Die IT-Security Landscape als Lösungsmodell praxisnaher Gesetzeskonkretisierung für KMUs im Bereich von KRITIS

Arbeitspapier im Rahmen des Forschungsprojekts
„Vernetzte IT-Sicherheit Kritischer Infrastrukturen“ (VeSiKi)
im BMBF-Förderschwerpunkt
„IT-Sicherheit für Kritische Infrastrukturen“

Stand: 15.08.2016

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Ansprechpartner Recht:

Dr. Dennis-Kenji Kipker

Institut für Informations-, Gesundheits- und Medizinrecht (IGMR)

Universität Bremen

Universitätsallee GW1

28359 Bremen

Tel.: 0421 218 66049

Mail: kipker@uni-bremen.de

Ansprechpartnerin Technik:

Sophia Harth

VDE e.V., Bereich DKE

Normung und Standardisierung

Stresemannallee 15

60596 Frankfurt am Main

Tel.: 069 6308 395

Mail: sophia.harth@vde.com

Gliederung

Abstract

Der folgende Beitrag befasst sich mit der Entwicklung einer interdisziplinären IT-Security Landscape, die sowohl die aktuellen rechtlichen wie auch die technischen Anforderungen an sichere IT-Systeme anwender- und praxisgerecht aufbereitet und als frei verfügbares Online-Tool miteinander verknüpft. Hierdurch soll insbesondere den IT-Sicherheitsbeauftragten in als KRITIS klassifizierten KMUs, denen oftmals die entsprechenden juristischen und technischen Ressourcen fehlen, eine effiziente Orientierungs- und Entscheidungshilfe an die Hand gegeben werden, um die IT-Sicherheit flächendeckend zu verbessern.

I. Transparenz und Anwenderverständlichkeit als Grundvoraussetzung guter Gesetze

Vorrangigstes Ziel eines jeden guten Gesetzes ist für den Anwender Verständlichkeit. Gerade in Arbeitsbereichen, in denen nicht nur ausgebildete Juristen mit rechtlichen Vorschriften konfrontiert werden, hat diese Vorgabe hohe Relevanz. Noch schwerer wiegt es, wenn die entsprechenden gesetzlichen Vorschriften Verpflichtungen bestimmen, die bei Nichteinhaltung haftungs- und bußgeldbewehrt sein können.

Gerade für den IT-Sicherheitsbereich stellen sich die vorgenannten Probleme der Verständlichkeit und Haftungsrelevanz von Rechtsvorschriften in besonderem Maße – und dies nicht erst seit Inkrafttreten des IT-Sicherheitsgesetzes im vergangenen Jahr, wo erstmals gezielt neue technische und organisatorische Anforderungen für die Betreiber von Kritischen Infrastrukturen bestimmt wurden. Ganz im Gegenteil, die Vorschriften des IT-Sicherheitsgesetzes dürften im Vergleich mit anderen Gesetzen hinsichtlich ihrer Transparenz und Verständlichkeit deutlich besser abschneiden, da sie bereits einen gesetzgeberisch intendierten Technikbezug aufweisen. Anders sieht es jedoch für solche Gesetze aus, die teils schon seit einigen Jahren existieren und bei denen der Bezug zu IT-Sicherheit und Datenschutz nicht explizit benannt wird, von denen als Bestandteil einer guten Corporate Governance und IT-Compliance aber anerkannt ist, dass sie auch einen eindeutigen Technikbezug besitzen.

Als allgemeingültigstes Beispiel einer solchen Vorschrift können die §§ 91 Abs. 2, 93 Abs. 1 AktG herangezogen werden. Davon ausgehend hat der Vorstand geeignete Maßnahmen zu treffen, damit „den Fortbestand der Gesellschaft gefährdende Entwicklungen“ frühzeitig erkannt werden. Daneben haben die Vorstandsmitglieder bei ihrer Geschäftsführung „die

Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters“ anzuwenden. Bei diesen beiden interpretationsbedürftigen Formulierungen ergibt sich der Bezug zur IT-Security nicht einmal aus dem Gesetzeswortlaut. Anerkannt ist dennoch, dass unter die vorgenannten Beobachtungs- und Sorgfaltspflichten des Gesellschaftsrechts auch Maßnahmen der IT-Sicherheit zu fassen sind. Dies gilt aber nicht nur für große, am Kapitalmarkt beteiligte Aktiengesellschaften, sondern auch für die zahllosen mittelständischen Unternehmen, die in der Rechtsform der GmbH agieren. Hier ist allgemeine Auffassung, dass die Geschäftsführer der Sache nach die gleichen Sorgfaltspflichten wie der Vorstand einer Aktiengesellschaft treffen. Dies lässt sich aus § 43 Abs. 1 GmbHG ableiten – auch hier aber ergibt sich der Bezug zur Datensicherheit nicht aus der Vorschrift selbst und ist für den Rechtslaien deshalb auch nicht ohne Weiteres erkennbar. Über diese beiden gesellschaftsrechtlichen Beispiele hinaus existiert eine unübersichtliche Vielzahl weiterer Gesetze aus allen möglichen Arbeitsbereichen im Europa-, Bundes- und Landesrecht wie auch in untergesetzlichen Rechtsvorschriften, die zum Teil weitere zwingende IT-Compliance-Vorgaben enthalten, ohne dass dies explizit im Gesetz festgeschrieben wird.

II. Unbestimmte Rechtsbegriffe als praktisches Auslegungs- und Anwendungsproblem gesetzlicher Vorschriften

Doch selbst wenn die gesetzliche Vorschrift ausdrücklich bestimmt, dass von den jeweils Verantwortlichen Maßnahmen der IT-Security zu implementieren sind, steht der Rechtsanwender und damit der Umsetzungspflichtige oft vor dem Problem, dass die gesetzlich getroffenen Vorgaben für die tatsächliche Realisierung nicht hinreichend konkret sind. Grund dafür sind die so genannten „unbestimmten Rechtsbegriffe“, teils auch als „Generalklauseln“ bezeichnet. Juristisch gesehen handelt es sich bei ihnen um begriffsoffene gesetzliche Formulierungen, die es ermöglichen, dass Sachverhalte, die eigentlich außerhalb des Rechts stehen, inhaltlich dennoch durch die Gesetze berücksichtigt werden können. Da die gesetzlichen Regelungen zur IT-Sicherheit regelmäßig auf technische Sachverhalte Bezug nehmen, sind klassischerweise verwandte Sachbegriffe in diesem Bereich die „anerkannten Regeln der Technik“, der „Stand der Wissenschaft und Technik“ sowie der „Stand der Technik“. Letzterer findet auch im novellierten BSI-Gesetz Anwendung, indem in dessen § 8a die Forderung erhoben wird, dass die Betreiber von Kritischen Infrastrukturen bei der Umsetzung der IT-Sicherheitsmaßnahmen den Stand der Technik einhalten sollen. Juristisch definiert bedeutet Stand der Technik den „Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Ziels gesichert erscheinen lässt. Verfahren Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben und sollten – wenn dies noch nicht der Fall ist – möglichst im Betrieb mit Erfolg erprobt worden sein“. Dem Juristen reicht für die Rechtsanwendung diese Definition im Regelfall aus – für den mit der Realisierung der IT-Sicherheit beauftragten Techniker jedoch stellt sie bestenfalls einen groben Anhaltspunkt für seine Arbeit dar. Um jedoch auch für den technischen Anwender den Abstraktionsgrad der für ihn einschlägigen gesetzlichen Vorschriften zu reduzieren, werden Auslegungshilfen

entwickelt. Speziell für die Vorgaben des IT-Sicherheitsgesetzes kann hier zum Beispiel die Handreichung zum „Stand der Technik“ des Bundesverbands IT-Sicherheit (TeleTrusT) e.V. herangezogen werden.

Für die allermeisten gesetzlich festgeschriebenen unbestimmten Rechtsbegriffe existiert jedoch keinerlei Handreichung oder ein Organisationsmodell, um die abstrakten Vorschriften praxisgerecht aufbereitet zu konkretisieren. Vielmehr werden die Rechtsbegriffe für den Einzelfall durch Behörden und insbesondere durch die Rechtsprechung der Gerichte ausgefüllt. Dies hat zur Folge, dass selbst wenn ein technischer Anwender sämtliche für ihn relevanten einschlägigen Vorschriften zur Umsetzung der Datensicherheit kennt, er dennoch vor dem Problem steht, diese gesetzeskonform umzusetzen – und dies auch in denjenigen Fällen, in denen noch keine Konkretisierung von staatlicher oder privater Seite aus stattgefunden hat. Allgemeingültige Handreichungen zu verfassen, die sektorenübergreifend umfassende IT-Sicherheitsanforderungen im Sinne eines konkreten Stand-alone-Maßnahmenkatalogs definieren, ist aufgrund der branchentypischen Besonderheiten moderner Datenverarbeitung darüber hinaus kaum möglich. Stets müssen mögliche Abwandlungen und andersartige Vorgaben berücksichtigt werden. Die gesetzgeberisch zwar intendierten, aber in vielen Fällen unzureichend konkretisierten unbestimmten Rechtsbegriffe können somit eine erhebliche Rechtsunsicherheit zur Folge haben.

III. Die Entwicklung einer IT-Security Landscape als Lösungsmodell praxisnaher Gesetzeskonkretisierung für KMUs im Bereich von KRITIS

An dieser Stelle setzt der Forschungsansatz zur praxisnahen Konkretisierung der unbestimmten Rechtsbegriffe an. In interdisziplinärer Zusammenarbeit sind zunächst sämtliche Rechtsvorschriften sowohl im Europa-, Bundes- und Landesrecht, die für die IT-Sicherheit eine Relevanz besitzen, für alle Sektoren Kritischer Infrastrukturen ermittelt worden. Zur Verbesserung der Anwenderfreundlichkeit hat eine geeignete Aufbereitung der Vorschriften sortiert nach Kategorien und Rechtsetzungsinstanz, daneben aber auch nach Anwenderrelevanz, stattgefunden. Für jede Kategorie von Rechtsvorschriften wurden darüber hinaus einschlägige Paper und Rechtsprechung erfasst. Zur leichteren Anwendbarkeit wurden sämtliche Gesetze online verlinkt, und relevante Einzelparagraphen werden separat nach Relevanz sortiert aufgeführt, sodass ein schneller und gezielter Abruf möglich ist. Diese so geschaffene, mehrere Hundert Gesetze umfassende Sammlung von Rechtsvorschriften erfährt eine laufende Aktualisierung und wird aller Voraussicht nach im Herbst 2016 online frei und kostenlos zur Nutzung verfügbar sein. Die Online-Maske enthält zudem verschiedene Filter, sodass eine einfache Nutzung möglich ist.

Um Juristen und technischen Anwendern nicht nur einen schnellen und einfachen Überblick über die für sie relevanten Gesetze verschaffen zu können, sondern die Gesetze und die in vielen von ihnen enthaltenen unbestimmten Rechtsbegriffe zu konkretisieren, werden in einem zweiten Schritt der wissenschaftlichen Forschung gezielt sämtliche in den Rechtsvorschriften enthaltenen unbestimmten Rechtsbegriffe ermittelt und katalogisiert.

Darauf basierend erfolgt im Anschluss die Konkretisierung der unbestimmten Rechtsbegriffe mit Technikbezug für sämtliche Sektoren Kritischer Infrastrukturen in Zusammenarbeit mit verschiedenen Normungsgremien. Von deren Seite wurde parallel zur Erstellung der Sammlung von Rechtsvorschriften eine korrespondierende, umfassende Übersicht sämtlicher relevanter technischer Normen und Standards mit IT-Sicherheitsbezug erstellt. Diese Normenlandschaft ist in ihrer ersten Version schon jetzt online verfügbar. In einer Symbiose aus Recht und Technik sollen in den kommenden zwei Jahren in enger Zusammenarbeit mit den Normungsgremien die Schnittstellen zwischen den Normen und Standards und den entsprechenden unbestimmten Rechtsbegriffen ermittelt werden, das heißt es wird für jede Generalklausel in jeder relevanten Rechtsvorschrift geprüft, welche Normen und Standards zur Ausfüllung herangezogen werden können. Nach Abschluss dieses Abgleichs soll es möglich sein, einen Großteil der Rechtsvorschriften und Normen aus den bestehenden Datenbanken zusammenzuführen und dem Anwender zugänglich zu machen.

Durch die damit geleistete Forschungsarbeit ist es erstmals möglich, nicht nur sämtliche Rechtsvorschriften zur IT-Sicherheit vollumfassend und einfach systematisiert darzustellen, sondern mit Hilfe der unmittelbar stattfindenden Konkretisierung durch einschlägige technische Normen und Standards dem Anwender eine sofortige und zuverlässige Erst-Entscheidungshilfe zur Verfügung zu stellen, um für ihn möglicherweise verpflichtende IT-Security-Maßnahmen auf angemessene Weise zu implementieren. Das neu geschaffene Tool steht kostenfrei jedermann im Internet zur Verfügung, zudem soll es laufend mit neuen Features ausgestattet werden, dazu gehören beispielsweise zusätzliche Such- und Filteroptionen, die Anzeige weiterer Informationen zur den Normen und Standards auf Anforderung des Nutzers und eine grafische Darstellung der Ergebnisse (z.B. zur Aktivität in Gremien/Domänen als Tortendiagramm und als Heat Map; Statistiken zur Zahl der Referenzierungen in Gesetzen und Standards). Da die Praxistauglichkeit der Plattform im Vordergrund steht, erhält auch der Anwender die Möglichkeit zur Mitwirkung, indem er selbst neue Gesetze sowie Normen und Standards vorschlagen kann, die nach einer Prüfung in die Datenbank implementiert und dort vernetzt werden.

IV. Fazit und Ausblick

Insgesamt soll durch die Forschung zur IT-Security Landscape erreicht werden, dass vor allem die in den KMUs tätigen ITler eine deutliche Entlastung in ihrer täglichen Arbeitspraxis erhalten, indem ihnen ein effektives und effizientes Werkzeug einerseits zur Bestimmung möglicher rechtlicher Pflichten im Bereich IT-Security, andererseits zur Konkretisierung der damit verbundenen technischen Vorgaben zur Seite gestellt wird. Gerade für den mit der Umsetzung gesetzlicher Bestimmungen konfrontierten Endadressaten, der möglicherweise nicht immer über den unmittelbaren Zugriff auf juristische Ressourcen sowie auf Normen und Standards verfügt, ist eine solche einfache, schnelle wie auch verlässliche Erstorientierung wichtig, um die rechtlichen und technischen Maßstäbe seiner Arbeit zeitsparend und kostengünstig definieren zu können. Erste Rückmeldungen aus den Fachkreisen zur online bereits abrufbaren Normenlandschaft bestätigen dies.