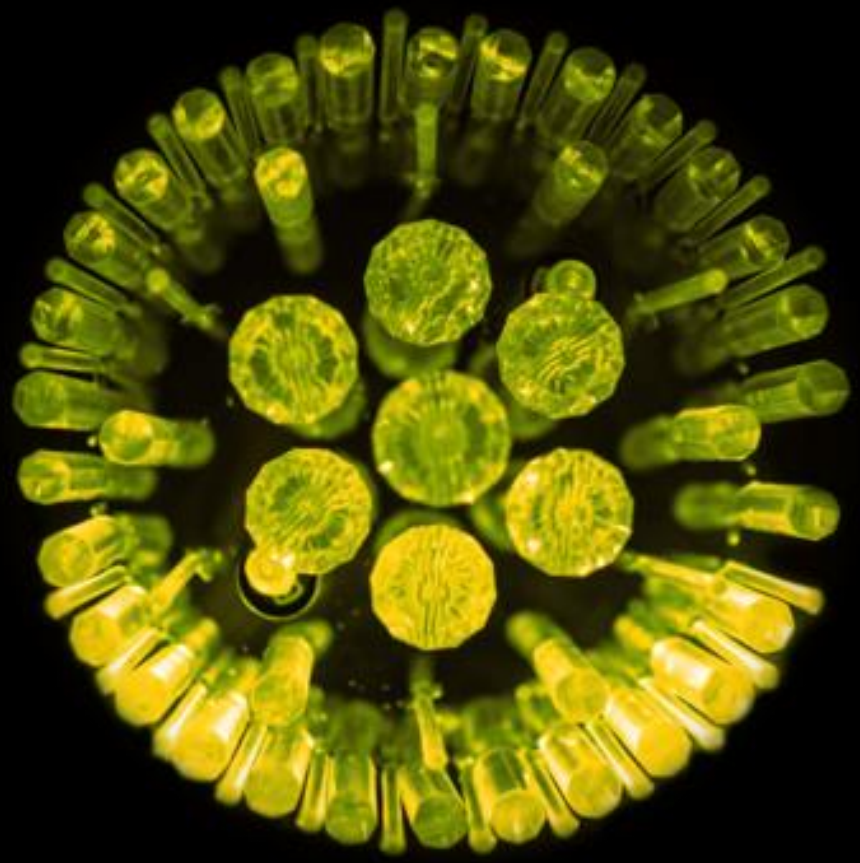
Deloitte. Legal

JANK WEILER OPERENYI RECHTSANWÄLTE



Persönliche Haftung des CISO im Bereich NIS 2 und DSGVO

3. September 2024 | RA Hon.-Prof. (FH) Mag. Sascha Jung, LL.M. LL.M.

CISO: Allgemeines

- Gesamtverantwortlicher für Informationssicherheit
- Entwicklung und Implementierung von Informationssicherheitsstrategien, -standards und -richtlinien
- Bereiche:
  - Security Operations
  - Cyber-Risiken und –Intelligence
  - Schutz vor Datenverlust und Betrug
  - Sicherheits-Architektur
  - Identitäts- und Zugangsmanagement (IAM)
  - Programm-Management
  - Forensik und Governance
- berichtet über die Ergebnisse des Information Security Management Systems („ISMS”) an die Geschäftsführung

Potenzielle Haftungsquellen für den CISO des Unternehmens iZm Cyber-Angriffen - Allgemeines

- An den CISO gemäß NIS 2 / DSGVO adressierte Geldbußen
- An den CISO als gemäß § 9 VStG verantwortlichen Beauftragten adressierte Geldbußen

Regress des CISO beim Unternehmen möglich?

- An das Unternehmen adressierte Geldbußen
- Direkte Schäden des Unternehmens (Betriebsausfälle, forensische Untersuchungen etc.)
- Schäden, für die das Unternehmen Dritten gegenüber haftet (gegen das Unternehmen gerichtete Schadenersatzansprüche wegen verspäteter/unterbliebener Lieferung/Leistung etc.)

Regress des Unternehmens beim CISO möglich?

Potenzielle Haftungsquellen für den CISO des Unternehmens iZm Cyber-Angriffen - Geldbußen

- Geldbußen nach NIS 2 und DSGVO adressieren das Unternehmen, dies gilt insbesondere für die Umsetzung von Risikomanagementmaßnahmen bzw. die DSGVO-Implementierungsmaßnahmen. CISO ist somit kein Haftungssubjekt für NIS 2 / DSGVO Geldbußen.

Keine NIS 2 / DSGVO Geldbußen gegen den CISO.

- Sofern und soweit CISO als verantwortlicher Beauftragter gemäß § 9 VStG bestellt wurde (nicht bei persönlichen Pflichten der GF; in Praxis nicht im Bereich der DSGVO; im Bereich von NIS 2 denkbar) ist CISO als Haftungssubjekt für verwaltungsstrafrechtliche Geldbußen zumindest denkbar.

§ 44 Abs 5 NISG 2024 bzw. § 30 Abs 3 DSG verhindern eine Übertragung der verwaltungsstrafrechtlichen Verantwortlichkeit: Von der Bestrafung des CISO als gemäß § 9 VStG verantwortlicher Beauftragter ist abzusehen, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person (Unternehmen) verhängt wird.

Potenzielle Haftungsquellen für den CISO des Unternehmens iZm Cyber-Angriffen - Schadenersatz

- An das Unternehmen adressierte Geldbußen
- Direkte Schäden des Unternehmens (Betriebsausfälle, forensische Untersuchungen etc.)
- Schäden, für die das Unternehmen Dritten gegenüber haftet (gegen das Unternehmen gerichtete Schadenersatzansprüche wegen verspäteter/unterbliebener Lieferung/Leistung etc.)

Regress für Schäden infolge schuldhafter Verletzung klar zugewiesener Handlungspflichten.

Anwendbarkeit des Dienstnehmerhaftpflichtgesetzes (keine Haftung bei entschuldbaren Fehlleistungen, richterliches Mäßigungsrecht bis auf Null bei leichter Fahrlässigkeit, richterliches Mäßigungsrecht bei grober Fahrlässigkeit) für Schäden des Arbeitgebers oder Dritter im Rahmen der Erfüllung der Dienstpflichten.

Alleine der Erfolg eines Hackangriffs bedeutet noch nicht zwingenderweise, dass die ergriffenen Sicherheitsmaßnahmen nicht ausreichend waren (EuGH C-340/21).

Potenzielle Haftungsquellen für den CISO des Unternehmens iZm Cyber-Angriffen - Handlungsempfehlungen

- Klar umschriebene Dienstpflichten
- Klar umschriebene (NIS 2) Projektpflichten
- Vollständige und rechtzeitige Umsetzung/Erfüllung von (NIS 2) Projektpflichten
- Bestätigung/Abnahme umgesetzter Projektpflichten
- Rechtlich wirksame Vereinbarung zur Übernahme von Verwaltungsstrafen (§ 9 VStG)

Deloitte. Legal | JANK WEILER OPERENYI RECHTSANWÄLTE

Stay in contact!

RA Hon.-Prof (FH) Mag. Sascha Jung, LL.M. LL.M.
Rechtsanwalt | Partner
Head of Data Protection | Cybersecurity & IP/IT | Media
Jank Weiler Operenyi Rechtsanwälte GmbH
Hohenstaufengasse 9, A-1010 Wien
T +43 1 513 09 13 DW 302 ; M +43 676 626 9912
s.jung@jankweiler.at / www.jankweiler.at