

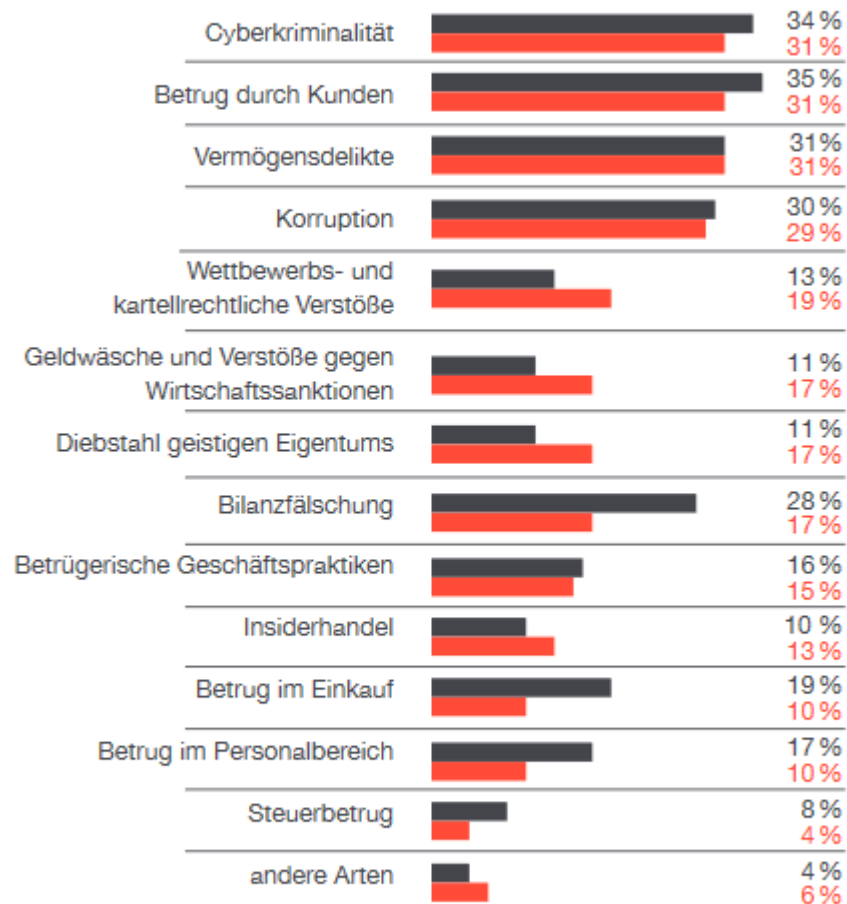
WhistlePro Webinar

Der Angriff auf das Unternehmen – Auswirkungen von Cyber-Attacken und Fake- President auf die Cyber-, VSV- und D&O- Versicherung

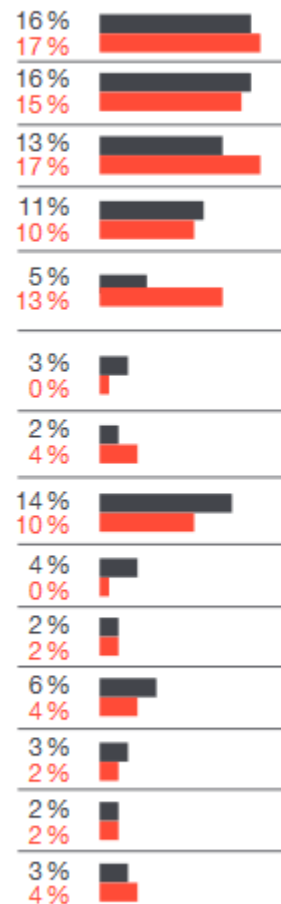
11. Mai 2021

Dr. Stefan Steinkühler, LL.M.

Von welchen Wirtschaftsdelikten waren Unternehmen in den letzten 24 Monaten betroffen?



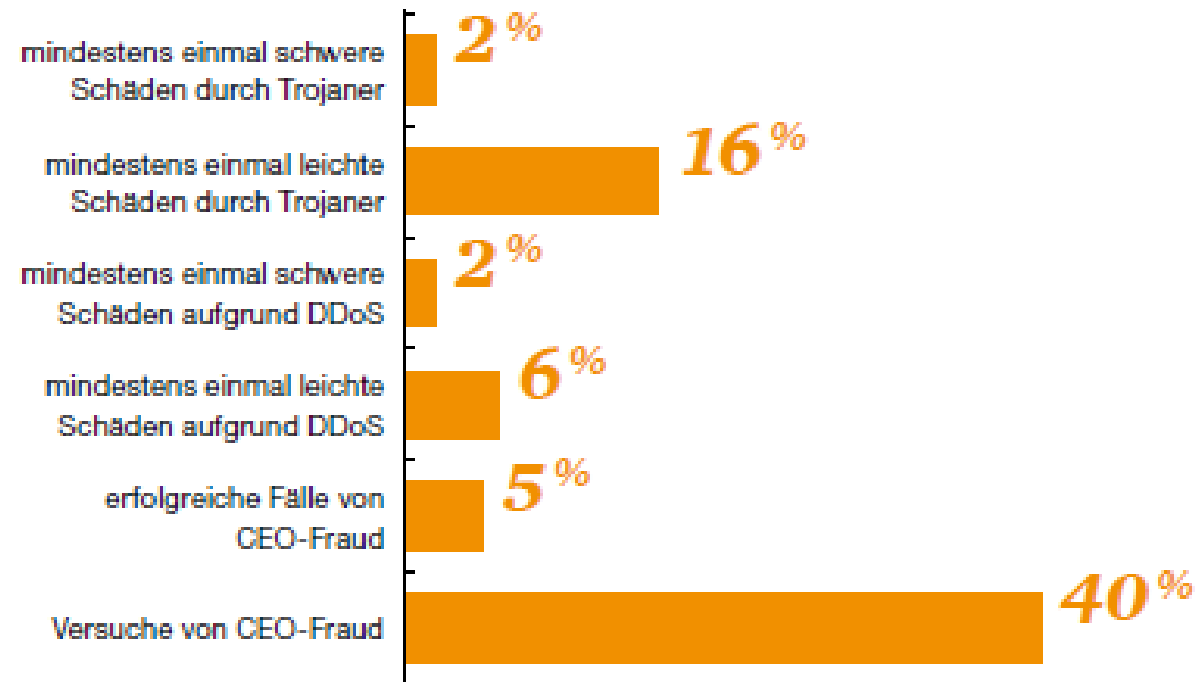
Welche Deliktart hat den schwerwiegendsten Schaden verursacht?



■ weltweit ■ Deutschland

Abb. 7 Von CEO-Fraud und Erpressungsfällen betroffene Unternehmen in den letzten zwei Jahren

Mehrfachnennungen waren möglich.



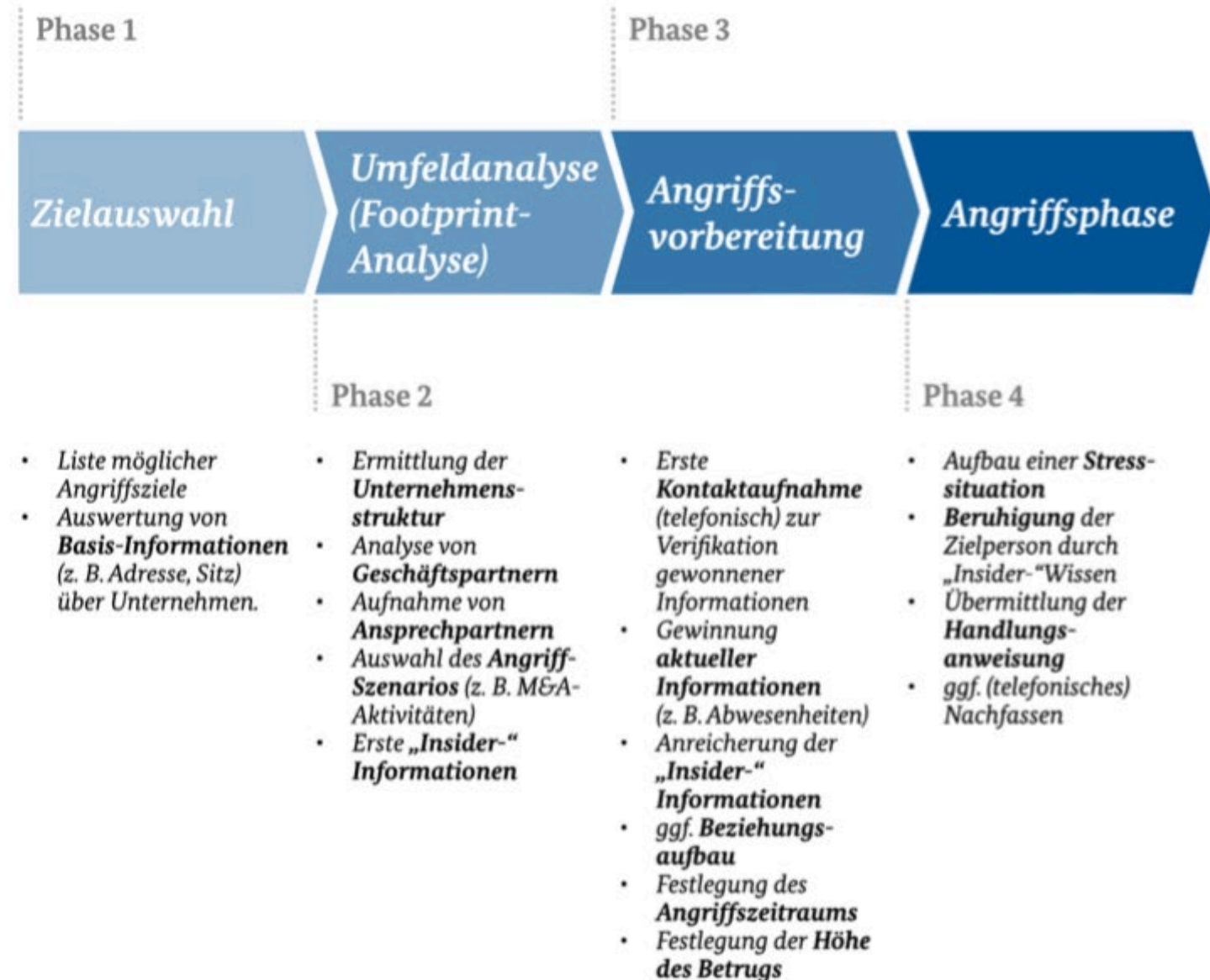
Quelle: pwc, 2018, <https://www.pwc.de/de/risk/pwc-wikri-2018.pdf>

➔ Schaden zwischen 2017 und 2018: über EUR 150 Mio. (GDV)

» Fake President-Angriffe nutzen das Abweichen von Regelprozessen aus. Dies war jüngst in der Corona-Pandemie durch eine Zunahme der Fälle wieder zu sehen. «

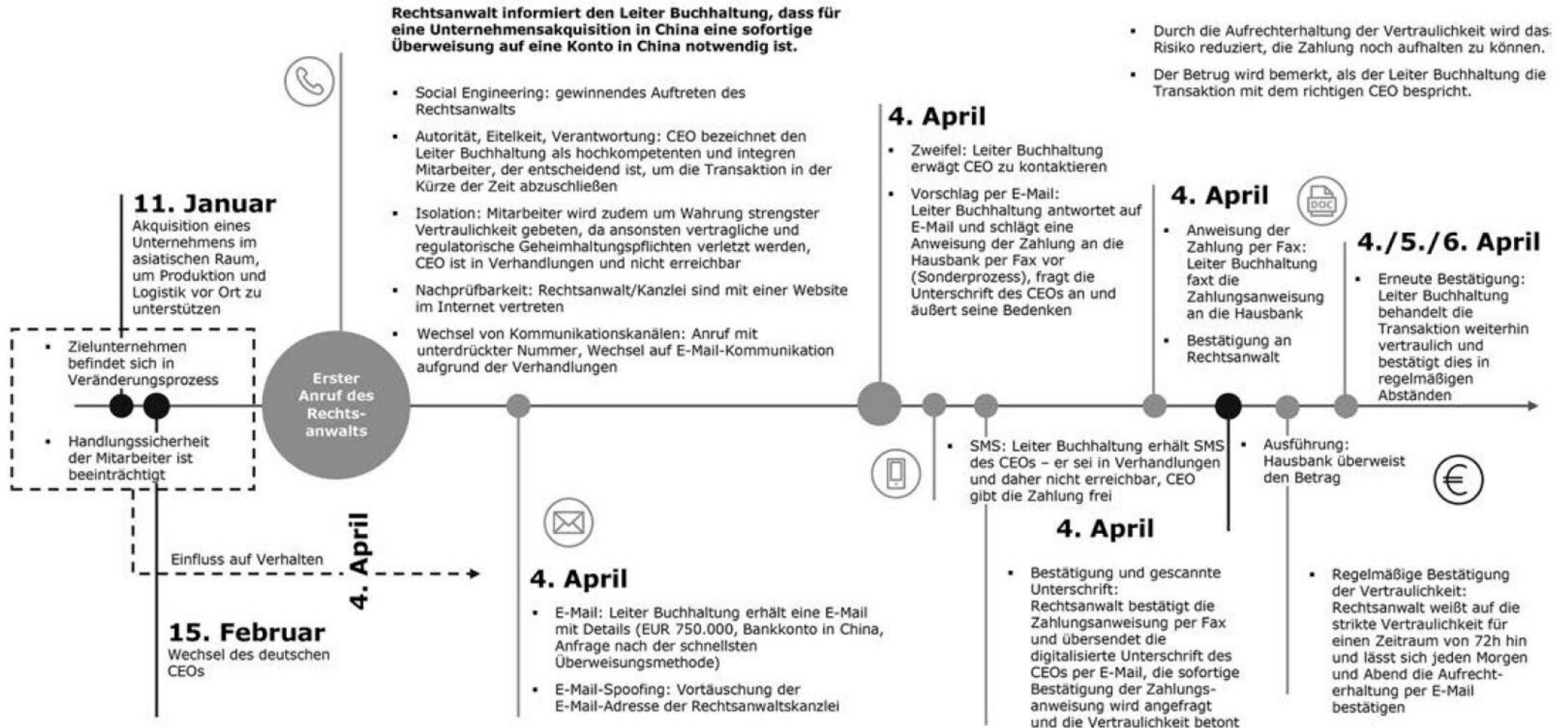
Quelle: KPMG, 2020, Wirtschaftskriminalität in Dt.

Die Kriminellen gehen beim CEO Fraud strukturiert vor und richten Ihre Angriffe nach Effizienzkriterien / Erfolgsaussichten aus.



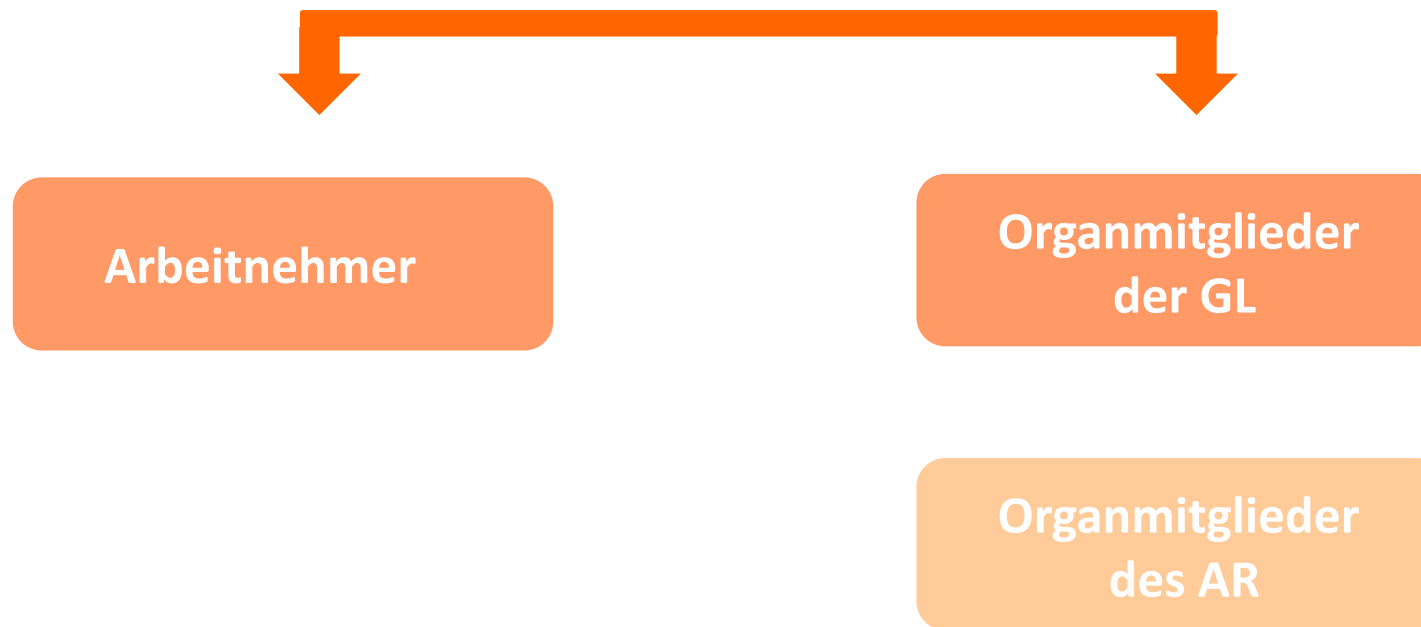
Quelle: BSI, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/partner/161115_expkr_statement02.pdf?__blob=publicationFile&v=5

- # Die Email
- # Der „interne“ Anruf des CFO
- # Die internationale Anwaltskanzlei
- # Die Whatsapp des CFO
- # Der „interne“ Anruf des CEO 2.0
z.B. mittels spezieller Software wie Lyrebird https://web.descript.com/?sign_up=true
(Vorbild ist der Leierschwanz (Englisch: Lyrebird), der alle möglichen Geräusche täuschend echt nachahmen kann, menschliche Stimmen eingeschlossen)
- # Die falsche IT-Abteilung



Quelle: Deloitte, <https://www2.deloitte.com/de/de/pages/finance/articles/fake-president-fraud.html>

/ Wer muss bzw. kann für den Schaden des Unternehmens haftbar gemacht werden?





= Innerbetrieblicher Schadenausgleich

/ Urteile im Zusammenhang mit Fake-President: Arbeitnehmer

- # **ArbG Chemnitz** (Az.: 13 Ca 895/16) hat getäuschte Finanzdirektorin für den entstandenen Schaden in Höhe von EUR 420.000 voll haften lassen; sie habe besonders grob fahrlässig gehandelt („größte Fahrlässigkeit“).

- # **Sächsische LAG** (Az.: 3 Sa 556/16) hat Entscheidung teilweise abgeändert. Arbeitnehmerin haftet in Höhe von EUR 150.000.
 - geringes Mitverschulden bei der Arbeitgeberin: **Minderung um 10%**
 - Mitverschulden der untergeordneten Mitarbeiterin, die die Überweisung letztlich tätigte und ihrerseits ebenfalls die internen Befugnisgrenzen missachtete. Diese sei von der Finanzdirektorin nicht derart eingeschüchtert worden, dass ihr die Einhaltung der internen Vorgaben nicht möglich gewesen sei: **Minderung um 40%**
 - Abschließend **Begrenzung** der Haftung auf einen Betrag von EUR 150.000,00 (statt EUR 210.000) nach Grundsätzen der beschränkten Arbeitnehmerhaftung.

- # **BAG** (Az.: 8 AZR 379/17) – Verfahren wurde (leider) im Vergleich beendet – Ergebnis nicht bekannt

Innenhaftung nach § 93 Abs. 2 AktG / § 43 Abs. 2 GmbHG:

- Pflichtverletzung
- Schaden
- Kausalität zwischen Pflichtverletzung und Schaden (tw. bei Kardinalspflichten vermutet)
- Verschulden wird vermutet

→ leichteste Fahrlässigkeit reicht aus

Business Judgement Rule (§ 93 Abs. 1 S. 2 AktG)

Danach liegt keine Pflichtverletzung vor, wenn das Organmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln.

Legalitätspflicht (keine unternehmerische Entscheidung)

Zu den Sorgfaltspflichten der Geschäftsleitung gehört grundsätzlich die Beachtung sämtlicher Rechtsvorschriften, z.B. Vorschriften des Zivil- und Wirtschaftsrechts, des Bilanz-, Kartell- und Wettbewerbsrechts, des Arbeits-, Sozial- und Steuerrechts, des Verwaltungsrechts und des Straf- und Ordnungswidrigkeitsrechts, und ein Hinwirken darauf, dass die Mitarbeiter des Unternehmens dies auch tun.

/ Urteil im Zusammenhang mit Fake-President: Geschäftsleiter

- # Der österr. Flugzeugkomponentenhersteller FACC wurde von Dezember 2015 bis Januar 2016 Opfer eines „Fake President Fraud“.
- # Betrüger gaben sich in E-Mails als Vorstandsmitglieder aus. Die Finanzabteilung erhielt in mehr als 100 Mails die „streng vertrauliche“ Aufforderung, Geld auf Konten in Asien und der Slowakei zu überweisen. Insgesamt EUR 50 Mio. wurden transferiert. Lediglich EUR 10 Mio. konnten im Zuge der Ermittlungen auf einem ausländischen Konto eingefroren werden.
- # Der ehemalige Vorstandschef steht seit Dezember 2018 als Beklagte in einem von der FACC angestregten Schadenersatzprozess vor Gericht. Er soll kein ausreichendes Kontroll- und Sicherheitssystem installiert haben. EUR 10 Mio. fordert das Unternehmen vor dem LG Ried.
- # Urteil vom 27.11.2019: LG sieht keine stichhaltigen Hinweise für Probleme in der Buchhaltung. Es konnte nicht bewiesen werden, dass kein Vier-Augen-Prinzip herrschte. Der ehemalige Vorstand habe demnach seine Aufsichtspflicht nicht verletzt.
- # Urteil ist nicht rechtskräftig, da Berufung.

Voraussetzung

Angriff in die IT des Unternehmens

(auch Hack eines Smartphones oder der Telefonanlage, Einschleusen eines Trojaners, um Fake-President vorzubereiten)

Problem

- Vermögensabfluss auch versichert?
- Wenn versichert, worauf?
- In der Regel geringes Sublimit
- Eigenschadenbaustein betroffen – Einwand der grobfahrlässigen Herbeiführung der Versicherungsfalls, § 81 VVG

Voraussetzung

Täuschung durch Dritte oder vorsätzlich handelnde Mitarbeiter

Problem

- Eigenschadenversicherung
- Grobfahrlässige Herbeiführung der Versicherungsfalls, § 81 VVG, weil nicht alle internen Sicherheitsvorkehrungen implementiert und überwacht wurden

These

Wer generell keine präventiven Kontrollmechanismen, wie ein 4-Augenprinzip ö.ä. oder auch Mitarbeiterschulungen in seinem Unternehmen einführt, braucht auch keine VSV-Versicherung

Voraussetzung:

- # Haftung eines Leitenden Angestellten und Haftung zu 100%
- # Haftung eines Organmitglieds, wenn Organisationsverschulden (unzureichende Implementierung interner Sicherheitsvorkehrungen und unzureichende Überwachung)

Problem?

- Haftpflichtversicherung für Leitende Angestellte und Organmitglieder; später gestörter Gesamtschuldnerausgleich?
- Bei Leitenden Angestellten unter Umständen (Mit-)Regulierung über Eigenschadenbaustein in Maklerkonzepten, aber Klauseln sind oft unbestimmt (dem Grunde oder der Höhe nach?)

„Der Versicherer bietet der Versicherungsnehmerin und Tochtergesellschaften Versicherungsschutz für Schäden auf Grund von Pflichtverletzungen, die begangen wurden durch versicherte Personen in Arbeitnehmerstatus, soweit sie aufgrund der Grundsätze über den innerbetrieblichen Schadenausgleich sowie entsprechender ausländischer Rechtsvorschriften von einer Haftung gegenüber der Versicherungsnehmerin oder Tochterunternehmen freigestellt sind.“

- Anwendung von § 81 VVG (?/+)
- **Tipp:** VSV und D&O-Versicherung bei demselben Versicherer/Versicherungskonzern

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

RA Dr. Stefan Steinkühler, LL.M.
info@ra-steinkuehler.de
www.ra-steinkuehler.de
www.die-managerhaftung.de