Schaden und Haftung bei IT-Sicherheitsvorfällen

IT Security Talks 2024
17.4.2024

Dr. Thomas Lapp, Frankfurt am Main

Rechtsanwalt und zertifizierter QVM-Mediator,
Fachanwalt für Informationstechnologierecht

Datenschutz
dr-lapp.de

IT-Kanzlei
dr-lapp.de

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 nicht nur sich selbst, sondern auch noch anderen Schaden zugefügt, etwa dem **Arbeitgeber**, **Vertrags-** oder **Kommunikationspartnern**

Unbekannte Täter

- Angriffe auf Informationstechnologie erfolgen heute regelmäßigen Formen organisierter Kriminalität
  - international
  - arbeitsteilig
  - professionell
  - mit Unterstützung von KI

Verursacher im Ausland

- Internationale Rechtsverfolgung
  - durchaus möglich (insbesondere in Europa)
  - aufwendig und teuer
  - langwierig
- Vollstreckung in- und ausländischer Urteile im Ausland stellt ein weiteres Problem dar

Mögliche Schäden

- Betriebsunterbrechung, Betriebsausfall: Haftung für
  - Verzugsschaden und Vertragsstrafen
  - Umsatzausfälle
- Reputationsschaden
- Verlust von Daten, Kosten für Wiederherstellung
- Gewährleistung
- etc.

Bsp. Ransomware (Emotet etc.)

- Ransomware ist nach wie vor Hauptbedrohung (vgl. BSI Bericht zur Lage der IT-Sicherheit in Deutschland 2023)
- wird durch die Angreifer fortlaufend weiterentwickelt
- Werkzeuge für jeden Schritt eines komplexen Angriffs können Angreifer als Dienstleistung einkaufen
- Angreifer gehen zunehmend den Weg des geringsten Widerstands → kleine und mittlere Unternehmen etc.

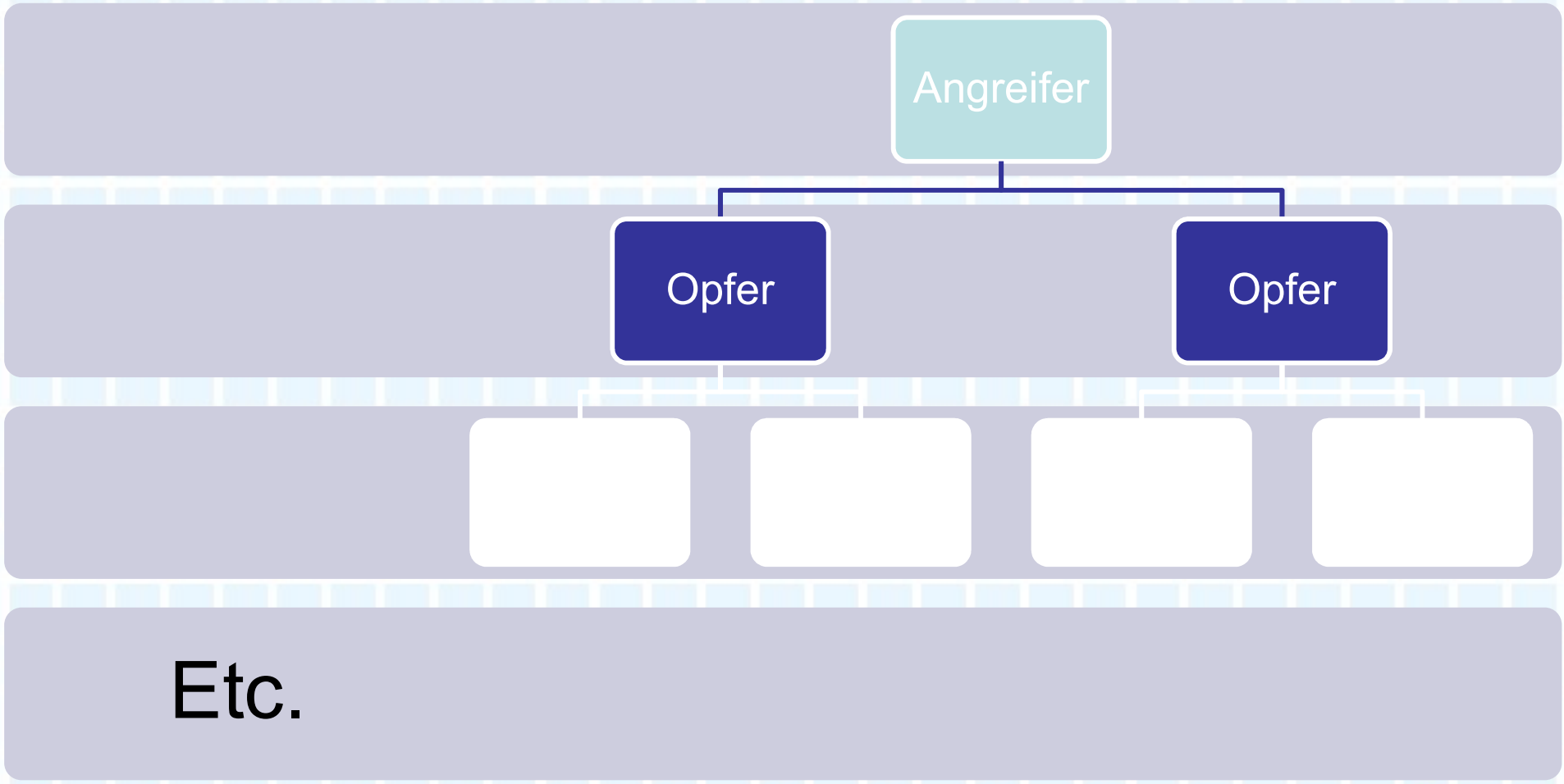
Bsp. Ransomware (Emotet etc.)

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

Verursacher im Inland

- Problem des Nachweises
- Auswahl des „richtigen“ Ersatzpflichtigen
- Wer hat den Schaden verursacht?

Verursacher



Rechtsgrundlage vertragliche Haftung

- Kaufvertrag, Mietvertrag, Werkvertrag, Dienstvertrag
- Kauf/Miete/Erstellung/Anpassung von Software, Cloud Computing etc.
- Vertragliche Nebenpflicht, die Rechte und Rechtsgüter des Vertragspartners zu schützen und die erforderliche Sorgfalt walten zu lassen – § 241 Abs. 2 BGB
- Haftung für alle im Rahmen des Vertrages eingesetzten Personen

Rechtsgrundlage: gesetzliche Haftung

- Verletzung von Eigentum (Eigentum an Daten?)
- Vermögensschäden bei Schutzgesetzen, § 823 Abs. 2 BGB
- Haftung für Mitarbeitende
- Haftung für Dritte – Exkulpation möglich, wenn sorgfältig ausgewählt und für Beschaffung von Soft-/Hardware und zur Leitung erforderliche Sorgfalt beobachtet wurde

Sorgfalt: 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

Sensibilisierung der Mitarbeitenden

- Sensibilität bei unerwarteten E-Mails
- Vorsicht beim Öffnen von Anhängen – gegebenenfalls Word-Dateien in Libre Office öffnen
- Ausreichend sichere Passwörter

– Keine 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)

Haftung der Arbeitnehmer

Leichte Fahrlässigkeit

- Keine Haftung der Arbeitnehmer

Mittlere Fahrlässigkeit

- Anteilige Haftung

Grobe Fahrlässigkeit, Vorsatz

- Arbeitnehmer haftet mit Privatvermögen

Verschulden

- Vorsatz
  - Direkter Vorsatz: ich will etwas erreichen und handle
  - Eventualvorsatz: 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, Beispiele:
  - Passwort: 12345, Passwort etc.
  - Verstoß gegen Vorgaben im Unternehmen
  - Einrichten von Diensten nebenbei während anderen Telefonat, unter Alkohol etc.
  - IT-Sicherheitsstandards werden nicht umgesetzt

Fahrlässigkeit

- Leichte Fahrlässigkeit
  - Verletzung von Sorgfaltspflichten durch

    Flüchtigkeitsfehler – bei normalen Arbeitnehmern

    Haftungsausschluss gegenüber Arbeitgeber
- Mittlere Fahrlässigkeit
  - Grauzone – führt bei Arbeitnehmern zur anteiligen

    Haftung für angerichtete Schäden

Stand der Technik

- Welche Sorgfaltspflichten bestehen, ist im Rahmen einer Risikoanalyse unter Berücksichtigung des Stands der Technik zu prüfen – 3-Stufen:
  - anerkannte Regeln der Technik
  - Stand der Technik
  - Stand von Wissenschaft und Forschung

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

  ➢ Durchgriffshaftung 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.

Aktuell Kapeka

- Schadsoftware, die virtuelle Hintertüren in Windows-Systemen einbaut und diese für Cyber-Angriffe verwundbar macht
- Microsoft „KnuckleTouch“ ist maßgeschneidertes Tool
- Microsoft entwickelt Abwehr
- Patch muss unverzüglich eingespielt werden, um die Bedrohung abzuwehren bzw. zu beenden

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

IT-Kanzlei dr-lapp.de