Security Breaches: Rechtliche Notfallmaßnahmen für betroffene Unternehmen

WOLF THEISS

Dr. Lukas Feiler, SSCP

Associate, Wolf Theiss Rechtsanwälte GmbH

TOPICS

1. Security Breaches aus strafrechtlicher Sicht
2. Data Breach Notification
3. Rechtliche Möglichkeiten der Täterausforschung

WOLF THEISS

Security Breaches aus strafrechtlicher Sicht – Die Täter

- Organisierte Kriminalität
  - “Diebstahl“ von Kreditkartendaten
- „Hacktivists“
  - Image-Schäden
- Insider / Eigene Mitarbeiter
  - Vandalismus
  - Industriespionage
- Advanced Persistent Threats (APTs)
  - Industriespionage

Hacking als Straftat

- Hacking ist strafbar, wenn (§ 118a StGB)
  - Zugangsverschaffung zu einem Computersystem (od. einem Teil davon) erfolgt
  - indem spezifische Sicherheitsvorkehrungen im Computersystem überwunden werden
    - Sofern der Täter
      - Spionageabsicht und
      - Daten-Verwendungsabsicht und
      - Gewinn- bzw. Schädigungsabsicht hat
  - Strafdrohung: 6 Monate
  - Nur mit Ermächtigung des Verletzten zu verfolgen

Strafloses Hacking

- Hacking ohne Überwindung einer „Sicherheitsvorkehrung im Computersystem“
  - Social Engineering
  - Überwindung von nur physischen Sicherheitsvorkehrungen
- Hacking ohne Spionageabsicht
  - Hacking von tausenden PCs zwecks Errichtung von Botnets für
    - Spamming
    - Vermietung des Botnets an den Meist-Bietenden
- Hacking ohne Gewinn- bzw. Schädigungsabsicht
  - zB: nur die Absicht, Sicherheitslücke aufzudecken

Datenbeschädigung

- Vermögensschädigung eines anderen durch Verändern/Löschen/Unterdrücken von Daten (§ 126a StGB)
- Strafdrohung: 6 Monate; bei Schaden von mehr als 3.000 EUR: 2 Jahre; bei mehr als 50.000 EUR: 5 Jahre

- z.B. Web-Defacement, sofern dadurch ein Vermögensschaden entsteht

Denial of Service (DoS) Attacks

- Schwere Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB)
  - Strafdrohung: 6 Monate; wenn Störung „länger andauert“: 2 Jahre
  - z.B.:
    - Vorsätzliche Teilnahme an einem Distributed Denial of Service (DDoS) Attack

Verwendung personenbezogener Daten

- Gerichtliche Straftat (§ 51 DSG 2000), wenn
  - Rechtswidrige Verwendung von widerrechtlich verschafften personenbezogener Daten
  - mit Gewinn- oder Schädigungsabsicht
  - Strafdrohung: bis zu 1 Jahr
  - → nicht, wenn Daten verschafft werden, um eine Sicherheitslücke beweisen zu können

Industriespionage

- Auskundschaftung eines Geschäftsgeheimnisses (§ 123 StGB)
  - Auskundschaftung
  - mit Verwertungs- oder Veröffentlichungsvorsatz
  - Strafdrohung: 2 Jahre
- Preisgabe von Geschäftsgeheimnissen durch Insider (§ 11 UWG)
  - Mitteilung des Geheimnisses an Dritte
  - durch Bediensteten während aufrechtem Dienstverhältnis
  - Strafdrohung: 3 Monate

Data Security Breach Notification

- *Die Pflicht betroffene Personen von der Kompromittierung ihrer personenbezogenen Daten zu informieren.*
- Eine „Erfindung“ aus Kalifornien:
  - California Senate Bill 1386 (2002)
- Zweck:
  - Betroffene sollen reaktive Maßnahmen ergreifen können
  - Markt-Transparenz hinsichtlich Daten-Sicherheit
- Rechtsquellen in Österreich:
  - Gesetz: § 24 Abs 2a DSG 2000; § 95a TKG 2003
  - Verträge

Breach Notification nach DSG 2000

- § 24 Abs 2a DSG 2000: Notifikations-Pflicht, wenn:
  - Unternehmen bekannt wird, dass personenbezogene Daten „systematisch und schwerwiegend“ unrechtmäßig verwendet wurden und
  - den Betroffenen Schaden droht
- Ausnahme: wenn Notifikation nicht im Verhältnis zum geringfügigen drohenden Schaden steht
- Form der Notifikation: „in geeigneter Form“
- Zeitpunkt der Notifikation: „unverzüglich“
- Rechtsfolge der Verletzung:
  - Verwaltungsstrafe: bis zu EUR 10.000 (§ 52 Abs 2 DSG 2000)
  - Haftung für Vermögensschäden nach allgem. Zivilrecht

Breach Notification nach TKG 2003

- § 95a TKG 2003: Notifikations-Pflicht, wenn:
  - Betreiber eines öffentlichen Telekommunikationsdienstes erfährt, dass Vernichtung, Verlust, Veränderung oder unbefugte Weitergabe/Zugang zu personenbezogenen Daten, die iZm Diensterbringung verarbeitet wurden
  - Datenschutzkommission ist immer zu informieren
  - Betroffene sind zu informieren, wenn anzunehmen ist, dass Privatsphäre oder personenbezogene Daten beeinträchtigt
- Ausnahme: geeignete technische Sicherheitsmaßnahmen getroffen
- Rechtsfolge der Verletzung:
  - Verwaltungsstrafe: bis zu EUR 37.000 (§ 109 Abs 3 TKG 2003)
  - Haftung für Vermögensschäden nach allgem. Zivilrecht

Breach Notification nach Vertrag

- Wenn Breach Notification in einem Vertrag nicht geregelt ist, gilt:
  - Notifikation einer Sicherheitsverletzung hat zu erfolgen, wenn dem Vertragspartner aus dieser ein Schaden droht (sog. nebenvertragliche Schutzpflicht)
  - Betroffene sind unverzüglich zu informieren
- Rechtsfolge der Verletzung:
  - Vertragliche Haftung für Vermögensschäden

Data Breach Notification: Auswirkungen auf den IT-Markt

WOLF THEISS

- Abbau der Informationsasymmetrie:
  - Kunden haben – im Unterschied zu Anbietern – idR keine Information über die Sicherheit eines Dienstes
  - Breach Notifications bringen neue Transparenz & Konkurrenz in Bezug auf IT-Sicherheit
  - Chance für Unternehmen, die mehr Daten-Sicherheit bieten!
- Internalisierung des Risikos Data Breach
  - Bisher: Data Breach weitgehend eine Externality
  - Nunmehr: Betroffenes Unternehmen trägt größeren Teil der negativen Folgen

Rechtliche Möglichkeiten der Täterausforschung

- Best-Case Scenario: Der Täter kann bis zu einer österreichischen IP-Adresse zurückverfolgt werden

- Frage: Wie erlangt man Auskunft darüber, wem eine IP-Adresse zum Tatzeitpunkt zugewiesen war?

Täterausforschung – Auskunft über eine IP-Adresse

WOLF THEISS

- Privater Auskunftsanspruch?
  - § 18 Abs 4 E-Commerce-Gesetz: Hosting-Provider haben Name und Adresse eines Nutzers auf Verlangen dritten Personen zu übermitteln, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers glaubhaft machen
  - Galt auch für Access-Provider (OGH 4 Ob 7/04i), nicht jedoch bei dynamischen IP-Adressen (OGH 4Ob41/09x)
  - Mit Einführung der Vorratsdatenspeicherung: keine Auskunftspflicht gegenüber Privaten (§ 99 Abs 5 TKG 2003)

Täterausforschung – Auskunft über eine IP-Adresse

WOLF THEISS

- Behördlicher Auskunftsanspruch
  - Seit 1.4.2012: Staatsanwalt hat das Recht, von einem Access-Provider Auskunft über Name & Anschrift zu erhalten (§ 76a StPO)
  - Um den Staatsanwalt einzuschalten:
    - Strafanzeige gegen Unbekannt einbringen
    - Wenn Ermächtigungsdelikt (zB § 118a StGB): Ermächtigung zur Strafverfolgung erteilen
  - Nicht möglich, wenn nur sog. Privatanklagedelikt (zB § 91 UrhG)

(Legal) Emergency Response Plan

- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Follow-Up

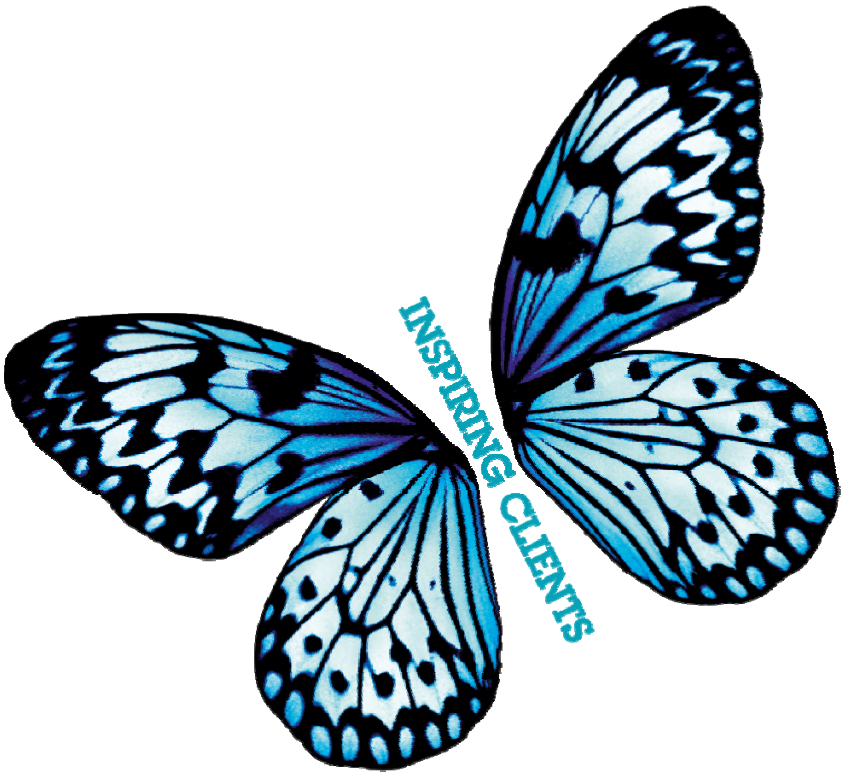
→ Kenntnisse der rechtlichen Pflichten

→ Breach Notification

→ Sammlung von Beweismitteln & Auskunftsansprüche gegen Provider

→ Gerichtliche Durchsetzung von Ansprüchen / strafrechtliche Verfolgung

Danke für Ihre Aufmerksamkeit!



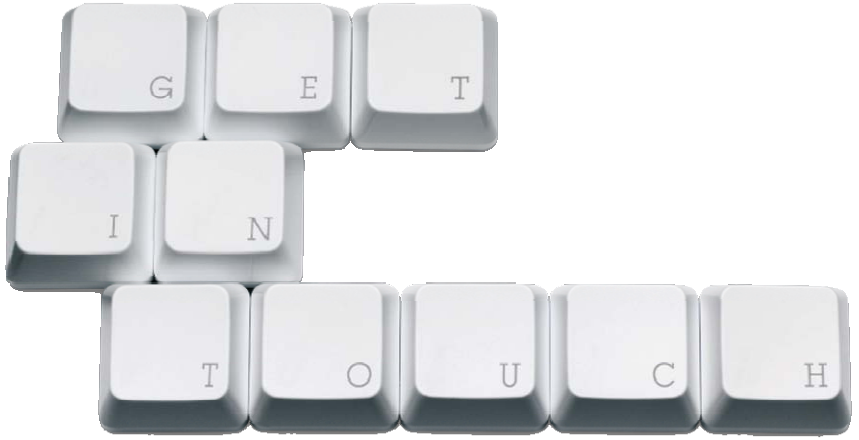
KONTAKTADRESSE

Dr. Lukas Feiler, SSCP

Wolf Theiss Rechtsanwälte GmbH
Schubertring 6, 1010 Wien

Tel: (+ 43 1) 515 10 5090
Fax: (+ 43 1) 515 10 665090

e-mail: lukas.feiler@wolftheiss.com



www.wolftheiss.com