Cyber Crime und seine rechtlichen Folgen für betroffene Unternehmen

WOLF THEISS

Dr. Lukas Feiler, SSCP

Associate, Wolf Theiss Rechtsanwälte GmbH

TOPICS

1. Überblick über das österreichische Computerstrafrecht
2. Haftungsrechtliche Folgen von Security Breaches
3. Data Breach Notification

Cyber Crime – Wer sind die Täter?

- Organisierte Kriminalität
  - Botnets
  - Phishing
  - “Diebstahl“ von Kreditkartendaten
- „Hacktivists“
  - Image-Schäden
- Advanced Persistent Threats (APTs)
  - Industriespionage

Hacking als Straftat

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

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

Sniffing

- Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB)
  - Gilt für menschliche Nachrichten am Übertragungsweg
  - Benützen einer Abhörvorrichtung
  - Mit Spionageabsicht
- Abfangen von Daten (§ 119a StGB)
  - Gilt für alle Daten am Übertragungsweg
  - Benützen einer Abhörvorrichtung
  - sofern der Täter
    - Spionageabsicht und
    - Daten-Verwendungsabsicht und
    - Gewinn- bzw. Schädigungsabsicht hat

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 einer 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
- Verwaltungsübertretung (§ 52 DSG 2000), wenn
  - Widerrechtliche Zugangsverschaffung zu einer Datenanwendung
  - Strafdrohung: Verwaltungsstrafe von bis zu 25.000 EUR

Industriespionage

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

Haftung von kompromittierten Unternehmen

- Haftung gegenüber Betroffenen, deren Daten kompromittiert wurden (§ § 14, 33 DSG 2000)
  - Wenn angemessene Sicherheitsmaßnahmen schuldhaft nicht implementiert wurden
  - Grds nur Haftung für Vermögensschäden
  - Haftung auch für ideelle Schäden: bei „Bloßstellung“ in der Öffentlichkeit

Haftung von kompromittierten Unternehmen #2

- Haftung gegenüber Vertrags-Kunden
  - Vertragliche Haftung
  - Grds nur Haftung für Vermögensschäden
  - Haftung wird meist auf grobe Fahrlässigkeit & Vorsatz beschränkt

Haftung von kompromittierten Unternehmen #3

- Haftung gegenüber Kreditkartenorganisationen (z.B. Visa oder MasterCard)
  - Unternehmen, die Kreditkartendaten verarbeiten sind oft vertraglich zur Einhaltung des Payment Card Industry Data Security Standard (PCI DSS) verpflichtet

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 personenbezogenen 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 von Sicherheitsverletzungen hat zu erfolgen, wenn dem Vertragspartner aus diesen ein Schaden droht (sog. nebenvertragliche Schutzpflicht)
  - Betroffene sind unverzüglich zu informieren
- Rechtsfolge der Verletzung:
  - Vertragliche Haftung für Vermögensschäden

Data Breach Notification: Mögliche Auswirkungen auf den IT-Markt

WOLF THEISS

- Wenn Fokus auf Ermöglichung reaktiver Maßnahmen durch Betroffene:
  - Viele Breaches werden nicht notifiziert, da kein (zusätzliches) Risiko – der Schaden ist oft bereits eingetreten
  - Betroffene wissen oft nicht, wie sie reagieren sollen
- Wenn Fokus auf Markt-Transparenz
  - Alle Data Breaches – unabhängig von einem Risiko – wären zu notifizieren
  - Der IT-Markt würde hinsichtlich Information Security an Transparenz gewinnen
  - Internalisierung des Risikos „Data Breach“
    → Neue Anreize für mehr Sicherheit werden geschaffen!

Danke für Ihre Aufmerksamkeit!

WOLF THEISS

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