Security as a Service

ICT-Security Outsourcings: Anforderungen und Lösungen aus rechtlicher Sicht

Dr. Jürg Schneider, Partner, Walder Wyss AG

22. November 2016
ISSS Berner Tagung 2016

walderwyss rechtsanwälte

Inhaltsübersicht

- Einführung in die Thematik
- Einige Beispiele und Zahlen
- Rechtliche Anforderungen an Informationssicherheit
- Verantwortung/Haftung für Informationssicherheit
- Security Services
- Pflicht zum Outsourcen?
- Schranken des Outsourcings
- Wichtige Regelungspunkte im Outsourcingvertrag
- Security Services über die Cloud
- Fünf «Take Aways»

Einführung in die Thematik

- Information ist wichtig(st)es Betriebsmittel und Wirtschaftsgut
- Informationsverlust oder Informationsdiebstahl kann Existenz eines Unternehmens bedrohen
- Keine einzelne allumfassende rechtliche Regelung im Bereich Informationssicherheit und Outsourcing
- Haftungs- und Reputationsrisiken werden oft unterschätzt

Einige Beispiele und Zahlen

- 500 Millionen Yahoo-Konten gehackt, 2014
- DDoS/Erpressung von ProtonMail, November 2015
- Cyber-Spionagefall bei der RUAG, Januar 2016
- Friend Finder Netzwerk gehackt, November 2016
- Gemäss Ponemon Institute (2016 Cost of Data Breach Study, June 2016):
  - 4 Mio. USD Kosten pro «Data Breach» (+29% seit 2013)
  - 158 USD Kosten pro verlorenen/gestohlenen Datensatz (+15% seit 2013)

Rechtliche Anforderungen an Informationssicherheit

- Gesetzliche Regelungen:
  - Datenschutzgesetzgebung (DSG, VDSG etc.)
  - Kaufmännische Rechnungslegung (Art. 957 ff. OR, GebüV)
  - Internes Kontrollsystem (Art. 728a Abs. 1 Ziff. 3 OR)
  - Geschäfts-, Amts- und Berufsgeheimnis (Art. 162 StGB, Art. 320 StGB und Art. 321 StGB)
  - Finanzmarktgesetzgebung (Finma Rundschreiben 2008/7 [Outsourcing], 2008/21 [Operationelle Risiken Banken] etc.), etc.
- Vertragliche Anforderungen
- Standards (ISO, etc.)
- Ausländische Anforderungen: z.B. EU Datenschutz-grundverordnung, EU Richtlinie für Netz- und Informations-sicherheit, etc.

Verantwortung/Haftung für Informationssicherheit

- Zivilrecht / Strafrecht
- Vertragliche Haftung (Art. 97 OR) / ausservertragliche Haftung (Art. 41 OR)
- Haftung des Geschäftsherrn: Art. 55 OR
- Haftung für Hilfspersonen: Art. 101 OR
- Organhaftung: Art. 754 OR, Art. 827 OR, Art. 916 OR

Pro memoria: Versicherung von Informationssicherheitsrisiken

Security Services

Outsourcing von z.B.

- Firewall / VPN / IDP
- DDoS Protection / Malware Protection
- komplette Cybersecurity Infrastruktur
- Penetration Testing, Security Audits
- Data Loss Prevention, Data Storage sowie Archiving Services
- Data Center Security (inkl. physischer Zugangsschutz)
- Encryption Services
- Information Security Officer Funktion
- bis zur umfassenden Gewährleistung der ICT-Sicherheit (as a Service)

Pflicht zum Outsourcen?

- Keine allgemeine und generelle Pflicht zum ICT-Security Outsourcing
- Verzicht kann jedoch im Schadenfall eine Haftung des Unternehmens auslösen:
  - Sorgfaltspflichtverletzung
  - Übernahmeverschulden (Fähigkeitsdefizit: Schuldner hätte eine Leistung oder Tätigkeit nicht übernehmen dürfen)
  - Organisationsverschulden (sachliche oder zeitliche Fehlallokation der Ressourcen Ressourcen)
- Verzicht kann zu einer persönlichen Haftung der Organe führen (Achtung: Oberaufsicht kann nicht delegiert werden)
- Steigende Komplexität der Informationssicherheit sowie steigende rechtliche Anforderungen erhöhen das Haftungsrisiko
- **Achtung**: Beizug eines Dienstleisters führt nicht dazu, dass die rechtlichen und vertraglichen Pflichten des Kunden in Bezug auf Informationssicherheit auf den Dienstleister übergehen; verpflichtet bleibt weiterhin der Kunde (er kann dann jedoch allenfalls seine Haftung limitieren/ausschliessen, sich exkulpieren und/oder Regress auf den Dienstleister nehmen)

Schranken des Outsourcings

- Schranken/Einschränkungen auf Grund von, z.B.
  - Datenschutz
  - vertragliche Geheimhaltungspflichten
  - Spezielle Branchengesetzgebung (z.B. Finanzmarktgesetzgebung)
- Thematik Berufsgeheimnis (Art. 321 StGB) sowie Bankkundengeheimnis (Art. 47 BankG)
  - Ist Dienstleister eine Hilfsperson des Berufsgeheimnisträgers? Umstritten. Falls ja, keine Einwilligung notwendig.
  - Bankkundengeheimnis: gemäss FINMA keine Einwilligung notwendig (jedoch vorgängige Information) (vgl. Rundschreiben 2008/7) (umstritten)
- Thematik «Blocking Statutes» (insb. Art. 273 StGB)
  - Fällt Zugänglichmachen von Informationen an einen ausländischen Dienstleister unter Art. 273 StGB?
- Auswahl des Anbieters («Due Diligence»)
- Retention des betriebsspezifischen Know-hows / Management der Provider-Schnittstelle / Reversibilität
- Achtung: spezielle Regelungen für die öffentliche Hand (z.B. im Bereich Datenschutz, Amtsgeheimnis etc.)

Wichtige Regelungspunkte im Outsourcingvertrag

- Präziser Leistungsbeschrieb, Service Levels, Einhaltung von Standards
- Klare Zuweisung der Verantwortlichkeiten und Regelung der Haftung
- Ausdrückliche Unterstellung unter Berufsgeheimnis und Bezeichnung als Hilfsperson (sofern anwendbar)
- Datenschutz (inkl. Dateninhaberschaft, Bearbeitungsort, Bearbeitungszwecke etc.)
- Behördenkontakte und Pflichten/Kooperation bei Verletzungsverfahren sowie Data Breaches
- Anpassung an gesetzliche Anforderungen sowie Standards
- Kontroll- und Prüfrechte
- Step-in und Beendigungsrechte
- Exit Services

Security Services über die Cloud

- Grundsätzlich ähnliche Anforderungen, jedoch
  - Datenschutz und Data Location
  - Kontroll- und Prüfrechte
  - Exit Services

  besonders wichtig

Fünf «Take Aways»

- Informationssicherheit ist Chefsache
- Je nach Konstellation ist der Beizug eines Dienstleisters erforderlich (Stichworte: Sorgfaltspflicht, Übernahmeverschulden, Organisationsverschulden)
- Verpflichtet bleibt weiterhin der Kunde (er kann dann jedoch allenfalls seine Haftung limitieren/ausschliessen, sich exkulpieren und/oder im Schadenfall Regress auf den Dienstleister nehmen)
- Gesetzliche (z.B. Datenschutz) und vertragliche Schranken beachten
- Saubere und präzise Vertragsgestaltung ist notwendig

Danke für Ihre Aufmerksamkeit

Kontakt

Walder Wyss AG

Dr. iur. Jürg Schneider, Partner

Seefeldstrasse 123

Postfach 1236

CH-8034 Zürich

Tel. +41 58 658 55 71

juerg.schneider@walderwyss.com

www.walderwyss.com