, Importeure und Distributoren
- Drohende Geldbußen bis zu **15 Mio. EUR** oder bis zu **2,5 % des Jahresumsatzes**

Digital Operational Resilience Act (DORA)

- Ziel: Gewährleistung der **Betriebsstabilität** und **Widerstandsfähigkeit digitaler Systeme des Finanzsektors**
- Lex specialis zu der NIS2-RL
- Wichtigste Neuerungen:
  - **IKT-Risikomanagement** und **Business-Continuity-Management**
  - **Berichterstattung** und Meldungen zu IKT-Vorfällen an nationale Behörden
  - **Prüfung** der digitalen Betriebsstabilität
  - **Steuerung und Überwachung** (bei 3rd Party IKT-Dienstleistern)
- Verwaltungsstrafen werden durch die nationalen Behörden verhängt
- Sanktionen müssen **wirksam, verhältnismäßig** und **abschreckend** sein

„Crime-as-a-Service“

Praxisbeispiele: von gefälschten Rechnungen bis zum durchdachten CEO Fraud

Gefälschte Rechnungen

- **Sachverhalt:** gefälschte Rechnungen vom E-Mail-Konto einer Mitarbeiterin durch unbekannte Dritte an einen Kunden geschickt → Kunde zahlt an die „gefälschte“ Kontonummer

  - Strafrechtlich: Betrug an dem Rechnungsempfänger durch den Dritten
  - Zivilrechtlich: Frage der schuldbefreienden Wirkung der Zahlung an einen Dritten (Nichtgläubiger)
    - ? Handeln mit der gebotenen Sorgfaltspflicht
    - ? Auffallenmüssen einer plötzlichen Kontoänderung bei einer ständigen Geschäftsbeziehung
    - ? Technisch-organisatorische Maßnahmen
    - ? Ausreichendes und wirksames internes Kontrollsystem

CEO Fraud

- **Imitation der Führungskräfte** durch Einsatz von verschiedenen technischen Mitteln (z.B. gefälschte E-Mails, Deep-Fake Anrufe oder Videokonferenzen) um Zahlungen zu veranlassen – oft unter Druckausübung
- Durch die Verbreitung von AI werden die Methoden immer raffinierter
- **Prävention:**
  - Sensibilisierung der Mitarbeiter
  - Freigabeverfahren und Mehrfach-Authentifizierung
  - Überwachung der Prozesse
  - Meldeverfahren
- Beim Vorfall ist Schnelligkeit das A und O → **Notfallpläne**

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN
2 minute read · Published 2:31 AM EST, Sun February 4, 2024

Authorities are increasingly concerned at the damaging potential posed by artificial intelligence technology. boonchai wedmakawand/Moment RF/Getty Images

https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

Fazit: Was haben die Unternehmen zu beachten?

Allgemeine Empfehlungen für Unternehmen

- Regelmäßige und methodische Identifizierung und Minimierung von Risiken
- Umsetzung von geeigneten Sicherheitsmaßnahmen inkl. Kontrollmechanismen:
  - **Technische Maßnahmen**: Antivirusprogramme, Firewalls, Datenverschlüsselung, geschützte Passwortmanager, 2-Faktor-Authentifizierung, richtige Konfiguration und Wartung von IT-Systemen
  - **Organisatorische Maßnahmen**: regelmäßige Durchführung von Backups und Updates, Passwort-Policy, Weiterbildung, Notfallpläne für Sicherheitsvorfälle, Clean Desk Policy
  - **Personelle Maßnahmen**: Bewusstseinsbildung und Etablierung von Verantwortlichkeiten
- Erforderlichenfalls Hinzuziehung von Experten mit Fokus auf IT- und Cybersicherheit
- Frühzeitige Umsetzung der Verpflichtungen nach NIS2 und CRA

Empfehlungen für Geschäftsleitung und Führungskräfte

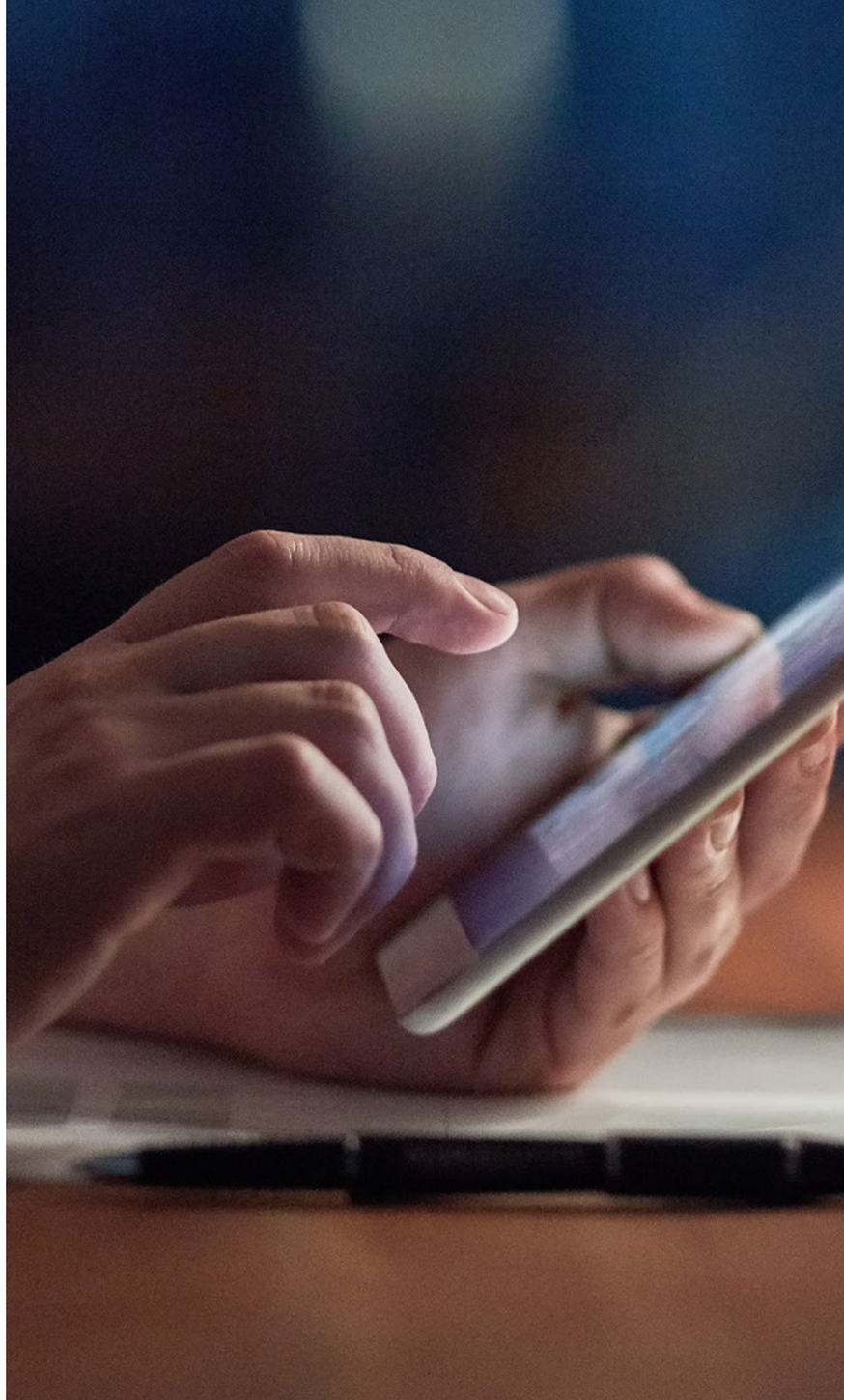
- Verantwortung des Managements bei IT-Sicherheitslücken und Cybervorfällen, wenn:
  - **Verletzung von Sorgfaltspflichten** bei der Geschäftsführung
  - Unzureichende Umsetzung von **technischen** und **organisatorischen Sicherheitsmaßnahmen**
  - Unzureichende Umsetzung von **Notfallplänen** und **Überwachungsverfahren**

→ Etablierung und Umsetzung einer **Corporate Governance:**

- Internes Kontrollsystem
- Risiko Management
- Compliance Management
- Stand der Technik
- Häufiger Austausch mit den zuständigen Fachabteilungen

Danke für Ihre Aufmerksamkeit!

Mag. Andreas Schütz, LL.M.
Partner
Taylor Wessing Wien
a.schuetz@taylorwessing.com



Europe > Middle East > Asia

taylorwessing.com