Cyber Security
Fälle & Rechtliche Grundlagen

Zürich – 15. November 2018

Was können Sie heute erwarten?

Verletzung der Cyber Security - akademisches Problem oder echte Bedrohung?

Verletzung der Cyber Security - akademisches Problem oder echte Bedrohung?

- British Airways
- Delta
- Air Canada
- Carphone
- Digitec
- EOS
- Groupe Mutuel
- Abbott Laboratories
- Industrielle Steuerungssysteme / IoT

Warum?

- Freude an der technischen Herausforderung
- Konkrete finanzielle Interessen
- Erpressung

  → Uber-Fall
- Angedrohter Cyber Security Angriff (DDoS)

Konsequenzen für ein Unternehmen?

- Finanzieller Schaden
- Managementkapazität
- Reputationsverlust
- Forderungen
- Sanktionen (?)

Einige Quellen

- MELANI

https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte.html

- FEDPOL

https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/cybercrime.html

Rechtlicher Rahmen - Überblick

- Internationales Recht:
  - Übereinkommen über Cyberkriminalität
  - Cloud-Act
- Nationale Gesetze
  - Schweizerisches Strafgesetzbuch, StGB
  - Schweizerisches Datenschutzgesetz DSG
  - Corporate Governance: Schweizerisches Obligationenrecht (716a OR)
  - Verordnung über die Aufbewahrung von Unternehmensbüchern (Aufbewahrung), Verordnung über Internet-Domains (VID), Finanzmarktauf-sichtsgesetz (FINMAG), etc.
- Gesetzgebungsentwicklungen Bundesrat und Bundesämter
  - NCS Strategie Cyberrisiken 2018-2022
  - Strategie Digitale Schweiz

Rechtlicher Rahmen – Strafrecht I

- Strafrecht (Schweizerisches Strafgesetzbuch, StGB)
  - Unbefugte Datenbeschaffung: Art. 143 StGB (elektronischer Diebstahl)
  - Unbefugtes Eindringen in ein Datenverarbeitungssystem: Art. 143bis StGB (Hacking)
  - Datenbeschädigung: Art. 144bis StGB (Denial-of-Service-Angriffe; Ransomeware)
  - Betrügerischer Missbrauch einer Datenverarbeitungsanlage: Art. 147 StGB (Computerbetrug)
  - Verletzung des Geheim- oder Privatbereichs durch Aufnahmegeräte: Art. 179^{quater} StGB
  - Unbefugtes Beschaffen von Personendaten: Art. 179^{novies} StGB
  - Wirtschaftlicher Nachrichtendienst (Art. 273 StGB)
  - Verletzung des Post- und Fernmeldegeheimnisses (Art. 321ter StGB)

Rechtlicher Rahmen - Strafrecht II

- Strafrecht - Zusammenhang mit anderen Straftaten
  - Betrug (Art. 146 StGB)
  - Erpressung (Art. 156 StGB)
  - Strafbare Handlungen gegen die Ehre und den Geheim- oder Privatbereich (Art. 173 ff. StGB)
  - Urkundenfälschung (Art. 251 ff. StGB) (Phishing)
  - Verantwortlichkeit/Strafbarkeit des Unternehmens (Art. 102 StGB)

Massnahmen vor, während und nach einem Vorfall

- Massnahmen vor dem Vorfall
- Massnahmen während oder unmittelbar nach einem Vorfall
- Massnahmen nach Vorfällen / Durchsetzung

Vorbeugende Massnahmen

- Technische und organisatorische Massnahmen (Art. 7 DSG / Art. 8 und 9 VDSG)
  - Technische Massnahmen (Authorisation/ Zugang; Übermittlung; Backup)
  - Umsetzung organisatorischer Massnahmen (IT-Sicherheitsrichtlinien; IT-Sicherheitsrichtlinien für Mitarbeiter; Datenschutzrichtlinien; Aufbewahrungsrichtlinien; Sensibilisierung & Training)
  - Einrichtung einer Task Force / Beauftragung externer Dienstleister
- Begrenzung der Haftungsrisiken gegenüber Dritten (vertragliche Massnahmen)
- Cyber Security Versicherung
- ISO-Zertifizierung

Massnahmen während oder unmittelbar nach dem Vorfall

→ Unbefugter Zugriff auf die Unternehmensdaten

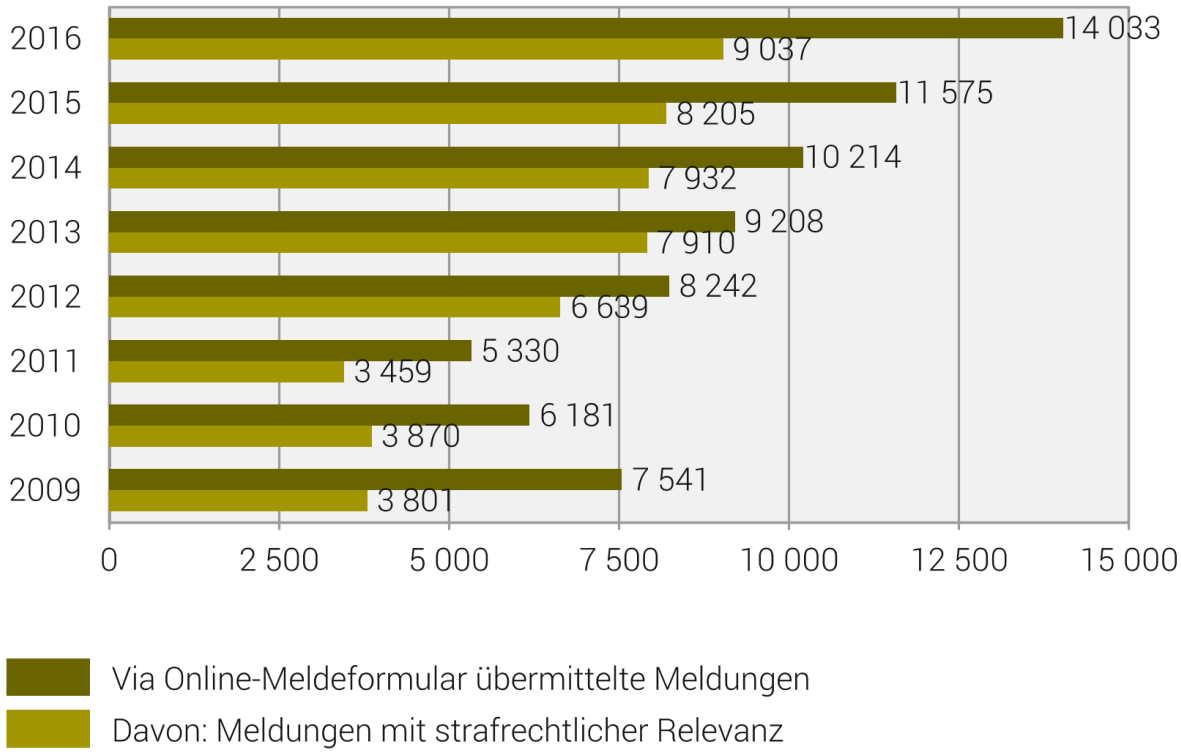
– Identifizieren und Analysieren	dringend
– Stoppen / Eindämmen	dringend
– Wiederherstellen	dringend
– Benachrichtigung der Datenschutzbehörden	dringend
– Benachrichtigung der Cyber Security-Versicherung	dringend
– Überprüfung / Behebung	nicht vergessen

Massnahmen nach einem Vorfall - Benachrichtigungen

- Meldung an MELANI
- Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)
- Benachrichtigung der betroffenen Personen
- Dritte benachrichtigen

Entwicklung der Cyberkriminalität

Anzahl an fedpol übermittelte Meldungen einschliesslich jener mit strafrechtlicher Relevanz, 2009-2016



Quelle: jahresbericht fedpol

Massnahmen nach einem Vorfall - Vollstreckung

- Durchsetzung
  - Strafanzeige
  - Zivilprozessrechtliche Massnahmen (Geltendmachung eines Anspruchs, Beantragung von vorsorglichen Massnahmen)
- Praktische Probleme
  - Offizial- vs. Antragsdelikte
  - Identifizierung des Täters
  - Gerichtsstand
  - Zusammenarbeit bei der internationalen Strafverfolgung

Haftung I

- Haftung der Vorstandsmitglieder
  - Die Vorstandsmitglieder haften für Schäden, die durch vorsätzliche oder fahrlässige Pflichtverletzungen verursacht werden.
  - Gesamthaftung, jedoch abhängig vom Grad der Fahrlässigkeit
  - Wer kann klagen (wann)
    - Gesellschafter (Unternehmensfortführung)
    - Gläubiger (in Konkurs)
    - Unternehmen (Going Concern)
- Exkurs:
  - Haftpflichtversicherung für Organmitglieder
  - Cybersicherheit Versicherung

Haftung II

- Das Vorstandsmitglied haftet, wenn folgende Voraussetzungen erfüllt sind:
  - Position und Tätigkeit als Vorstandsmitglied
  - Pflichtverletzung
  - Fahrlässiges oder vorsätzliches Verhalten
  - Schäden
  - Keine Exkulpation und Kausalität
  - Recht zur Geltendmachung von Haftungsansprüchen
  - Beweislast

Beratungsbedarf in der Praxis

- Reglemente:
  - IT Reglemente
  - TOS
  - E-Mail und Internetüberwachung
  - Datenschutzerklärungen
- Beratung bei Haftungsfragen
- Unterstützung bei der Notifikation von Data Breaches
- Unterstützung bei der Einreichung von Strafanzeigen und Klagen
- Unterstützung bei einem Data Breach und den «Aufräumarbeiten»

Fälle aus der Praxis

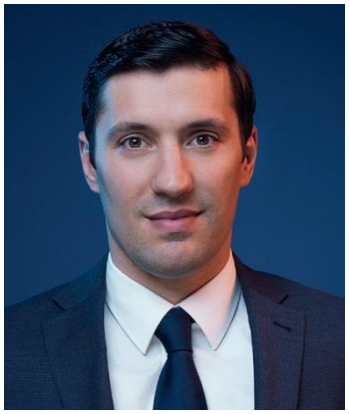
- Datendiebstahl durch einen Mitarbeiter
- Hacking: Kreditkartendaten von 1000 Kunden
- Hacking: Verbreitung von Gesundheitsdaten im Internet
- Angedrohte DDos Attacke bei einer Privatbank
- Spoofing: E-Mailaustausch mit falscher E-Mailadresse
- Identitätsdiebstahl: fremde Firma wird missbraucht für das Fundraising bei einem ICO

Fragen?

THANK YOU

Your Contacts

Clara-Ann Gordon
clara-ann.gordon@nkf.ch
D +41 58 800 84 26



Victor Stancescu
victor.stancescu@nkf.ch
D +41 58 800 82 29

Niederer Kraft Frey Ltd Bahnhofstrasse 53 CH-8001 Zurich T +41 58 800 80 00 F +41 58 800 80 80 nkf.ch