TCI RECHTSANWÄLTE

TCI RECHTSANWÄLTE TOP LISTED IN Best Lawyers® INTERNATIONAL

Corporate INTL Global Awards 2012 Winner

Persönliche Verantwortung und Haftungsrisiken des CISO / IT-Sicherheitsbeauftragten

Stephan Schmidt

Rechtsanwalt und Fachanwalt für IT-Recht

Gesellschaft für Informatik e.V. – Frankfurt a.M. – 09.11.2012

TCI
RECHTSANWÄLTE

„DER CISO IST PREDIGER, GEHEIM-AGENT UND NOTARZT IN EINEM.“

SIMON HÜLSBÖMER, COMPUTERWOCHE

…UND DEN DEUTSCHEN GESETZEN GÄNZLICH UNBEKANNT.

TCI
RECHTSANWÄLTE

I.

ERFORDERLICHKEIT EINES CISO / ITSB

TCI
RECHTSANWÄLTE

- Keine direkte gesetzliche Pflicht
  - Ausnahmen:
    - § 109 Absatz 3 TKG
    - Leitlinien zur Gewährleistung der Informationssicherheit (Niedersachsen – Ziffer 6 ISLL)
- zahlreiche gesellschaftsrechtliche Einfallstore (Pflicht zur ordnungsgemäßen Geschäftsführung - Sorgfaltspflichten, Leitungspflichten, Überwachungspflichten – z.B. Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, § 43 GmbHG, 93 Absatz 2 AktG und 116 AktG)
- Bestandteil dieser Pflichten ist die Zuständigkeit für wesentliche unternehmerische Entscheidungen

TCI
RECHTSANWÄLTE

- Geschäftsleitung muss sich selbst und höchstpersönlich um die Grundzüge der Unternehmenspolitik kümmern und darf diese Pflicht nicht delegieren,
- Grundzüge der Unternehmenspolitik liegen dann vor, wenn Aufgaben und Entscheidungen für das Unternehmen von besonderer Bedeutung sind (außergewöhnlich oder besondere Risiken)
- daher mittelbare Pflicht zur Ernennung eines CISO/ITSB, wenn betriebliche Erforderlichkeit gegeben (Ermessensfrage)

TCI
RECHTSANWÄLTE

II.

TYPISCHE FUNKTIONEN UND AUFGABEN

TCI
RECHTSANWÄLTE

- Definition IT-Sicherheit
  - *§ 2 Absatz 2 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik: „Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen*
    1. *in informationstechnischen Systemen, Komponenten oder Prozessen oder*
    2. *bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.“*
- Gegenwärtiger Stand der Technik zu gewährleisten (BSI-Grundschutzhandbuch, ISO/IEC 27001 oder ISO/IEC 15048)

TCI RECHTSANWÄLTE

ITSB

- Mangels gesetzlicher Regelung nur zugewiesene einmalige und laufende Aufgaben
- In der Regel Stabsstelle mit ausschließlich beratender Funktion (Haftung dann nur für Erkennung von Risiken)
- Wenn gewünscht, aktive Einräumung von Befugnissen erforderlich
- Überwachungsfunktion erfordert auch Durchsetzungsmöglichkeiten
- gegenüber Geschäftsleitung immer nur Beratung möglich
- Berichtspflichten an Geschäftsleitung

TCI RECHTSANWÄLTE

CISO auf Leitungsebene

- Gleiche Aufgaben wie der ITSB

aber

- wenn Mitglied der Geschäftsleitung, dann direkte Weisungsbefugnisse und entsprechende Verantwortlichkeiten und Haftung

TCI
RECHTSANWÄLTE

III.

AUSWAHLKRITERIEN

TCI RECHTSANWÄLTE

ITSB

Intern

- mögliche Kollision mit anderen Aufgaben (z.B. Tätigkeiten in IT-Abteilung, Sicherheitsbeauftragter nach SGB und DSB (BAG, Urteil v. 22.04.1994 – a.A. LAG Hamm, Beschluss v. 8.4.2011)
- eingeschränkte Haftung
- Keine Minderungs-möglichkeit bei Schlechtleistung
- Lohnfortzahlung im Krankheitsfall

Extern

- Risiko für vertrauliche Daten
- Zugriff auf Betriebsinterna
- keine Privilegierte Arbeitnehmerhaftung
- Verschuldensvermutung bei Pflichtverletzung
- Personelle Kontinuität muss sichergestellt sein

TCI
RECHTSANWÄLTE

- Persönliche Eignung
  - Anforderungen nicht gesetzlich geregelt
  - erforderliche Fachkenntnisse und hohe Zuverlässigkeit erforderlich
  - muss Risiken erkennen, Maßnahmen treffen und vermitteln können
  - Eventuell Anlehnungen an seit 1.11.2012 geltende Anforderungen an Compliance-Beauftragten nach Wertpapierhandelsgesetz-Mitarbeiteranzeigeverordnung
  - Zertifizierung möglich
  - öffentlichen Verwaltung - Bundesakademie für öffentliche Verwaltung: "IT-Sicherheitsbeauftragter der Öffentlichen Verwaltung“

TCI
RECHTSANWÄLTE

IV.

RECHTLICHE AUSGESTALTUNG

TCI
RECHTSANWÄLTE

- Interner ITSB → schriftliche Zusatzvereinbarung / Stellenbeschreibung zum Arbeitsvertrag
  - Bloße Weisung nicht ausreichend!
  - regelmäßige Überprüfung erforderlich
- Externer ITSB → Vertrag mit Dienst- und Werkvertraglichen Elementen
  - Vorsicht bei reinen Dienstverträgen – oft keine ausreichende Mängelhaftung, wenn kein Werk geschuldet
- Grundsatzregelung mit Betriebsrat hinsichtlich erforderlicher Eilmaßnahmen des ITSB / CISO erforderlich (vorläufige Zulässigkeit trotz Beteiligungsrecht)

TCI
RECHTSANWÄLTE

V.

HAFTUNG

TCI
RECHTSANWÄLTE

- Interne ITSB (1):
  - Haften als Arbeitnehmer aus arbeitsvertraglichen Pflichtverletzungen persönlich auf Schadensersatz, wenn Pflichtenkreis verletzt ist – gestaffelt nach Verschuldensgrad
    - Vorsatz → Volle Haftung
    - Grobe Fahrlässigkeit → Volle Haftung, wenn verhältnismäßig
    - „mittlere“ Fahrlässigkeit → anteilige Haftung
    - leichte Fahrlässigkeit → keine Haftung
  - Wenn Arbeitsvertrag keinen Pflichtenkreis bestimmt, Rückgriff auf BSI-Grundschutzhandbuch Kapitel M 2.193
  - Mindestens vertragliche Nebenpflicht Arbeitgeber auf Bedrohungen und Risiken hinzuweisen

TCI
RECHTSANWÄLTE

- Interne ITSB (2):
  - Haftung gegenüber Dritten für eigenes Fehlverhalten

    ABER: Haftungsmaßstäbe sind streng auszulegen
    - Beispiel: Vertragsgestaltung und -dokumentation bei komplexen Projekten ohne juristische Beratung
  - Haftung nach allgemeinen Gesetzen wie z.B. §§ 823, 831 BGB und Spezialregelungen wie § 44 TKG und §§ 7, 9 BDSG
  - Mögliche strafrechtliche Haftung (Fernmeldegeheimnis, Computerstraftaten, Urkundenunterdrückung …)

TCI
RECHTSANWÄLTE

- Externe ITSB:
  - Ähnliche Haftung wie interner ITSB, nur aus schuldrechtlichem Vertrag
  - aber kein arbeitsrechtliches Haftungsprivileg
  - Individualvertragliche Haftungsbeschränkungen möglich
  - von Haftungsbeschränkungen in Standardverträgen oder AGBs ist wegen den Einschränkungen des AGB-Rechts abzuraten

TCI
RECHTSANWÄLTE

- CISO auf Leitungsebene:
  - Haftung für Organisations- und Auswahlverschulden hinsichtlich Mitarbeiter
  - Haftung für eigene Organisationsfehler
  - Haftung bsp. nach § 91 Abs. 2 AktG → keine vollständige Befreiung durch Delegation möglich
  - Strafbarkeit wegen Unterlassen trotz Garantenstellung möglich
    - BGH Urteil zum CCO v. 17.17.2009 - 5 StR 394/08

TCI
RECHTSANWÄLTE

VI.

SCHUTZ VOR HAFTUNG

TCI
RECHTSANWÄLTE

- Vertragsrechtliche Lösungen
  - Ergänzende Haftungsbeschränkungen zum Arbeitsvertrag möglich
  - jedoch unüblich und schwer durchzusetzen
  - Bei externen ITSB Haftungsbegrenzung im Vertrag möglich

- Versicherungsrechtliche Lösungen
  - D&O-Versicherungen nur für CISO auf Geschäftsleitungsebene
  - Keine Lösung für interne ITSB
  - Haftpflichtversicherungen für externe ITSB möglich

TCI
RECHTSANWÄLTE

Geschafft… noch Fragen?

Rechtsanwalt Stephan Schmidt
Fachanwalt für Informationstechnologierecht

TCI Rechtsanwälte
Isaac-Fulda-Allee 5
D-55124 Mainz
Telefon: +49 - (0) 6131 - 302 90 460
Telefax: +49 - (0) 6131 - 302 90 466
E-Mail: sschmidt@tcilaw.de
Internet: www.tcilaw.de

Mitglied im iT klub
Eine Initiative der IT-Akademie Mainz und der Wirtschaftsförderung