ATB. LAW

# Geschäftsführerhaftung bei Cyber-Angriffen

Mag. Anela Blöch, LL.M.

Patrick Brunsteiner, LL.M. (WU)

ATB. LAW

# Heutige Agenda

- Grundlagen der Geschäftsführerhaftung
- Sorgfaltspflichten der Geschäftsführung iZm Cyber-Angriffen
- Mögliche sonstige Sanktionen

ATB. LAW

# Grundlagen der Geschäftsführerhaftung

ATB. LAW

# Cyber-Angriffe sind alltäglich

ÜBERWACHUNGSSYSTEM INFILTRIERT

## Cyberangriff trifft Flughafen Hamburg

Hinter dem Angriff steckt eine Hackergruppe namens Just Evil. Diese hat auf Telegram unter anderem Bilder von Überwachungskameras des Hamburger Flughafens geteilt.

22. Mai 2024, 10:59 Uhr, Marc Stöckel

in Pocket speichern | merken


## Cyberangriff bei Varta: Produkt immer gelähmt

23.02.2024 | Lesezeit: ca. 4 Minuten

Der Batteriehersteller Varta des österreichischen Investors Michael Tojner wurde Angriff einer Cyberattacke und musste die Produktion in Deutschland herunterfahren. Die Attacke trifft das Unternehmen gerade in der dringend notwendigen Sanierung. Noch die Produktion. Über die Täter gibt es aber nun erste Informationen.


Landtechnik-Branche

## Hackerangriff auf Landtechnikhersteller Lemken – nichts geht mehr

© Julia Eder An den Lemken-Standorten bleiben viele Bildschirme noch schwarz und auch die Produktion steht still. Doch die Mitarbeiter seien für Kunden per Mail oder Mobiltelefon erreic Lemken.

Teilen | Twittern | Pinnen | Teilen | Mail | Druck

Redaktion agrarheute, agrarheute
am Donnerstag, 16.05.2024 - 11:16

## Cyber-Attacke auf KLV ohne grobe Sch

Die Kärntner Landesversicherung ist am Wochenende Opfer eines Cyber-Angriffs geworden. Dank eines Alarmsystems konnte die Attacke aus heutiger Sicht weitestgehend abgewehrt und schlimmerer Schaden verhindert werden. Kundendaten sind vermutlich nicht betroffen, bei Online-Diensten muss jedoch mit Einschränkungen gerechnet werden.

11. März 2024, 12.44 Uhr

## Cyberangriffe in NÖ: Auch Therme Laa und WIFI betroffen

1 KOMMENTAR 9.02.2024 09:27 (Akt. 9.02.2024 12:51)

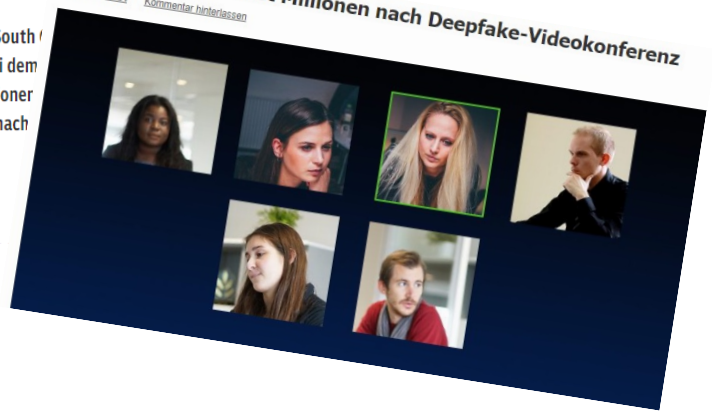
## Millionenbetrug mit gefälschter Videokonferenz

Betitelt mit „Alle sahen echt aus" berichtet die Zeitung „South ( von einem derzeit für Aufsehen sorgenden Betrugsfall, bei dem Unternehmen in Hongkong um umgerechnet rund 23 Millioner Geld sei trotz anfänglicher Zweifel überwiesen worden – nach Intelligenz (KI) gefälschten Videokonferenz.

5. Februar 2024, 22.38 Uhr

## Mitarbeiter überweist Millionen nach Deepfake-Videokonferenz

6. Februar 2024 Kommentar hinterlassen



ATB. LAW

# Wer ersetzt bei Cyber-Angriffen den Schaden?

- Primär – soweit bekannt – der/die Täter selbst

- Sonstige mögliche Anspruchsgegner: IT-Dienstleister, Versicherung oder sonstige Dienstleister

- Wenn kein Anspruchsgegner vorhanden ist → Geltendmachung von Schadenersatzansprüchen innerhalb des Unternehmens

ATB. LAW

# Wer haftet bei Cyber-Angriffen im Unternehmen?

- Bei Fahrlässigkeit kein (voller) Ersatzanspruch gegenüber den handelnden Mitarbeitern (DHG)

- DHG bei Geschäftsführern nicht anwendbar

→ mögliche Schadensersatzansprüche gegen den/die Geschäftsführer direkt

ATB. LAW

# Gesetzliche Bestimmungen

- **§ 25 GmbHG**

  *(1) „Die Geschäftsführer sind der Gesellschaft gegenüber **verpflichtet**, bei ihrer Geschäftsführung die **Sorgfalt eines ordentlichen Geschäftsmannes** anzuwenden.“*

  *(2) „Geschäftsführer, die ihre Obliegenheiten verletzen, haften der Gesellschaft **zur ungeteilten Hand** für den daraus entstandenen Schaden.“*

- **§ 84 AktG**

  *(1) „Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die **Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters** anzuwenden. Über **vertrauliche Angaben** haben sie **Stillschweigen** zu bewahren.“*

  *(2) „Vorstandsmitglieder, die ihre Obliegenheiten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens **als Gesamtschuldner** verpflichtet. Sie können sich von der Schadenersatzpflicht durch den **Gegenbeweis** befreien, daß sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewendet haben.“*

ATB. LAW

# Keine Haftung bei…

- Handeln im Rahmen der **Business Judgement Rule**

  **25 Abs 1a GmbHG:** *„Ein Geschäftsführer handelt jedenfalls **im Einklang mit der Sorgfalt eines ordentlichen Geschäftsmannes**, wenn er sich bei einer*

  - ✓ ***unternehmerischen Entscheidung***
  - ✓ ***nicht** von **sachfremden Interessen** leiten lässt und*
  - ✓ *auf der **Grundlage angemessener Information** annehmen darf,*
  - ✓ *zum **Wohle der Gesellschaft** zu handeln.“*

- Fehlender **Kausalität** bzw fehlendem **Verschulden**

- Einhaltung der **objektiv erforderlichen Sorgfalt** („Beweislastumkehr“)

ATB. LAW

# Sorgfaltspflichten iZm Cyber-Angriffen

# Umfang der Sorgfaltspflichten

- OGH **8 ObA 109/20t, Rz 54**:

  *„Die **rechtliche Beurteilung, ob gesetzlichen Präventions-, Prüfungs- und Sorgfaltspflichten ausreichend nachgekommen wurde**, ist grundsätzlich eine **Frage des Einzelfalls**.“*

- Die Geschäftsführung schuldet keinen bestimmten Erfolg, sondern „eine **branchen-, größen- und situationsadäquate Bemühung**“

# Maßstab der Sorgfaltspflichten

**Unternehmensgegenstand**

sonstige Branchen — sensible Branchen

zB Banken, Gesundheitswesen, Finanzdienstleister

**niedrig** → **hoch**

Einzelunternehmen | Privatstiftung | KMU | (große) GmbH/AG | börsenotierte Gesellschaft

**Unternehmensgröße / Kapitalausstattung**

# Timeline der Sorgfaltspflichten

**CYBER-ANGRIFF**

←

→

**Präventive Maßnahmen**

**Reaktive Maßnahmen**

# Präventive Maßnahmen I

- Ressortverteilung innerhalb der Geschäftsführung
  - Haftungsminimierung der übrigen, nicht zuständigen Geschäftsführer
- Compliance Management Systems („CMS“)
  - Präventions-, Aufdeckungs- und Reaktionsfunktion

# Präventive Maßnahmen II

- Einrichten eines Internen Kontrollsystems („IKS“, § 22 GmbHG)
  - wirtschaftlich vertretbares Maßnahmenpaket, das die Wahrscheinlichkeit eines Schadens am Vermögen des Unternehmens minimiert → schriftliche Dokumentation!
  - muss nicht nur eingerichtet, sondern auch laufend geprüft und aktualisiert werden
  - Überwachungsmaßnahmen organisatorischer und EDV-technischer Art wie Unterschriftenregelungen („4-Augen-Prinzip“) und EDV-Zugriffsbeschränkungen
  - Arbeitsanweisungen
  - Kontrollmaßnahmen

ATB. LAW

# Präventive Maßnahmen III

- Erstellen eines sog. Cyber Incident Response Plans („CIRP“), welcher zumindest folgende Themen abdecken muss:
  - Wer ist mein Response Team?
  - Identifizierung möglicher Cyber-Angriffe
  - Maßnahmen zur Schadensminimierung
  - Maßnahmen zur Schadensbehebung
  - Beschreibung der Kommunikationskanäle für den Angriffsfall
  - Fristen für die notwendigen Meldungen (DSB, FMA etc)
- Abschluss einer Cyber-Versicherung
  - nicht verpflichtend aber empfehlenswert, weil D&O Versicherung oft nicht greift

# Reaktive Maßnahmen I

- Evaluierung von Umfang und Intensität des Cyber-Angriffs
- Verständigung von Behörden, Mitarbeitern, Vertragspartner oder Kunden
- Schadenfallmeldung an Versicherung
- Data Breach-Meldung und Vorbereitung auf Betroffenenanfragen

# Reaktive Maßnahmen II

- Post Incident Analyse auf Basis des bestehenden CIRP
- Geltendmachung von Schadenersatzansprüchen der Gesellschaft
- Umsetzung der Ergebnisse der Post Incident Analyse in der IKS und Verbesserung der Systeme

ATB. LAW

# Mögliche sonstige Sanktionen

# Mögliche sonstige Sanktionen

- Haftung gemäß NIS-2-RL (Direkthaftung der GF!)
  - „Wesentliche“ Einrichtungen bis zu 10 Mio. oder 2 % des weltweiten Jahresumsatzes
  - „Wichtige“ Einrichtungen bis zu 7 Mio. oder 4 % des weltweiten Jahresumsatzes
- Art 83 DSGVO (im Regressweg)
  - Strafen bis zu EUR 20 Mio. oder 4 % des Umsatzes

ATB. LAW

# Vielen Dank für die Aufmerksamkeit!

Rechtsanwält:innen in Kooperation | Bauernmarkt 24, Top 15 | 1010 Wien | office@atb.law | www.atb.law