BAKER & McKENZIE

Cybersecurity Insurance

Versicherbare rechtliche Cyber-Risiken

RA Dr. Lukas Feiler, SSCP, CIPP/E

Security Forum 2015
23. April 2015

Topics

I. Zentrale rechtliche Cybersecurity-Risiken
   a. Persönliche Haftung der Geschäftsleitung für IKS
   b. Verwaltungsstrafrechtliche Verantwortlichkeit
   c. Schadenersatzpflicht bei Datenschutzverletzungen
   d. Kosten einer Data Breach Notification
   e. Verlust der Patentfähigkeit von Erfindungen
   f. Schadenersatzpflichten gegenüber Kunden

II. Versicherbarkeit von Cybersecurity-Risiken
   a. Fallstricke in Versicherungsbedingungen
   b. Praktische Behandlung von Schadenfällen

Persönliche Haftung der Gesellschaftsleitung für das Interne Kontrollsystem

- Kapitalgesellschaften sind zur Führung eines IKS verpflichtet (§ 82 AktG / § 22 GmbHG)
- Geschäftsleitung haftet der Gesellschaft für IKS
  - Objektiver Sorgfaltsmaßstab: Sorgfalt eines ordentlichen Geschäftsmannes (§ 25 GmbHG / § 84 AktG)
- IKS: Methoden und Maßnahmen, die dazu dienen
  - das Vermögen zu sichern,
    - Vertraulichkeit von Geschäftsgeheimnissen
    - Integrität von urheberrechtlich geschützten Werken (zB Software)
    - Verfügbarkeit aller Digital Assets
  - die Genauigkeit und Zuverlässigkeit der Abrechnungsdaten zu gewährleisten
    - Integrität des Buchhaltungssystems

Verwaltungsstrafrechtliche Verantwortlichkeit

- Geschäftsleitung oder gewerberechtlicher Geschäftsführer haftet für Verwaltungsstrafen – Gesellschaft haftet solidarisch
- Verstöße gegen das Datenschutzgesetz
  - Verwaltungsstrafen von bis zu EUR 10.000, wenn personenbezogene Daten nicht angemessen geschützt werden (§ 52 DSG 2000)
- Neue Pflichten nach IT-Sicherheitsgesetz
  - Netzwerk- und Informationssicherheits-Richtlinie der EU sieht verpflichtende Sicherheitsmaßnahmen für Betreiber kritischer Infrastrukturen vor (Energie, Verkehr, Banken, Gesundheit, …)
  - Frühzeitige Umsetzung durch österr. IT-Sicherheitsgesetz

Schadenersatzpflicht bei Datenschutzverletzungen

- Bei schuldhafter Missachtung der Datensicherheitspflichten haftet ein Unternehmen (§ 33 DSG 2000)
  - für Vermögensschaden, der durch Sicherheitsverletzung entsteht
  - für immateriellen Schaden wenn
    - Daten öffentlich zugänglich werden
    - zur Bloßstellung des Betroffenen geeignet (insb. bei sensiblen Daten)
- Unternehmen haftet auch für das Verschulden seiner Leute
- Unternehmen muss beweisen, dass es kein Verschulden trifft

Kosten einer verpflichtenden Breach Notification

- Gesetzliche Notifikationspflicht (§ 24 Abs 2a DSG 2000), wenn:
  - Dem Unternehmen bekannt wird, dass personenbezogene Daten "systematisch und schwerwiegend" unrechtmäßig verwendet wurden und
  - den Betroffenen Schaden droht
  - Ausnahme: Notifikation unverhältnismäßig zu drohendem Schaden
  - Notifikation in "geeigneter" Form und "unverzüglich"
- Vertragliche Notifikationspflicht
  - wenn dem Vertragspartner Schaden droht
  - Unabhängig, ob "systematisch und schwerwiegend"

Verlust der Patentfähigkeit von Erfindungen

- Erfindungen können nur dann als Patent angemeldet werden, wenn sie insb „neu“ sind
  - dh nicht zum Stand der Technik gehören, der aus allem besteht, was der Öffentlichkeit vor der Anmeldung zugänglich war
  - Auch von Hacker/Konkurrent veröffentliche Informationen können Verlust der Neuheit bewirken
  - Einzige mögliche Verteidigung des Anmelders: Beweis des Zusammenhangs zwischen Hacking & neuheitsschädlicher Veröffentlichung (§ 3 Abs 4 Z 1 PatG)

Schadenersatzpflicht gegenüber Kunden

- Weitgehende Haftungsausschlüsse in Verträgen üblich
- Allerdings: Übliche Geheimhaltungsklauseln sind Einfallstor für Haftung:
  - Der Vertragspartner verpflichtet sich vertrauliche Informationen nicht offenzulegen und die Offenlegung mit demselben Maß an Sorgfalt zu verhindern, wie für seine eigenen vertraulichen Informationen – ohne dabei ein angemessenes Maß an Sorgfalt zu unterschreiten.
- Haftung für sämtliche Vermögensschäden des Vertragspartners einschließlich entgangener Gewinn, Reputationsschäden etc.

Versicherbarkeit von Cybersecurity-Risiken

- Marktentwicklungen
  - Kosten einer Sicherheitsverletzung können signifikant sein
    - Rechtliche Risiken
    - Wirtschaftliche Risiken (für welche Geschäftsleitung haftbar sein kann)

    → Wachsende Anreize Cybersecurity-Versicherungen abzuschließen
  - Versicherungsunternehmen bieten zunehmend Cybersecurity-Versicherungsprodukte an

Mögliche Bausteine für eine Cybersecurity-Versicherung

- Datenbeschädigung oder -verlust (Datenwiederherstellung, Forensik, Krisenkommunikation)
- Personal Data Breach (Notifikationskosten, Verfahrenskosten, Verwaltungsstrafen, …)
- Haftung für Personal Data Breach (Schadenersatzpflicht, Beratungs- und Vertretungskosten)
- Vertragshaftung (zB PCI-DSS od Pönalen in Kundenverträgen)
- Sachschaden
- Betriebsunterbrechung (insb. entgangener Gewinn)
- Reputationsschaden
- Cyber-Epressung/Lösegeld

Tücken der Cybersecurity-Versicherung

- Gutes quantitatives Risk Assessment als Vorbedingung
- Versicherungsschutz genau definieren
  - Schwachstellen in Standard-Software oft ausgenommen
    - "Class Breaks" schwer versicherbar
    - Heartbleed, Shellshock, GHOST
  - Outsourcing ausgenommen?
    - Daten auch versichert, wenn bei Dienstleister gespeichert?
  - Patentrecht ausgenommen?
    - Risiken insb. nach US-Recht schwer versicherbar

Baker & McKenzie denkt von Anfang an global. Seit der Gründung.
Internationalität liegt uns in den Genen.