Diskussion zum Begriff „Stand der Technik“

Lenkungskreis Informationssicherheit

Frankfurt am Main

21.09.2017

Dr. Dennis-Kenji Kipker
IGMR
Universität Bremen

Gefördert vom
FKZ: 16KIS0213
bis 16KIS0216
Bundesministerium für Bildung und Forschung

Universität der Bundeswehr München

FAU Friedrich-Alexander Universität Erlangen-Nürnberg

DKE VDE DIN

Universität Bremen

- Erkenntnisquellen für die IT-Security Compliance – “von A bis Z”:
  - AktG, § 91
  - AtG, §§ 7 ff., 44b
  - BDSG, §§ 9, 9a, 11, 42a
  - BSIG, §§ 3, 4, 7, 7a, 8a ff.
  - EnWG, §§ 11 ff., 21e, 49
  - GmbHG, § 43
  - KWG, § 25a
  - TKG, §§ 109, 109a
  - TMG, § 13
  - VAG, § 64a
  - WpHG, § 33
  - …
  - **IT-SiG (2015), EU NIS-RL (2016) + nationales Umsetzungsgesetz (2017)**

- § 8a BSIG – Sicherheit in der Informationstechnik Kritischer Infrastrukturen:

  (1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 **angemessene organisatorische und technische Vorkehrungen** zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der **Stand der Technik** eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

- Gesetzliche Verwendung „unbestimmter Rechtsbegriffe“:
  - Gesetzgebungswerkzeug: **Normkonkretisierende gleitende Verweisung**
  - **Drei wesentliche Kategorien** von unbestimmten Rechtsbegriffen in der gesetzgeberischen Verwendung:
    - Allgemein anerkannte Regeln der Technik
    - Stand der Technik
    - Stand von Wissenschaft und Technik
  - Konkretisiert durch **BMJV: Handbuch der Rechtsförmlichkeit**

Unbestimmte Rechtsbegriffe und deren Konkretisierung

- Drei-Stufen-Theorie (BVerfG, Beschluss vom 08.08.1978, 2 BvL 8/77):
  - Ermöglicht bessere **Abgrenzung** zwischen vorgenannten drei unbestimmten Rechtsbegriffen
  - Je weiter eine bestimmte technische Vorgehensweise oder Methode in der Praxis etabliert und allgemein anerkannt ist, umso eher wird von einer **allgemein anerkannten Regel der Technik** auszugehen sein
    - Folglich immer dann einschlägig, wenn eine Maßnahme der **Mehrheitsauffassung** aller Praktiker entspricht
  - Gegensatz dazu: **Stand von Wissenschaft und Technik**
    - Vornehmlich solche Methoden, die nur dem aktuellsten technischen Erkenntnisstand entsprechen und sich folglich in der Praxis **noch nicht durchgesetzt** haben
  - **Stand der Technik** als Mittelmaß
    - Solche Vorkehrungen, die zwar noch **nicht unbedingt bei jedem Fachmann** oder Anwender angelangt sein müssen, aber zugleich auch nicht so neu sind, dass sie die Grenze des wissenschaftlich bzw. technisch Realisierbaren bedeuten

- Auslegungsansätze zur Ermittlung des technischen Sinngehaltes unbestimmter Rechtsbegriffe:
  - **„Stand der Technik“** oftmals alleiniger und damit entscheidungserheblicher Faktor
  - **Zwar juristisch definier-, aber nicht konkretisierbar!**

- **Konkretisierungsvorschläge zum „Stand der Technik“:**
  - Normung und Standardisierung, z.B.:
    - DIN EN ISO/IEC 27001:2017-06
    - DIN EN ISO/IEC 27002:2017-06
    - DIN EN ISO/IEC 27040:2016
    - DIN EN ISO/IEC 27041:2016-12
    - DIN EN 61918-3 (VDE 0800-500):2017-02
  - BSI-Veröffentlichungen zur Cybersicherheit, Diskussionspapiere
  - TeleTrusT-Handreichung zum „Stand der Technik“ im Sinne des IT-SiG
  - B3S, z.B. für Wasser/Abwasser
  - Spezialfälle: Z.B. Sicherheitskataloge BNetzA, MaRisk
  - Reifegradmodelle, z.B. über SPICE (vgl. Kipker/Pfeil, DuD 2016, 810 ff.)
  - Fachpublikationen
  - Mailinglists
  - Was leisten andere Unternehmen in vergleichbaren Sektoren/Branchen?
  - Gerichte/Grundsatzentscheidungen für IT-Sicherheit

- **Aber ist das schon alles?!**
- → Blick auf IT-Sicherheit vornehmlich **durch KRITIS geprägt**, Diskussion hierauf fokussiert
- Welche Anforderungen gelten z.B. für **KMU im Nicht-KRITIS-Bereich**?
  - Institut für Mittelstandsforschung IfM Bonn, Jahresstatistik: Deutsche KMUs steuerten 2014 rund 55% zur gesamten Nettowertschöpfung deutscher Unternehmen bei

- §§ 91 Abs. 2, 93 Abs. 1 AktG – Organisation, Sorgfaltspflicht und Verantwortlichkeit der Vorstandsmitglieder:
  - Der Vorstand hat geeignete Maßnahmen zu treffen, damit „**den Fortbestand der Gesellschaft gefährdende Entwicklungen**“ frühzeitig erkannt werden
  - Die Vorstandsmitglieder haben bei ihrer Geschäftsführung „**die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters**“ anzuwenden

  → **„Stand der Technik“? KRITIS?**

- § 43 GmbHG – Haftung der Geschäftsführer:

  (1) Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft **die Sorgfalt eines ordentlichen Geschäftsmannes** anzuwenden.

  (2) Geschäftsführer, welche ihre **Obliegenheiten verletzen, haften** der Gesellschaft solidarisch für den entstandenen Schaden.

→ „Stand der Technik“? KRITIS?

- IGMR, juristisches Gutachten von September 2017:
  - **§ 91 II AktG** verpflichtet den Vorstand einer Aktiengesellschaft zur Einrichtung eines Systems, dass bestandsgefährdende Risiken frühzeitig erkennen kann. Darunter fällt auch die **Abwehr IT-spezifischer Risiken**.
  - Dies gilt grundsätzlich gem. **§ 43 I GmbHG analog** für den Geschäftsführer einer Gesellschaft mit beschränkter Haftung. Der Umfang des Risikomanagements bemisst sich dabei an der Größe der Gesellschaft.

Unbestimmte Rechtsbegriffe und deren Konkretisierung

- Auf den juristischen Blickwinkel kommt es an:
  - Juristische **„Rahmenvorschriften“** eröffnen IT-Sicherheitsverpflichtungen für theoretisch nahezu **alle Wirtschaftsbereiche** und **alle Unternehmensgrößen**
  - Wo die **Konkretisierung** unbestimmter Rechtsbegriffe für KRITIS noch unzureichend ist, **fehlt** sie in diesem Segment nahezu völlig
  - Gleichwohl **erhebliche (wirtschaftliche) Relevanz**, s.o.
  - Konkretisierung durch Gerichte? Jedenfalls für den Regelfall nicht zumutbar!
  - Wie können **KMU** flächendeckend bei der Bestimmung des für sie notwendigen Security-Ansatzes unterstützt werden?
  - **Forschungsansatz: Automatisierte, algorithmenbasierte Bestimmung** des angemessen Technikmaßstabes für die IT-Security: Auf welche technischen Standards wird beispielsweise in besonderem Maße referenziert?
    - → Kann ggf. auch für den Bereich KRITIS fruchtbar gemacht werden

Dr. Dennis-Kenji Kipker
Wissenschaftlicher Geschäftsführer
Institut für Informations-, Gesundheits- und Medizinrecht (IGMR)
Universität Bremen
Universitätsallee GW1
28359 Bremen
Tel.: 0421 218 66049
Mail: kipker@uni-bremen.de

Besuchen Sie unsere Website: www.itskritis.de
Folgen Sie uns auf Twitter: @itskritis

Universität der Bundeswehr München
FAU Friedrich-Alexander Universität Erlangen-Nürnberg
DKE VDE DIN
Universität Bremen