WILHELM
RECHTSANWÄLTE

PETRA RUF & DR. DAVID ULRICH

WENN DER CYBERSCHADEN ZUM D&O-FALL WIRD

D&O-DECKUNG BEI LEISTUNGSFREIHEIT DES CYBERVERSICHERERS

GVNW Cyber und Financial Lines 2025
19. März 2025

WILHELM
RECHTSANWÄLTE

PETRA RUF

- Rechtsanwältin und Fachanwältin für Versicherungsrecht sowie für Bank- und Kapitalmarktrecht
- Spezialisiert auf Prozessführung in Haftungs- und Deckungsprozessen

petra.ruf@wilhelm-rae.de

+49 (0) 30.81 72 732 40

Mehr erfahren:

WILHELM
RECHTSANWÄLTE

DR. DAVID ULRICH, LL.M. (KENT)

- Rechtsanwalt mit Fokus auf Haftpflicht und Cyber
- Promovierte zur D&O-Versicherung
- Macht für Sie eine kurze Pause aus der Elternzeit

david.ulrich@wilhelm-rae.de

+49 (0) 30.81 72 732 40

Mehr erfahren:

WILHELM
RECHTSANWÄLTE

AGENDA

1. DER CYBERSCHADEN
2. PFLICHTEN EINES MANAGERS
3. DECKUNG UNTER DER D&O-VERSICHERUNG?
4. FAZIT & AUSBLICK

WILHELM
RECHTSANWÄLTE

1 DER CYBER-SCHADEN

WILHELM
RECHTSANWÄLTE

DER CYBERANGRIFF

WILHELM
RECHTSANWÄLTE

DECKUNG DES CYBERSCHADENS

WILHELM
RECHTSANWÄLTE

DECKUNG DES CYBERSCHADENS

WILHELM
RECHTSANWÄLTE

2 PFLICHTEN EINES MANAGERS

WILHELM
RECHTSANWÄLTE

WILHELM
RECHTSANWÄLTE

PFLICHTEN EINES MANAGERS

§ 93 AktG (bzw. § 43 GmbHG):

- *„Die [Geschäftsleiter] haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Eine Pflichtverletzung liegt nicht vor, wenn [der Geschäftsleiter] bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln.“*

  => Hinreichende Entscheidungsgrundlage und Unternehmenswohl

WILHELM
RECHTSANWÄLTE

PFLICHTEN EINES MANAGERS – BSIG-E (NIS2)

§ 38 BSIG-E:

- (1) „*Geschäftsleitungen […] sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen*."

  => Umsetzungs- und Überwachungspflicht der Risikomanagementmaßnahmen i.S.d. § 30

- (3) „*Die Geschäftsleitungen […] müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten […] im Bereich [IT-Sicherheit] zu erlangen sowie um die Auswirkungen von Risiken […] auf die […] erbrachten Dienste beurteilen zu können.*"

  => Schulungspflicht für Manager

WILHELM
RECHTSANWÄLTE

PFLICHTEN EINES MANAGERS – BSIG-E (NIS2)

§ 30 BSIG-E Risikomanagementmaßnahmen:

- (1) *„[Unternehmen] sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, […] um Störungen […] zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten[…]. Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.“*

- (2) *„Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen […]. Die Maßnahmen müssen zumindest Folgendes umfassen:*
  - *Konzepte in Bezug auf [Risikoanalyse und IT-Sicherheit],*
  - *Bewältigung von Sicherheitsvorfällen,*
  - *Aufrechterhaltung des Betriebs […] nach einem Notfall, und Krisenmanagement,*
  - *Sicherheit der Lieferkette […],*
  - *Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von [IT-Systemen],*
  - *Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen […],*
  - *[…],*
  - *Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen,*
  - *Verwendung von Lösungen zur Multi-Faktor-Authentifizierung […].“*

WILHELM
RECHTSANWÄLTE

3 DECKUNG UNTER DER D&O-VERSICHERUNG?

WILHELM
RECHTSANWÄLTE

1. SZENARIO: KEINE CYBER-VERSICHERUNG

- Manager M verzichtet auf den Abschluss einer Cyberversicherung

(a) nach sorgfältiger Risikoabwägung, weil verfügbare Versicherungssumme zu niedrig ist und M dokumentiert dies

oder

(b) nach Hinweis im Jahresgespräch, weil „*das Internet für uns alle Neuland*“ ist

=> Cyberschaden ohne Cyberversicherung

WILHELM
RECHTSANWÄLTE

Abschluss einer Cyberversicherung
=> unternehmerische Ermessens-entscheidung (Business Judgment Rule)

Erfolgte die Entscheidung auf Grundlage angemessener Informationen?

ja

Keine Pflichtverletzung → Keine D&O Deckung

ABER, wenn Ermessensreduzierung auf Null:

Pflichtverletzung + → D&O-Deckung möglich

nein

Pflichtverletzung + → D&O-Deckung möglich

KEINE CYBER-VERSICHERUNG - ABER DECKUNG ÜBER D&O ?

WILHELM
RECHTSANWÄLTE

ABSCHLUSS CYBER-VERSICHERUNG - UNTERNEHMERISCHE ERMESSENS-ENTSCHEIDUNG

- Es besteht keine generelle Pflicht zum Abschluss einer Cyberversicherung.
- => Unternehmerische Ermessensentscheidung, Stichwort: Business Judgment Rule („BJR“)
- => Ohne angemessene Informationsgrundlage über das spezifische IT-Risiko kann sich ein Manager nicht auf die Business Judgement Rule berufen.
- Welche angemessenen Informationen müssen dem Manager vorliegen? Konkrete und mögliche Datenrisiken, Auswirkungen eines möglichen Cyberangriffs, Erfahrungen aus der Vergangenheit, Cyberversicherungsmarkt, Kosten, verbleibende Restrisiken, u.a.
- Eine Pflicht zum Abschluss einer Cyberversicherung besteht, wenn die einzig vertretbare Entscheidung der Abschluss einer Cyberversicherung ist (Stichwort: Ermessensreduzierung auf Null, gebundene Entscheidung).

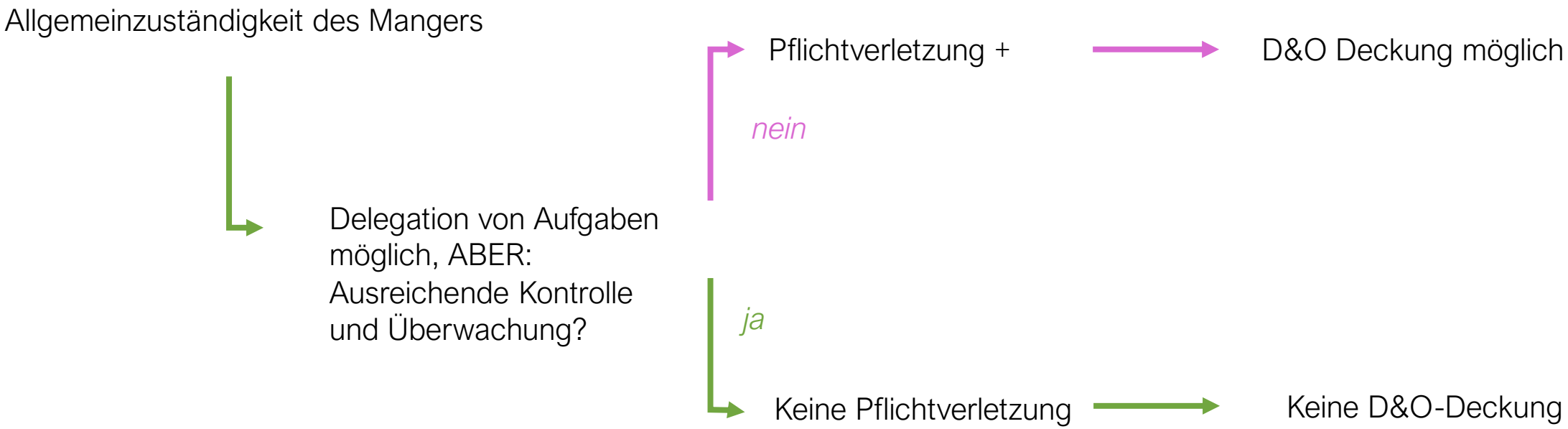
WILHELM
RECHTSANWÄLTE

2. SZENARIO: RÜCKTRITT DES CYBER-VERSICHERERS

- Cyberversicherer verlangt vor Vertragsschluss Beantwortung eines Risikofragebogens
- Eine Frage lautet:
  - „*Erfolgt der Zugriff auf Administratorenkonten mittels MFA*“?
- Leiter IT-Sicherheit beantwortet die Frage grob fahrlässig falsch mit „*Ja*“
- Angreifer verschlüsseln Unternehmensnetzwerk, weil Administratorenkonten nicht mittels MFA gesichert
- Cyberversicherer tritt wirksam nach § 19 VVG zurück

  => Kein Cyberversicherungsschutz

WILHELM
RECHTSANWÄLTE



RÜCKTRITT DES CYBERVERSICHERERS - DECKT DIE D&O DEN CYBERSCHADEN?

WILHELM
RECHTSANWÄLTE

DELEGATION VON AUFGABEN DES RISIKO-MANAGEMENTS

- Risikomanagement ist „Chefsache“ und „Daueraufgabe“.
- Vertikale / horizontale Delegation beim Umgang mit Cyberrisiken an fachlich qualifizierte Personen ist grundsätzlich möglich.
- Nach Delegation wandelt sich die eigene Handlungspflicht des Managers in eine Überwachungs- und Kontrollpflicht um.
- Letztverantwortung verbleibt bei der Geschäftsführung.

WILHELM
RECHTSANWÄLTE

3. SZENARIO: LEISTUNGS-KÜRZUNG NACH § 81 II VVG

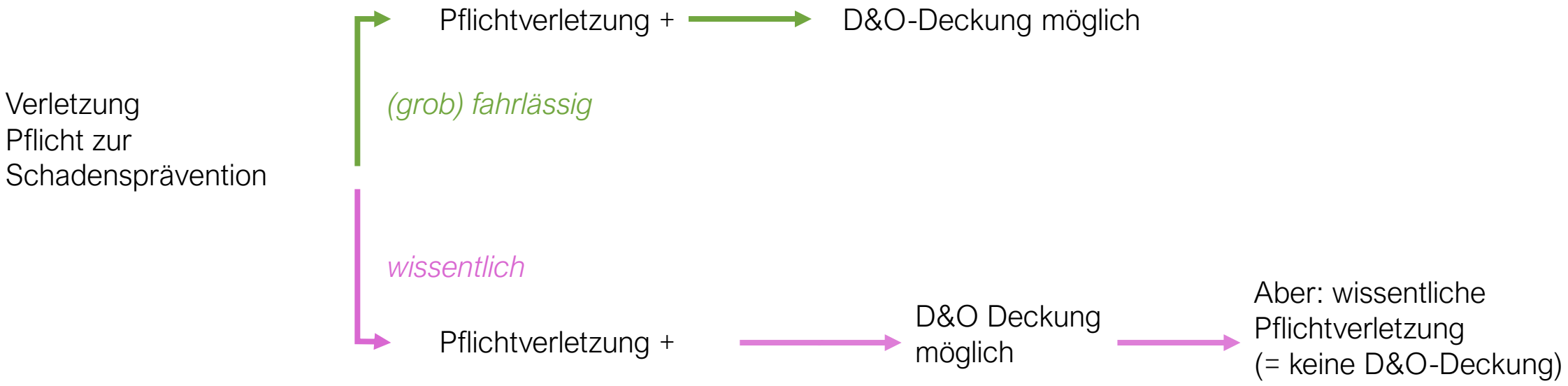
- Unternehmen führt Penetrationstest durch
- Penetrationstest offenbart erhebliche Sicherheitslücke
- Manager M verzögert Schließung der Sicherheitslücke

  (a) weil Jahresendstress, oder

  (b) weil Kosten seinen Bonus mindern
- Cyberangriff gelingt über Sicherheitslücke
- Cyberversicherer wendet ein:
  - Unterlassene Schließung = grob fahrlässige Herbeiführung des Versicherungsfalls (§ 81 Abs. 2 VVG)

  => Cyberversicherer macht Leistungskürzung auf Null geltend

WILHELM
RECHTSANWÄLTE



LEISTUNGSKÜRZUNG NACH § 81 II VVG – DECKT DIE D&O DEN CYBERSCHADEN?

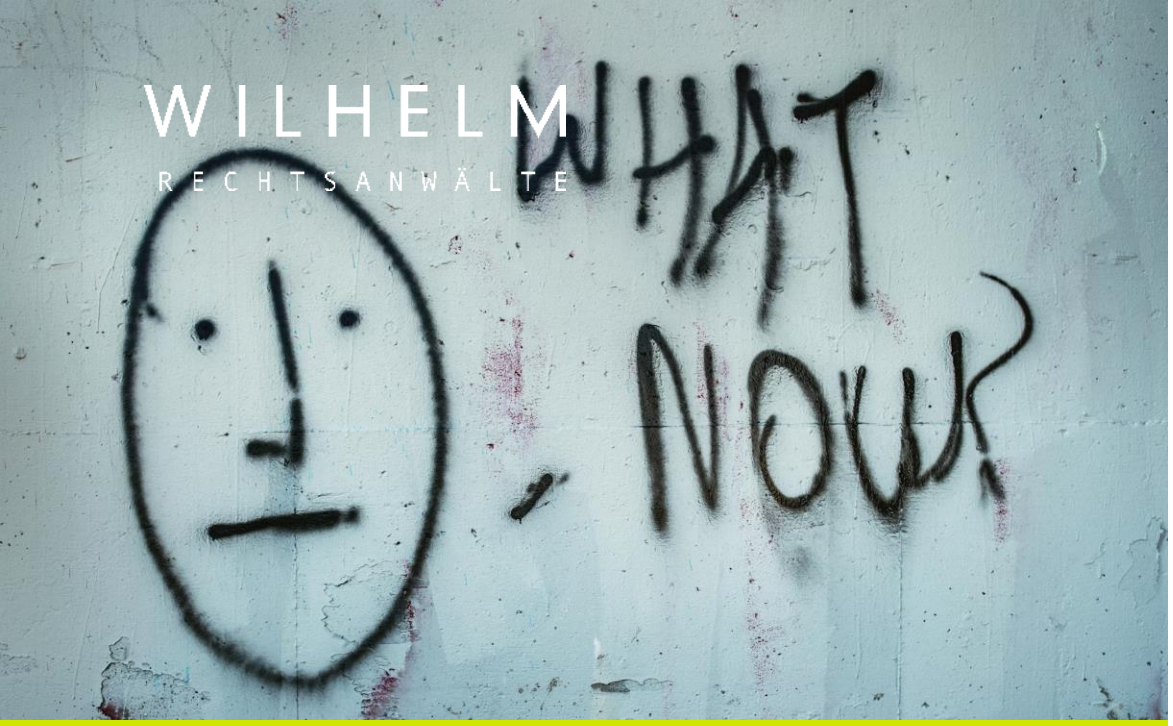
WILHELM
RECHTSANWÄLTE

PFLICHT ZUR SCHADENS-PRÄVENTION

- Die Geschäftsführung ist verpflichtet, die Cybersicherheit des Unternehmens durch geeignete Maßnahmen aufzubauen und zu erhalten.
- Die für das Unternehmen relevanten IT-Risiken muss die Geschäftsleitung kennen und geeignete Maßnahmen zur Vermeidung von Cyberattacken ergreifen, Stichwort: Schadensprävention.
- Bspw. Einrichtung von Notfallplänen und Maßnahmenkatalogen nach Entdeckung von Sicherheitslücken oder bei akuten Cyberangriffen (Stichwort Notfallmanagement).
- Eine regelmäßige Aktualisierung und Überprüfung sowie Anpassung der Notfallpläne und deren Dokumentation ist notwendig.
- Die Einhaltung der festgelegten Maßnahmen muss die Geschäftsleitung überwachen.

WILHELM
RECHTSANWÄLTE

4 FAZIT & AUSBLICK



MITTELBARER VERSICHERUNGS-SCHUTZ DURCH D&O-VERSICHERUNG

- Grundsätzlich:
  - D&O-Versicherung ist kein subsidiärer Cyberversicherungsschutz
- Im Einzelfall:
  - Beruht ein unversicherter Cyberschaden auf einem Managerfehler und kann über eine D&O Versicherung gedeckt sein
- Handlungsempfehlungen:
  - Bei fehlendem Cyberversicherungsschutz immer eine Managerhaftung bedenken
  - Bei Abschluss einer D&O-Versicherung darauf achten, dass der Vertrag keinen Ausschluss für Cyberschäden enthält

WILHELM
RECHTSANWÄLTE

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Bleiben wir im Gespräch:

Düsseldorf: +49 (0)211 68 77 460 | Berlin: +49 (0)30 81 72 7320
www.wilhelm-rae.de