Michael Knopp

Stand der Technik

Ein alter Hut oder eine neue Größe?

Der unbestimmte Rechtsbegriff „Stand der Technik" ist als Anforderung zuletzt mit dem IT-Sicherheitsgesetz und der Datenschutz-Grundverordnung gleich in mehrere zentrale Regelungen für die IT-Sicherheit aufgenommen worden. Mangels näherer begleitender Bestimmungen des Begriffs und teilweiser hoher Sanktionen bei mangelnder Pflichterfüllung besteht bei den Adressaten Unsicherheit zu den Auswirkungen dieser Begriffseinführung.

1 Stand der Technik – ein alter Hut?

Als Rechtsbegriff blickt die Formulierung „Stand der Technik" auf eine lange Geschichte zurück.[1] Die Definition des Begriffes in § 3 Abs. 6 BImSchG (Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge) beispielsweise war bereits in der Gesetzesveröffentlichung von 1974 enthalten. Sie hat ursprünglich gelautet: „Stand der Technik im Sinne dieses Gesetzes ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zur Begrenzung von Emissionen gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere vergleichbare Verfahren, Einrichtungen oder Betriebsweisen heranzuziehen, die mit Erfolg im Betrieb erprobt worden sind."[2] Die heutige Fassung hat den Bezug erheblich erweitert und verweist zur Bestimmung auf die Kriterien der Gesetzesanlage, ansonsten haben sich die entscheidenden Formulierungen nicht verändert.

Die bis heute weiter zur Definition oder Begriffsabgrenzung herangezogene „Kalkar"-Entscheidung des Bundesverfassungsgerichts geht ebenfalls weit zurück, nämlich auf das Jahr 1978.[3]

Für die Verantwortlichen im Bereich des Datenschutzes und der Datensicherheit hat der Begriff jedoch durch verschiedene Gesetzesänderungen eine neue Aktualität gewonnen: Durch das IT-Sicherheitsgesetz vom 17.07.2015 ist der Begriff des „Standes der Technik" in § 13 Abs. 7 TMG (Telemediengesetz) sowie im Zuge der Regulierung der Kritischen Infrastrukturen in § 8a Abs. 1 S. 2 BSI-G (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) eingeführt worden.[4] Zum 10.05.2018 werden diese Pflichten dann durch den aus der Umsetzung der NIS-Richtlinie (europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit) stammenden § 8c BSI-G ergänzt werden. Dieser legt den Anbietern digitaler Dienste die Pflicht auf, Maßnahmen nach dem „Stand der Technik" zur Begrenzung der Auswirkungen von Sicherheitsvorfällen zu ergreifen.[5] Von besonderer Tragweite ist jedoch, dass die Datenschutz-Grundverordnung[6] sich in Art. 32 Abs. 1 S. 1 in der deutschen Übersetzung auf den „Stand der Technik" bezieht, während dieser in § 9 BDSG (Bundesdatenschutzgesetz) keine Erwähnung fand.[7]

Damit ist der „Stand der Technik" nun in mehreren die IT-Sicherheit betreffenden Kernnormen zum Anforderungskriterium geworden.

Allerdings ist die Begriffsverwendung in Bezug auf IT-Sicherheit auch keineswegs gänzlich neu: In § 109 Abs. 1 TKG (Telekommunikationsgesetz) wird die Berücksichtigung des „Stands der Technik" bereits seit dem 10.05.2012 gefordert.

Dennoch führt die Auslegung des Begriffes bei der Vorbereitung der nach § 8a Abs. 3 BSI-G zu erbringenden Nachweise oder bei den vielfach derzeit laufenden Vorbereitungsprojekten zur Compliance mit der Datenschutz-Grundverordnung aktuell

1 S.a. Seibel, Abgrenzung der „allgemein anerkannten Regeln der Technik" vom „Stand der Technik", NJW 2013, 3000.

2 Bundes-Immissionsschutzgesetz vom 15.03.1974, BGBl I Nr. 27, S. 721.

3 BVerfGE 49, 89 (135 f) (Beschluss vom 8.8.1978).

Michael Knopp, Jurist

Berater bei der Secorvo Security Consulting GmbH. Schwerpunkte: Datenschutz und Rechtsfragen im Kontext der IT-Sicherheit.

E-Mail: michael.knopp@secorvo.de

4 Das IT-Sicherheitsgesetz hat die Berücksichtigung des „Standes der Technik" außerdem in § 109 Abs. 2 S. 3 TKG eingefügt. Im ebenfalls durch das IT-Sicherheitsgesetz angepassten Energiewirtschaftsgesetz oder dem Atomgesetz fehlen entsprechende Bezüge auf den „Stand der Technik" dagegen. S. IT-Sicherheitsgesetz, BGBl I Nr. 31, S. 1324, vom 24.07.2015.

5 Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 06.07.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union vom 23.06.2017, BGBl I 2017 Nr. 40, S. 1885 vom 29.06.2017, abrufbar unter https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s1885.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s1885.pdf%27%5D__1506335215080

6 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679 vom 27.04.2016.

7 Genau genommen ist ein Bezug auf den „Stand der Technik" in den letzten Satz der Anlage zu § 9 BDSG bereits am 1.9.2009 durch das DSRÄndG vom 14.08.2009 (BGBl I 2009, S. 2814) aufgenommen worden. Dort diente er bislang jedoch nur zur Qualifizierung von zu verwendenden Verschlüsselungsmaßnahmen als geeignete Maßnahme zur Zugangs-, Zugriffs- und Weitergabekontrolle.

zu Diskussionen, die zeigen, dass die Auslegung in dem neuen Kontext durchaus nicht als längst ausdiskutiert angesehen wird.[8]

2 Stand der Technik für die IT-Sicherheit

Die Unsicherheiten bei der Begriffsauslegung werden durch verschiedene Umstände begründet.

In vielen Verwendungskontexten wird der unbestimmte Rechtsbegriff „Stand der Technik" bereits durch einen Verweis auf begleitende technische Normen näher bestimmt. Beispiele hierfür sind die Vermutung der Einhaltung des „Stands der Technik" bei Umsetzung einer begleitend erlassenen Technischen Richtlinie in § 18 Abs. 2 S. 2 De-Mail-Gesetz, der Verweis auf die Richtlinien der Bundesärztekammer in § 18 Abs. 2 Transfusionsgesetz, natürlich der Verweis auf die Gesetzesanlage in § 3 Abs. 6 BImSchG oder der vergleichbare Anlagenverweis in § 3 Nr. 11 WHG (Wasserhaushaltsgesetz). Weder das BSI-Gesetz noch die Datenschutz-Grundverordnung enthalten vergleichbare Verweise. Das BSI-Gesetz sieht allerdings in § 8 Abs. 1 BSI-G durch das BSI erlassene Mindeststandards für die Stellen des Bundes vor und ermöglicht den Branchenverbänden eigene Sicherheitsstandards vorzulegen (§ 8a Abs. 2 BSI-G).

Ein weiterer Unterschied zu anderen Regelungskontexten ist die Messbarkeit. Im Bereich des Umweltrechts beispielsweise kann das Maßnahmenziel durch die Einhaltung bestimmter Grenzwerte definiert werden. Für den Schutz personenbezogener Daten oder die angemessene Sicherheit informationstechnischer Systeme sind die zu erreichenden Ziele deutlich schwieriger zu bestimmen.

Auf der anderen Seite aber wird die nicht ausreichende Pflichterfüllung beim Ergreifen technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Maßnahmen in Art. 83 Abs. 4 a) DS-GVO mit Geldbußen von bis zu 10 Millionen Euro oder bis 2% des weltweit erzielten Jahresumsatzes sanktioniert und auch im Fall einer Verletzung der Pflichten aus § 8a BSI-G drohen nach § 14 Abs. 2 BSI-G 50.000 Euro Geldbuße.

Die verschiedenen Definitionsansätze verwenden zudem Formulierungen wie „Stand der Technik ist […] der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der die praktische Eignung einer Maßnahme zur [Zweckangabe der Maßnahmen] zur Erreichung eines allgemein hohen Schutzniveaus für [Angabe des Schutzgegenstandes] insgesamt gesichert erscheinen lässt."[9] Diese Formulierung greift auch die Begründung des IT-Sicherheitsgesetzes für § 8a BSI-G auf. In der Begründung erfolgt auch der Verweis auf einschlägige internationale, europäische und nationale Normen und Standards. Voraussetzung ist allerdings die erfolgreiche Erprobung der Verfahren, Einrichtungen und Betriebsweisen in der Praxis.[10]

Aus der Kalkar-Entscheidung stammt die folgende Formulierung: „Der rechtliche Maßstab für das Erlaubte oder Gebotene wird hierdurch an die Front der technischen Entwicklung verlagert […]". Während „fortschrittliche Verfahren" zwar bereits die Aktualität erfordert, erweckt „Front der technischen Entwicklung" den Eindruck, als würden nur die neuesten Verfahren oder Mittel dem „Stand der Technik" entsprechen.

Die Entscheidung des Bundesverfassungsgerichts greift zudem die „Drei-Stufen-Theorie" auf, die den „Stand der Technik" bezüglich der Aktualität und Anerkennung oder empirischen Feststellung der Eignung zwischen den anerkannten Regeln der Technik und dem Stand der Wissenschaft und Forschung ansiedelt. Bezogen auf die Verfahren, Einrichtungen, Betriebsweisen oder Mittel der Informationssicherheit geht diese Einordnung jedoch ohnehin von einem wenig relevanten Bild aus. Die Entwicklung der IT-Sicherheit vollzieht sich nicht als wissenschaftliches Konzept, das zunächst als Theorie und experimenteller Prototyp besteht, dann in der Praxis zur Anwendung kommt und seine Eignung beweist, um zuletzt zum anerkannten Standard zu werden. Zudem spielen die anderen beiden Stufen bislang begrifflich in Bezug auf Maßnahmenanforderungen keine Rolle.

Forschung und Entwicklung sind in der schnelllebigen IT-Sicherheit viel stärker von der gezielten Produktentwicklung getrieben. Die Eignung gilt regelmäßig der Abwehr sich künftig entwickelnder Gefahren. Die Einordnung durch die „Drei-Stufen-Theorie" ist also bezogen auf die IT-Sicherheit wenig aussagekräftig.

Die genannten Formulierungen sind jedoch vermutlich der Ursprung für neuere, auf die IT-Sicherheit bezogene Auslegungen, die diese Kritik zwar aufgreifen, die Anforderungen durch den Verweis auf den „Stand der Technik" jedoch eher noch weiter nach oben schrauben: „Beim Stand der Technik handele es sich um die im Waren- und Dienstleistungsverkehr verfügbaren Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele am wirkungsvollsten gewährleisten kann." Oder: Es handele sich „um die am Markt verfügbaren Bestleistungen von Maßnahmen zum Schutz der IT-Sicherheit".[11]

Es gibt weder Anhaltspunkte dafür, dass die Maßnahmen überhaupt Gegenstand eines Dienstleistungsverkehrs sein müssen, noch dafür dass der „Stand der Technik" nur gewahrt wäre, wenn es sich um die wirkungsvollste oder die verfügbare Bestleistung handelt. Zudem wirft diese Auslegung die Frage auf, wie überhaupt der Wirkungsgrad verschiedener Maßnahmen mit einem vergleichbaren Ziel in der IT-Sicherheit vergleichbar gemacht werden soll.

Der Umgang mit dem unbestimmten Rechtsbegriff „Stand der Technik" ist angesichts dieser Umstände nicht leicht. Hinzu kommt, dass sich bereits die Einbindung des Begriffs in allen drei Regelungen (DS-GVO, TMG, BSIG) unterscheidet. In keiner der genannten Regelungen bemessen sich jedoch tatsächlich die zu ergreifenden Maßnahmen auch nur hauptsächlich nach dem „Stand der Technik".

3 Stand der Technik in Art. 32 DS-GVO

In Art. 32 Abs. 2 DS-GVO ist das Ziel, die Risiken der Verarbeitung personenbezogener Daten insbesondere durch Vernichtung, Verlust, Veränderung. unbefugte Offenlegung oder unbefugten Zugang einzudämmen.

8 S. beispielsweise Bartels, Gretchenfrage, iX 7/2017, 48; TeleTrusT – Bundesverband IT-Sicherheit e.V., Handreichung zum Stand der Technik im Sinne des IT-Sicherheitsgesetzes, abrufbar unter https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/TeleTrusT-Handreichung_Stand_der_Technik.pdf.

9 § 3 Abs. 6 BImSchG, § 3 Nr. 11 WHG, nahezu wortgleich.

10 BT-Drs. 18/4096, S. 26.

11 Bartels, Gretchenfrage, iX 7/2017, 49 (50).

Bei der Beurteilung des angemessenen Schutzniveaus, das durch die technischen und organisatorischen Maßnahmen erreicht werden soll, sollen neben dem „Stand der Technik“ die Implementierungskosten, die Eintrittswahrscheinlichkeit, die Schwere des Risikos für die Betroffenen und Art, Umfang, Umstände und Zwecke der Verarbeitung berücksichtigt werden. Dass die Maßnahmen dem „Stand der Technik“ entsprechen ist also hier nur eines aus einer Reihe von Bewertungskriterien, die zu berücksichtigen sind.

Die Erwägungsgründe gehen hier nicht weiter auf die Bestimmung des „Standes der Technik“ ein. Zu beachten ist bei der Auslegung des „Stands der Technik“ in der Datenschutz-Grundverordnung jedoch, dass hier nicht ohne weiteres von den Definitionsversuchen des deutschen Rechts, der deutschen Rechtsprechung oder der deutschen Rechtswissenschaft ausgegangen werden kann. Da hinter der Datenschutz-Grundverordnung die europäischen Rechtsetzungsorgane stehen, sind im Grundsatz die Definitionsansätze sämtlicher europäischer Rechtskreise zu berücksichtigen. Anzusetzen ist hier bereits bei den unterschiedlichen Sprachfassungen, z.B. „state oft he art“ in der englischen Fassung der Datenschutz-Grundverordnung.

Das heißt, dass im Rahmen der Datenschutz-Grundverordnung ohnehin eine eigenständige Interpretation des Begriffes gefunden werden muss.

4 Stand der Technik in § 8a BSI-G

§ 8a BSI-G verpflichtet die Betreiber Kritischer Infrastrukturen, organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, der Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme zu treffen. Die Vorkehrungen sollen im Verhältnis zu den Folgen möglicher Störungen stehen.

Der „Stand der Technik“ soll dabei eingehalten werden. Er ist damit hier nicht lediglich als ein Kriterium in die Bewertung einzubeziehen. Im Rahmen des § 8a BSI-G ist es eine unmittelbare Voraussetzung für das Ausreichen einer Vorkehrung, dass sie dem „Stand der Technik“ entspricht.

Dennoch bestimmt das Gesetz nicht weiter, wie der „Stand der Technik“ ermittelt werden soll. Das Gesetz eröffnet lediglich den Branchenverbänden die Möglichkeit, Sicherheitsstandards festzulegen. Die Gesetzesbegründung nimmt dann, wie oben bereits dargestellt, Bezug auf einschlägige internationale, europäische und nationale Normen und Standards, aber auch auf vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden. Ein Bestimmungskriterium ist damit der erfolgreiche praktische Einsatz. Wie aktuell die getroffenen Vorkehrungen technisch zu sein haben, lässt sich dagegen nicht ableiten.

5 Stand der Technik in § 13 Abs. 7 TMG

Bezüglich § 13 Abs. 7 TMG stellt sich ohnehin die Frage, in welchem Verhältnis die Regelung künftig zu § 8c BSI-G stehen soll. Schutzziele der Regelung sind der Ausschluss unerlaubter Zugriffe auf die durch die Telemedien genutzten technischen Einrichtungen und die Sicherung gegen Datenschutzverletzungen sowie äußere Angriffe.

Der „Stand der Technik“ ist erneut nur zu berücksichtigen. Weitere Kriterien für die technischen und organisatorischen Vorkehrungen sind die technische Möglichkeit und die wirtschaftliche Zumutbarkeit.

6 Praktischer Umgang mit dem Stand der Technik

Der Regelungskontext zeigt deutlich, dass die Bedeutung des Verweises auf den „Stand der Technik“ nicht zu hoch bewertet werden sollte. Lediglich in § 8a BSI-G ist das Einhalten des „Standes der Technik“ überhaupt eine direkte Voraussetzung für das Ausreichen der jeweiligen Vorkehrung.

Die Unterschiede zu vielen bisherigen Verwendungen des Begriffs mit direktem Bezug auf ergänzende technische Regelwerke rechtfertigen zudem eine eigenständige Begriffsauslegung in Bezug auf Vorkehrungen zur Informationssicherheit.

Kern der diesbezüglichen Überlegungen sollte der Zweck der Einfügung des unbestimmten Rechtsbegriffs sein. Ebenfalls in der oben zitierten Kalkar-Entscheidung hat das Bundesverfassungsgericht hierzu ausgeführt: „Auf Gebieten […], bei denen durch die rasche technische Entwicklung ständig mit Neuerungen zu rechnen ist, [ist zu bedenken], dass der Gesetzgeber, hätte er tatsächlich einmal eine detaillierte Regelung getroffen, diese laufend auf den jeweils neuesten Stand bringen müsste.“ „Durch die Verwendung unbestimmter Rechtsbegriffe werden die Schwierigkeiten der verbindlichen Konkretisierung und der laufenden Anpassung an die wissenschaftliche und technische Entwicklung mehr oder weniger auf die administrative und – soweit es zu Rechtsstreitigkeiten kommt – auf die judikative Ebene verlagert.“

Ein Zweck des Begriffes ist es also, die Regelung dynamisch zu halten, um die Weiterentwicklung einerseits zu berücksichtigen, andererseits aber die getroffene Regelung nachhaltig zu fassen. Die Berücksichtigung des „Standes der Technik“ soll also verhindern, dass einmal getroffene Vorkehrungen als endgültig betrachtet werden können. Durch die Berücksichtigung des sich fortentwickelnden „Stands der Technik“ müssen die Vorkehrungen kontinuierlich auf ein Entfallen ihrer Eignung durch Veraltung überprüft werden.

Hieraus jedoch zu folgern, die Vorkehrungen müssten stets auf dem neusten Stand sein, ginge zu weit. Solange die Vorkehrungen geeignet sind, die Schutzziele zu erfüllen, soll durch die Berücksichtigung des „Stands der Technik“ keine verschärfte Anforderung geschaffen werden.

Versuche, Leitfäden zu schaffen und Maßnahmen daraufhin zu bewerten, ob sie dem „Stand der Technik“ entsprechen,[12] sind dennoch lobenswert und praktisch sicher hilfreich, da es die Auswahl möglicher Vorkehrungen erleichtert. Besonders im Zusammenhang mit Maßnahmen zur IT-Sicherheit sollte jedoch immer im Blick behalten werden, dass diese lediglich dazu dienen, ein von der IT-Nutzung ausgehendes Risiko akzeptabel zu machen. Ob die hierzu genutzten Maßnahmen neu oder auf dem letzten Stand sind, ist letztlich gleichgültig, solange sie dieses Ziel erreichen.

Einen Rechner mit einer kritischen Anwendung komplett isoliert zu halten und nicht weiter zu vernetzen, ist sicher kein fortgeschrittenes Verfahren. Unter bestimmten Umständen ist es aber eine nach wie vor effektive und taugliche Maßnahme. Es besteht kein Anlass anzunehmen, dass solche Maßnahmen durch den Verweis auf den „Stand der Technik“ unzulässig gemacht werden sollen.

Letztendlich ist in den hier genannten Kontexten der gewahrte „Stand der Technik“ eine Anforderung, jedoch nicht alleiniges Kriterium für die Angemessenheit der Maßnahmen.

Zusammenfassung

Mit dem IT-Sicherheitsgesetz und der Datenschutz-Grundverordnung sind an mehreren für die IT-Sicherheit maßgeblichen Stellen die Berücksichtigung oder Wahrung des „Stands der Technik“ in die Maßnahmenanforderungen aufgenommen worden.

Schon wegen der unterschiedlichen Gesetzgeber, aber auch durch die fehlenden Regelungen zur näheren Bestimmung kann die Auslegung des Begriffs jedoch nicht einfach und unkritisch auf das herkömmliche Verständnis gestützt werden. Gleichzeitig ist der „Stand der Technik“ bezogen auf die IT-Sicherheit der falsche Ansatzpunkt, um die Schutzanforderungen zu verschärfen.

Der Verweis auf den „Stand der Technik“ sollte daher im Kontext der IT-Sicherheit lediglich als Aufforderung verstanden werden, die Eignung der getroffenen Maßnahmen angesichts der fortschreitenden technischen Entwicklung regelmäßig zu überprüfen. Die Berücksichtigung des „Stands der Technik“ verhindert, dass Sicherheitslücken durch Überalterung der Schutzvorkehrungen entstehen. Die Verwendung des Begriffes soll nicht dazu zwingen, ohne tatsächliche Notwendigkeit stets die neueste oder bestmögliche Maßnahme zu ergreifen.

Der Impuls zu einer verstärkten IT-Sicherheit, der sicher wünschenswert ist, muss von der Angemessenheitsbewertung und der Risikoeinschätzung sowie von der Ermittlung der tatsächlichen Angriffsmöglichkeiten ausgehen.

Ein alter Hut ist die Berücksichtigung des „Stands der Technik“ für IT-Sicherheitsmaßnahmen dennoch nicht, dazu wirft er bezüglich seiner Auslegung für die IT-Sicherheit zu viele Fragen auf.

12 Teletrust – Bundesverband IT-Sicherheit e.V., Handreichung zum „Stand der Technik“ im Sinne des IT-Sicherheitsgesetzes, abrufbar unter https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/TeleTrusT-Handreichung_Stand_der_Technik.pdf