BESTIMMUNG DES »STAND DER TECHNIK«

Tomasz Lawicki

Im Juli 2015 trat das IT-Sicherheitsgesetz (IT-SiG) in Kraft. Damit wurde ein branchenübergreifendes Fundament für die nachhaltige Verbesserung der IT-Sicherheit in Deutschland geschaffen. Obwohl sich IT-SiG augenscheinlich an die sogenannten Betreiber kritischer Infrastrukturen (KRITIS-Betreiber) richtet, sind auch die Nicht-KRITIS-Betreiber mittelbar und unmittelbar dazu verpflichtet, den geforderten »Stand der Technik« einzuhalten, denn die Verpflichtung zur Einhaltung der gesetzlichen Vorgaben werden die KRITIS-Betreiber bei ihren Dienstleistern vertraglich einfordern. Eine weitere Verpflichtung beruht auf den mit dem IT-SiG eingeführten Änderungen im Telemediengesetz (TMG). Dort wird zumindest die Berücksichtigung des »Stands der Technik« klar gefordert und zwar unabhängig von der KRITIS-Einordnung.

Doch was bedeutet »Stand der Technik« konkret? Wie kann man ihn nachweisen und die geforderten technischen und organisatorischen Maßnahmen umsetzen? Welche Maßnahmen gilt es mindestens zu berücksichtigen? Diese Fragen werden weder im IT-SiG noch in der bisher veröffentlichten KRITIS-Verordnung zur Bestimmung der KRITIS-Betreiber beantwortet.

In der Gesetzgebung wird der Begriff »Stand der Technik« gerne verwendet, weil er zeitlos, unverbindlich, aber dennoch zweckdienlich ist. Einerseits wird die vom Gesetzgeber gewollte Zielrichtung vorgegeben, andererseits bleibt der Gesetzestext unabhängig von der technologischen Entwicklung entkoppelt und ist somit stets aktuell. Doch wenn es darum geht, den »Stand der Technik« einzuhalten und gar nachzuweisen, wird es für die Betroffenen schwierig, diesen praxistauglich zu bestimmen.

Der »Stand der Technik« muss von den begrifflich ähnlich lautenden Generalklauseln wie »allgemein anerkannte Regeln der Technik« und »Stand der Wissenschaft und Technik« abgegrenzt werden.

Begrifflich ist der »Stand der Technik« zwischen den beiden Generalklauseln anzusehen.[1]

Sollen bereits implementierte oder erst zu planende Maßnahmen eingeordnet werden, bedarf es einer Methodik mit eindeutigen und nachvollziehbaren Kriterien.[2] Die Methodik muss es ermöglichen, die Maßnahmen objektiv zu bewerten, mit Alternativen zu vergleichen und zu dokumentieren.

Neben den einzelnen Maßnahmen und deren Alternativen muss auch die Gesamtheit der Maßnahmen betrachtet werden, denn die Wirksamkeit der eingesetzten Maßnahmen ist nur so gut wie ihr schwächster Bestandteil.

Für die initiale Analyse wird auf die vom TeleTrusT, Bundesverband für IT-Sicherheit im Mai dieses Jahres veröffentlichte »Handreichung zum Stand der Technik im Sinne des IT-Sicherheitsgesetzes« verwiesen.[3] Das Dokument kann als Referenz für Vereinbarungen zu Sicherheitsmaßnahmen bzw. für die Einordnung implementierter Sicherheitsmaßnahmen dienen. Da die heutigen, als »Stand der Technik« geltenden, Maßnahmen aufgrund der evolutionsbedingten Verschiebung vielleicht schon morgen eher den »allgemein anerkannten Regeln der Technik« zuzuordnen sind, muss ihre Aktualität fortlaufend geprüft werden.

Auch die Europäische Datenschutzgrundverordnung (DSGVO) fordert bei der Umsetzung von technischen und organisatorischen Maßnahmen die Berücksichtigung des »Stands der Technik«. Auch in diesem Fall wurden die geforderten Schutzmaßnahmen nicht eindeutig konkretisiert. Der Arbeitskreis »Stand der Technik« des TeleTrust wird daher weitere Unterstützung leisten und die oben erwähnte Handreichung im Hinblick auf die datenschutzrechtlichen Bestimmungen aus technischer Sicht ergänzen. So kann die Forderung zur Einhaltung des »Stands der Technik« als verbindendes Element eine Brücke zwischen dem geforderten Datenschutz und der IT-Sicherheit schlagen.

[1] Vgl. Bundesministerium für Justiz und Verbraucherschutz, Handbuch der Rechtsförmlichkeit, Seite 4, *http://hdr.bmj.de/page_b.4.html*

[2] Vgl. dazu Michaelis, Der „Stand der Technik" im Kontext regulatorischer Anforderungen, DuD 2016, S. 458 ff.

[3] Die „Handreichung zum Stand der Technik im Sinne des IT-Sicherheitsgesetzes" ist frei abrufbar auf der Internetseite von TeleTrust unter: *https://www.teletrust.de/publikationen/broschueren/stand-der-technik/*

Über den Autor

Tomasz Lawicki
Associated Senior Auditor, AC – The Auditing Company, Sachverständigen-Sozietät Dr. Schwerhoff,
Leiter des Arbeitskreises »Stand der Technik« TeleTrusT,
Bundesverband für IT-Sicherheit