

## Rechtliche Folgen bei Angriffen

# IoT – Security by Default and Design?

Das «Internet der Fühler» durchdringt zunehmend industrielle Prozesse bis in die äusseren Kapillaren und wird auch in Zukunft das Leben in der Informationsgesellschaft prägen. Aber: Flächendeckende Vernetzung heisst auch flächenweite Angriffsvektoren. Dies hat auch rechtliche Konsequenzen.

→ MARK SCHIEWECK & ALEXANDER HOFMANN, LAUX LAWYERS

Cyberattacken haben in den letzten Jahren genauso zugenommen wie die Menge der in unserem Umfeld eingesetzten vernetzten Geräte und Sensoren. Gerätschaften, die gestern noch offline ohne jede Anbindung funktioniert haben, sind in der neuen Welt des IoT ein Ziel für Hacker geworden und dienen als Eingangstore zu den gesamten «E-cosystemen», deren Teil sie sind. Die Folgen von Sicherheitsmängeln solcher Produkte können eine ernste Gefahr darstellen, sogar für Leib und Leben. Cyber Risiken sind immer auch rechtliche Risiken und die Frage ist, welches Mass an Cybersicherheit aus rechtlicher Sicht verlangt ist, um den neuen Bedrohungen zu begegnen.

Das Recht dient u. a. dem Schutz von Rechtsgütern vor negativen Beeinträchtigungen – solche Rechtsgüter können etwa sein: die Privat- und Geheimsphäre, die Persönlichkeit, die körperliche und geistige Unversehrtheit, das Eigentum, aber auch staatliche Geheimnisse oder das Funktionieren staatlicher Institutionen an sich. Das Grundprinzip, welches viele Schutznormen verfolgt, lässt sich in der Essenz auf den dem Haftpflichtrecht entlehnten sogenannten «Gefahrensatz» zurückführen: Wer eine Gefahr für schützenswerte Rechtsgüter schafft oder unterhält, hat die zur Vermeidung von Schaden notwendigen Massnahmen zu treffen.

Es gibt heute erst relativ wenige Kodifikationen, die sich auch nur indirekt mit Cybersicherheit befassen. In vielen privatrechtlichen Gesetzen wie zum Beispiel dem Haftpflicht- und Produkthaftpflichtrecht fehlen spezifische Regelungen und Anforderungen. Anstehender Revisionsbedarf wird aber im Hinblick auf den Einsatz von Robotern und künstlicher Intelligenz schon heute diskutiert.

Anhand einiger moderner Kodifikationen, wie zum Beispiel der im Juni 2019 in Kraft getretenen Cybersecurity-Richtlinie der EU, der EU-Datenschutz-Grundverordnung (DSGVO), dem deutschen IT-Sicherheitsgesetz oder auch dem US IoT Cybersecurity Improvement Act 2017, lässt sich ein interessanter gemeinsamer Trend ausmachen: Sie propagieren einen risikobasierten Ansatz nach dem Credo «Security by Default and Design». Dieses Prinzip unterscheidet sich im Grunde nur wenig vom altbekannten und etablierten «Gefahrensatz» und es ist deshalb denkbar, dass

sich «Security by Default and Design» zu einer allgemeinen rechtlichen Leitlinie mausern kann. Unternehmen sind bei der Entwicklung vernetzter Produkte und Systeme jedenfalls schon heute gut beraten, wenn sie in der Frühphase des Entwicklungszyklus im Zuge eines «Security Breach Impact Assessment» produktinhärente Sicherheitsrisiken zu identifizieren versuchen, um diese von allem Anfang an durch geeignete technische und organisatorische Sicherheitsmassregeln risikogerecht zu adressieren.

## «Cyber Risiken sind immer auch rechtliche Risiken»

Alexander Hofmann

Von Beginn weg durchdachte, risikoadäquate, sich stetig der Bedrohungslage anpassende und vom Anwender in der Praxis auch nutzbare Cybersicherheit wird fraglos ihr Preisgeld tragen. Einiges erheblicher dürften demgegenüber die Folgekosten im Hinblick auf Security Breaches zu Buche schlagen. Die Aufwendungen für deren sachgerechte Aufarbeitung fallen dabei schlimmstenfalls nicht einmal so sehr ins Gewicht wie allfällige Schadensersatzforderungen, die sich vor allem im Konsumentenbereich, vorgängig meist nur beschränkt, rechtlich einschränken oder wegbedingen lassen. Unternehmen verbleibt zwar die Möglichkeit, Restrisiken im Bereich Cybersicherheit versichern zu lassen – aber auch dies schlägt sich in höheren Kosten nieder.

Kurzum: Die Herstellung und Aufrechterhaltung adäquater Cybersicherheit ist im Zuge der Entwicklung vernetzter Produkte aus einer rechtlichen Optik unbedingt zu berücksichtigen. Die Sicherheit vernetzter Produkte ist aber auch ein Kostenfaktor, der in jedem IoT Business Case sorgfältige Beachtung finden muss. ←



### DIE AUTOREN

**Alexander Hofmann,**  
**Mark Schieweck**

Rechtsanwalt Alexander Hofmann ist Mitglied der swissICT-Rechtskommission und Partner bei Laux Lawyers. Marc Schieweck ist ebenfalls Rechtsanwalt und Partner bei Laux Lawyers, einer auf IT-Recht spezialisierten Kanzlei. Die Rechtskommission von swissICT berichtet in der Kolumne «Recht & IT» über aktuelle juristische Themen im digitalen Bereich.

→ [www.swissict.ch/recht](http://www.swissict.ch/recht)