Haftung für Cybersicherheitsvorfälle

Nationale Initiative für Internet- und Informations-Sicherheit

10.10.2019 – IT SA Nürnberg

Themen

- Arbeit von NIFIS e. V.
- Daten- und Informationssicherheit in Deutschland
- Verbindung von IT-Anwendern und Anbietern von IT-Sicherheit
- Fragebogen zur IT-Sicherheit in Deutschland

Cybersicherheitsvorfälle

Es kann jeden treffen – schneller als gedacht – und dann:

- Wer den Schaden hat, kann oft nicht den Verursacher finden
- Nicht selten sind die Täter im Ausland schwer greifbar
- Manchmal hat man durch Unachtsamkeit zudem noch anderen Schaden zugefügt, etwa dem Arbeitgeber, Vertrags- oder Kommunikationspartnern

Unbekannte Täter

- Angriffe auf Informationstechnologie erfolgen heute regelmäßigen Formen organisierter Kriminalität
  - International
  - Arbeitsteilig
  - Professionell

Verursacher im Ausland

- Internationale Rechtsverfolgung
  - durchaus möglich, insbesondere in Europa
  - aufwendig und teuer
  - langwierig
- Sonderproblem Vollstreckung in- und ausländischer Urteile

Verursacher im Inland

- Problem des Nachweises
- Auswahl des „richtigen“ Ersatzpflichtigen
- Gegebenenfalls sogenannte *Streitverkündung*
  - Verhindert, dass im Prozeß gg. einen möglichen Ersatzpflichtigen der Nachweis nicht gelingt, weil vielleicht ein anderer verantwortlich ist und umgekehrt – Ergebnis des ersten Streits gilt auch gegen den anderen

Rechtsgrundlagen

- Vertragliche Haftung
  - Kaufvertrag, Mietvertrag, Werkvertrag, Dienstvertrag
  - Kauf/Miete/Erstellung/Anpassung von Software, Cloud Computing etc.
- Gesetzliche Haftung
  - Verletzung von Eigentum (Eigentum an Daten?)
  - Vermögensschäden bei sogenannten Schutzgesetzen
  - Haftung für Dritte - Exkulpation

Mögliche Schäden

- Betriebsunterbrechung, Betriebsausfall
  - Haftung für Verzug, Vertragsstrafen
  - Umsatzausfälle
- Reputationsschaden
- Verlust von Daten, Kosten für Wiederherstellung
- Gewährleistung
- Etc.

Bsp. Ransomware (Emotet etc.)

- Verbreitung insbesondere durch sogenanntes „Outlook-Harvesting“, das heißt durch
  - Erzeugen authentisch wirkender Spam-Mails
  - anhand ausgelesener E-Mail-Inhalte und
  - Kontaktdaten

Gegenmaßnahmen

- **Maßnahmen** in Unternehmen zu ergreifen
  - Einspielen aktueller Sicherheitsupdates
  - Funktionierendes Back-up System – regelmäßige Kontrollen
  - Gruppenrichtlinien gegen Ausführung von Makros
  - Schulung und Sensibilisierung der Mitarbeiter
  - Einsatz von Passwortmanagern

Verhalten der Mitarbeiter

- Sensibilität bei unerwarteten E-Mails
- Vorsicht beim Öffnen von Anhängen – gegebenenfalls Word-Dateien in Libre Office öffnen
- Ausreichend sichere Passwörter
- Ausreden
  - Fehlende Schulung, fehlende Sensibilisierung
  - keine ausreichenden Vorkehrungen der Unternehmen

Beteiligte/Geschädigte

Haftung für eingetretene Schäden

- Unternehmen haften
  - Gegenüber ihren Kunden vertraglich
  - Gegenüber Dritten aufgrund gesetzlicher Haftung
- Erforderlich ist Kausalität – der eingetretene Schaden muss durch das Unternehmen verursacht sein
- Verschulden (Vorsatz oder Fahrlässigkeit)

Verschulden

- Vorsatz
  - Direkter Vorsatz: ich will etwas erreichen und handle
  - Eventuell Vorsatz: Ich will den Schaden nicht verursachen, ich weiß, dass das Risiko besteht und handele trotzdem bzw. unternehme nichts dagegen (obwohl ich dazu verpflichtet bin)

Grobe Fahrlässigkeit

- Die erforderliche Sorgfalt wird in besonders grober Weise verletzt –
  - Passwort: 12345, Passwort etc.
  - Verstoß gegen Vorgaben im Unternehmen
  - Einrichten von Diensten nebenbei während anderen Telefonat, unter Alkohol etc.

Fahrlässigkeit

- Leichte Fahrlässigkeit
  - Verletzung von Sorgfaltspflichten durch Flüchtigkeitsfehler – bei normalen Arbeitnehmern Haftungsausschluss gegenüber Arbeitgeber
- Mittlere Fahrlässigkeit
  - Grauzone – führt bei Arbeitnehmern zur anteiliger Haftung

Verantwortliche Personen

- Compliance Officer, IT-Sicherheitsbeauftragte, ähnliche Positionen: erhöhte Verpflichtungen der Mitarbeiter
- Mitarbeiter sind in D&O-Versicherung aufzunehmen
- MA müssen ihre getroffenen und insbesondere vorgeschlagenen Maßnahmen dokumentieren, gegebenenfalls eskalieren

Mitverschulden

- Hat der Geschädigte seinerseits die erforderlichen Maßnahmen unterlassen oder unvorsichtig gehandelt, ist Mitverschulden gegeben
  - Schaden ist anteilig nach dem Maß der jeweiligen Verantwortung zu tragen oder
  - Schadensersatz kann komplett ausgeschlossen sein

Vorsorge durch Rechtsgestaltung

- Haftungsausschluss durch Allgemeine Geschäftsbedingungen
- Haftungsbegrenzung durch Rechtsform (GmbH, UG etc.)
- Wirksamkeit ist fraglich, da Klauselkontrolle und Durchgriifshaftung entgegenstehen können

Versicherungen

- Cyberversicherung
- Haftpflichtversicherung, allgemeine Rechtsschutzversicherung
- D&O-Versicherungen

- Ersetzen nicht die ausreichende Vorsorge
- Setzen einige Obliegenheitspflichten
- Können im Einzelfall Rückgriff nehmen, insbesondere bei grob fahrlässigem Verhalten

Andere Szenarien

- Vertrieb von Software mit Schadcode
  - Vertriebsstufen mit unterschiedlicher Verantwortung
- Installation von Updates
  - Frage der Prüfpflicht für Updates
- Infizierte Webseiten
- DDOS-Angriffe, Trojaner etc.

IT-Kanzlei dr-lapp.de

- Dr. Thomas Lapp
  Rechtsanwalt und zertifizierter Mediator,
  Fachanwalt für IT-Recht, Datenschutzbeauftragter

- Corinna Lapp
  Rechtsanwältin und Mediatorin,
  Fachanwältin für IT-Recht

Berkersheimer Bahnstraße 5, 60435 Frankfurt am Main

Tel.: 069/9540 8865

anwalt@dr-lapp.de - www.dr-lapp.de

Datenschutz dr-lapp.de

NIFIS e. V.

- **Nationale Initiative für Informations- und Internetsicherheit e. V.**
- **Dr. Thomas Lapp -** Vorsitzender der NIFIS
  Rechtsanwalt und zertifizierter Mediator
  Fachanwalt für Informationstechnologierecht
- Berkersheimer Bahnstraße 5
  60435 Frankfurt am Main
  Tel.: +49 69 2444 4757
  Mobil: +49 700 RA DR Lapp (=+49 700 72 37 5277)
  www.nifis.de - thomas.lapp@nifis.de - http://twitter.com/NIFIS

Vielen Dank für Ihre Aufmerksamkeit!

Weitere Informationen unter www.nifis.de