

Cybersicherheitsvorfälle – Zivilrechtliche Haftung

Lawyer meets IT: it-sa insights
Nürnberg, 09.10.2019

Dr. Thomas Lapp, Frankfurt am Main

Rechtsanwalt und zertifizierter Mediator, Fachanwalt für
Informationstechnologierecht

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

Verursacher im Inland

- Problem des Nachweises
- Auswahl des „richtigen“ Ersatzpflichtigen
- Gegebenenfalls sogenannte Streitverkündung

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

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

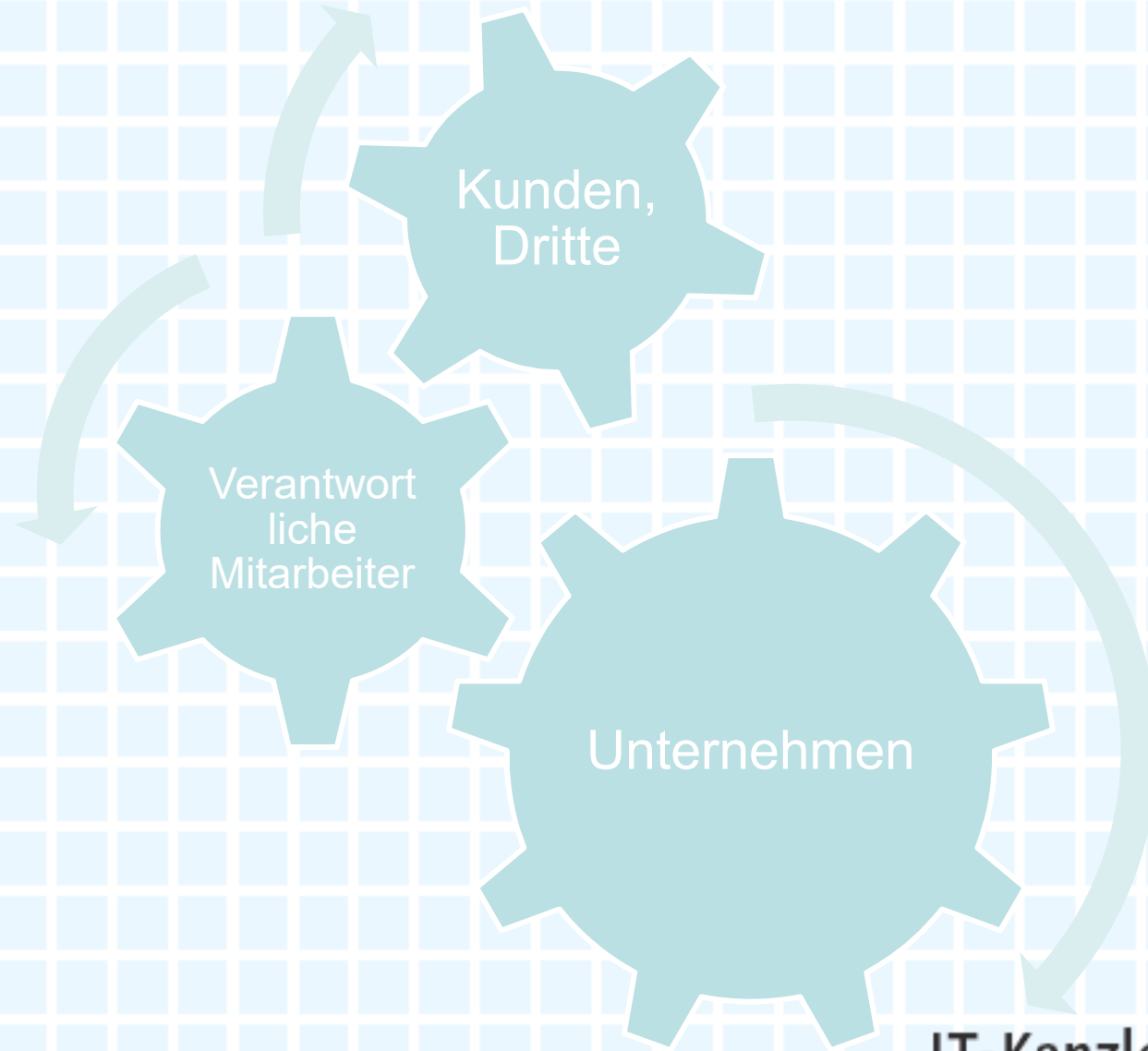
Gegenmaßnahmen

- Maßnahmen in Unternehmen
 - 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

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



Mitverschulden

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

Vorsorge durch Rechtsgestaltung

- Haftungsausschluss durch Allgemeine Geschäftsbedingungen
- Haftungsbegrenzung durch Rechtsform (GmbH, UG etc.)
 - Wirksamkeit ist fraglich

Versicherungen

- Cyberversicherung
- Haftpflichtversicherung
- D&O-Versicherungen
- Ersetzen keine ausreichende Vorsorge
- Setzen einige Obliegenheitspflichten
- Können im Einzelfall Rückgriff nehmen



Andere Szenarien

- Vertrieb von Software mit Schadcode
- Installation von 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
Tel.: 069/9540 8865
anwalt@dr-lapp.de
www.dr-lapp.de