TeleTrusT – Bundesverband IT-Sicherheit e.V.

Der IT-Sicherheitsverband.

Berlin, 13.08.2016

Stellungnahme

zum "Diskussionspapier zur Absicherung von Telemediendiensten nach Stand der Technik" des BSI

(TeleTrusT-AG "Recht")

TeleTrusT - Bundesverband IT-Sicherheit e.V.
Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.), "TeleTrusT Engineer for System Security" (T.E.S.S.) und "Certified Professional for Secure Software Engineering" (CPSSE) sowie des Qualitätszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

1 Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik hat am 05.07.2016 ein Diskussionspapier zur Absicherung von Telemediendiensten nach Stand der Technik veröffentlicht und zu einer kritischen Stellungnahme bis zum 15.08.2016 aufgerufen.

Das Diskussionspapier richtet sich an die Adressaten des durch das IT-Sicherheitsgesetz von Juli 2015 geänderten § 13 Abs. 7 TMG. Insbesondere hat das Diskussionspapier zum Ziel, den unbestimmten Rechtsbegriff "Stand der Technik", welcher gemäß Art. 13 Abs. 7 S. 2 TMG "zu berücksichtigen" ist, mit praxistauglichen und konkreten Inhalten auszufüllen.

Das Diskussionspapier gliedert sich in die Nennung und Erläuterung der drei Provider-Typen von Telemediendiensten (Content, Host und Access Provider) sowie die anschließende Aufzählung und Beschreibung von "Maßnahmen zur Absicherung". Im Rahmen dieses zweiten Punktes werden zum einen tabellarisch für jeden Provider-Typ sogenannte "Basis"- und "Standardmaßnahmen" aufgezählt, wobei erstere umgesetzt werden müssten, letztere hingegen umgesetzt werden sollten. Im Anschluss werden die einzelnen Basis- und Standardmaßnahmen mit Beispielen erläutert und auch zum Teil konkretisiert, hauptsächlich unter Verweisung auf den IT-Grundschutz-Katalog und Technische Richtlinien (TR) des BSI. Als Referenzen werden zudem andere Dokumente angegeben, beispielsweise der Allianz für Cybersicherheit, welche selbst an der Ausarbeitung des Diskussionspapiers mitgewirkt hat.

Positiv ist hervorzuheben, dass dieses Diskussionspapier den Versuch unternimmt, den im Gesetz nicht weiter ausgefüllten Begriff des "Standes der Technik" zu umgrenzen und mit Leben auszufüllen. Anders als bei den Betreibern kritischer Infrastrukturen (KRITIS), an welche ähnliche gesetzliche Anforderungen gestellt werden (insbesondere § 8a BSIG), ist für die Adressaten des § 13 Abs. 7 TMG nicht vorgesehen, dass "branchenspezifische Mindestanforderungen" zur Konkretisierung dieser Anforderungen aufgestellt werden. Deshalb ist es zu begrüßen, dass das BSI einen Schritt auf die Anbieter von Telemediendiensten zugeht.

2 Kritik - keine methodische Annäherung
Neben einzelnen inhaltlichen Kritikpunkten (hierzu unten) ist hauptsächlich der fehlende methodische Ansatz des Diskussionspapiers zu bemängeln. Das Diskussionspapier beschäftigt sich ausschließlich mit praktischen Inhalten des "Standes der Technik", jedoch zum einen völlig losgelöst von seinem rechtlichen Kontext und zum anderen ohne zu erklären, wie das BSI methodisch zu der Erkenntnis gelangt ist, dass die genannten Maßnahmen dem "Stand der Technik" entsprechen (methodische Annäherung). Der Gesetzesadressat wird beispielsweise darüber informiert, dass "sichere Passwörter" für alle Provider-Typen als Basis-Maßnahme einzustufen seien und wird dabei auf den IT-Grundschutzkatalog M.2.11 verwiesen.

Eine für Praxis notwendige Methode zur Ermittlung des "Standes der Technik" wurde jedoch nicht entwickelt. Eine methodische Annäherung an die Ermittlung des Standes der Technik wäre in einer solchen Ausarbeitung jedoch aus mehreren Gründen erforderlich gewesen: Die konkreten Maßnahmen zur Umsetzung der Anforderungen an die Sicherheit informationstechnischer Systeme von Telemediendiensten, die durch § 13 Abs. 7 TMG aufgestellt werden, unterliegen naturgemäß dem Wandel und dem technischen Fortschritt und eigenen sich deshalb weder für eine gesetzliche Fixierung noch eine Ausführungsbestimmung per Rechtsverordnung. Gleiches gilt jedoch für die vorliegende Ausarbeitung des BSI. Auch diese wird über kurz oder lang nicht mehr aktuell sein und dem lesenden Rechtsanwender deshalb nur einen Mehrwert bringen, wenn sie nicht nur konkrete (aber dem Lauf der technischen Entwicklung anheimfallende) Maßnahmen benennt, sondern bereits einen Schritt zuvor ansetzt und die Kriterien und Überlegungen des BSI zur Ermittlung dieser Maßnahmen als Stand der Technik transparent macht.

Dem Rechtsanwender ein solides Handwerkszeug mit auf den Weg zu geben, ist nicht zuletzt deshalb wichtig, da Verstöße gegen § 13 Abs. 7 TMG größtenteils bußgeldbewährt sind und der "Stand der Technik" als unbestimmter Rechtsbegriff der vollen gerichtlichen Kontrolle unterliegt.[1]

3 Verbesserung: erst abstrakt, dann konkret
Dem Diskussionspapier wurde zunächst der Wortlaut des § 13 Abs. 7 TMG abgebildet. Es bleibt jedoch offen, warum - gerade in Bezug auf die Zielrichtung der Ausarbeitung des BSI - nur Satz 1 und 2, jedoch nicht Satz 3 ("Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens") widergegeben wurden.

In einem ersten Schritt sollte jedenfalls eine definitorische Auseinandersetzung mit der Begrifflichkeit "Stand der Technik" erfolgen. Die Gesetzesbegründung zum IT-Sicherheitsgesetz enthält im Rahmen des § 8a BSIG eine Definition zum Stand der Technik. Diese lautet: *"Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt."*[2]

Üblicherweise wird der "Stand der Technik" von zwei weiteren Verweisungsbegriffen[3] abgegrenzt: Ein geringeres Schutzniveau als der "Stand der Technik" weisen gemeinhin die "anerkannten Regeln der Technik" auf. Diese beziehen sich auf Vorkehrungen, die sich in der Praxis bewährt und durchgesetzt haben, ohne dabei den technischen Fortschritt einzubeziehen, weshalb auch veraltete Verfahren erfasst werden. Ein höheres Schutzniveau bildet der "Stand von Wissenschaft und Technik" ab, der die neuesten wissenschaftlichen Erkenntnisse einbezieht. Diese müssen nicht erprobt, nicht regulär auf dem Markt erhältlich sein. Auf eine praktische Realisierbarkeit kommt es mithin nicht an. Durch diese Abgrenzung wird bereits deutlich, dass der "Stand der Technik" die Verwendung solcher technischen und organisatorischen Maßnahmen meint, die praktisch erprobt und realisierbar sind, aber an der vordersten Front des technisch Möglichen einzuordnen sind.

Diese Einstufung und Abgrenzung schlägt sich in der Definition des Gesetzgebers in der Formulierung "Entwicklungsstand *fortschrittlicher* Verfahren, Einrichtungen und Betriebsweisen" nieder. Im Ergebnis fordert der "Stand der Technik" damit, dass die Maßnahmen den Schutzzweck am besten verwirklichen.

An dieser Stelle wäre eine Einschätzung des BSI wünschenswert, die in abstrakter Weise verdeutlicht, wie es den "Stand der Technik" im Zusammenhang mit den gesetzgeberischen Ausführungen definiert. Methodisch

[1] Vgl. "Stand der Technik" im Bundesimmissionsschutzgesetz; dazu Schulte, Martin/Michalk, Kathleen, in: BeckOK Umweltrecht, Hrsg. Giesbert/Reinhardt, BImSchG, § 3 Rn. 92
[2] BT Drs. 18/4096, S. 26
[3] Siehe zur Abgrenzung bereits BVerfG, NJW 1979, S. 359 ff. (362)

würde es dem Rechtsanwender helfen, Hinweise darauf zu erhalten, welche generellen Anforderungen in Bezug auf die Maßnahmen im Sinne des § 13 Abs. 7 TMG üblicherweise an ihn gestellt werden. Es müsste unter anderem darauf eingegangen werden, wie die methodische Vorgehensweise des Telemediendienstanbieters auszusehen hat.[4] Möglich wäre in einem ersten Schritt, im Rahmen einer limitierten Schutzbedarfsanalyse die technischen Einrichtungen des Telemedienangebotes zu erfassen. Ein zweiter Schritt könnte darin bestehen, die in der Branche typischerweise praktisch genutzten und erprobten technischen Vorkehrungen zum Schutz von Telemedien sowie bereits bestehende Sicherheitsstandards zu identifizieren.[5] Hier sollten zudem Technologien aus anderen Arbeitsgebieten herangezogen und deren Übertragbarkeit geprüft werden. Das BSI sollte in diesem Zusammenhang deutlich machen, dass es im Rahmen des "Standes der Technik" immer darauf ankommt, dass die technischen Vorkehrungen dabei unter der Prämisse zu prüfen und auszuwählen sind, dass sie den bestmöglichen Schutz der auf dem Markt erhältlichen Produkte bieten.

In diesem Zusammenhang erscheint das Diskussionspapier in einem weiteren Aspekt zu eindimensional. In § 13 Abs. 7 TMG bezieht sich die Berücksichtigung des Standes der Technik nicht ausschließlich auf die in S. 1 geforderten technischen Vorkehrungen, sondern gleichermaßen auf die organisatorischen Vorkehrungen.

Auch wenn es sprachlich gewöhnungsbedürftig sein mag, organisatorischen Maßnahmen einen Stand der *Technik* zu geben,[6] so sollte die Ausarbeitung des BSI eindeutig dazu Stellung nehmen, dass nach § 13 Abs. 7 S. 1 TMG auch bei organisatorischen Vorkehrungen der "Stand der Technik" zu berücksichtigen ist. An dieser Stelle wäre eine Konkretisierung wünschenswert, wie die Ermittlung geeigneter, dem Stand der Technik entsprechender organisatorischer Maßnahmen oder Maßnahmenpakete durchzuführen ist bzw. auch hierzu konkrete Vorschläge zu unterbreiten. Zwar wird in dem Papier des BSI die organisatorische Maßnahme genannt, die bereits in der Gesetzesbegründung zu § 13 Abs. 7 TMG angesprochenen wurde:[7] nämlich die Notwendigkeit, beauftragte Unternehmen (z. B. Werbedienstleister) zu bestimmten Schutzmaßnahmen vertraglich zu verpflichten. In der Ausarbeitung des BSI fehlt es jedoch an einer strukturellen Unterteilung in die methodische Ermittlung und Benennung sowohl technischer als auch organisatorischer Vorkehrungen und deren jeweiliger Relation zum Stand der Technik.

4 Wenn konkret, dann konkret

Der Hauptteil des Diskussionspapiers beschäftigt sich mit der Auflistung und Erläuterung der konkreten Maßnahmen, die als dem "Stand der Technik" entsprechend gelten sollen.

Dies ist positiv zu bewerten. Die einzelnen aufgezählten Maßnahmen geben dem Rechtsanwender eine Idee, welche konkreten Anforderungen an die IT-Sicherheit seines Telemedienangebotes gestellt werden.
Dennoch sind auch an dieser Stelle einige Kritikpunkte hervorzuheben: Zum einen ist die Liste oberflächlich und deshalb eher als erster Anhaltspunkt brauchbar. Die Auflistung kann höchstens eine Art Checklistenfunktion einnehmen. Zum anderen ist zu bemängeln, dass die Verweise den Ratsuchenden nicht zu einer konkreten Maßnahme führen. Es ist sinnvoll, mit Verweisen zu arbeiten, da hier die Aktualität eines solchen Papiers länger gewährleistet bleibt. Der Leser wird aber dazu gezwungen, sich selbst die entsprechenden Informationen aus dem Grundschutz-Katalog herauszufiltern bzw. den weiteren Verweisen - zum Beispiel auf TRs - zu folgen und dort weiterzusuchen. Er wird oftmals innerhalb der Verweise nicht geführt, sondern muss sich selbst zurechtfinden und eigene (Zwischen-)Entscheidungen treffen. Damit wird die Auflistung und Erläuterung notwendiger Maßnahmen trotz ihrer Oberflächlichkeit sehr unhandlich und anwenderunfreundlich.

Eine systematische, zielführende und dabei konkrete Ausarbeitung technischer Maßnahmen ist zum Beispiel die Handreichung zum "Stand der Technik" im Sinne des IT-Sicherheitsgesetzes von TeleTrusT - Bundesverband IT-Sicherheit e.V.[8]

Zudem stellt sich die Frage, deren positive Beantwortung die Stellungnahme des BSI zwar offensichtlich voraussetzt, aber tatsächlich nicht begründet wird, warum der IT Grundschutz-Katalog und die Technischen Richtlinien des BSI sowie die anderen Referenzen tatsächlich den "Stand der Technik" widerspiegeln sollten. Die Herleitung oder Ermittlung bleibt dem Leser verborgen. Es darf auch nicht der Fehler begangen werden, dies ohne Begründung einfach vorauszusetzen. In der Gesetzesbegründung des § 13 Abs. 7 TMG heißt es: "Authentifizierungsverfahren nach den entsprechenden aktuellen und veröffentlichten Technischen Richtlinien des

[4] Hierzu und zum Folgenden vgl. Bartels/Backer, ITSiG-konforme Telemedien, DuD 2016, S. 22 ff. (26)
[5] Vgl. dazu Michaelis, Der "Stand der Technik" im Kontext regulatorischer Anforderungen, DuD 2016, S. 458 ff.
[6] Die englische Fassung "State of the Art" lässt dies begrifflich leichter fassen.
[7] BT Drs. 18/4096, S. 34
[8] Abrufbar unter https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

BSI sind dabei jedenfalls als dem Stand der Technik gemäß hinreichend sicher anzusehen."[9] Daraus geht im Wege des Umkehrschlusses hervor, dass nicht schlechthin und bereichsübergreifend davon auszugehen ist, dass die TR des BSI und auch nicht der IT-Grundschutz Katalog unkritisch als "Stand der Technik" ausgewiesen werden können. Vor diesem Hintergrund wäre es wünschenswert, den Leser und Anwender transparent und nachvollziehbar in die Vorüberlegungen einzubeziehen und deutlich zu machen, aus welchen Ermittlungen und Analysen heraus der/ die jeweiligen IT-Grundschutz-Katalog oder TR als "Stand der Technik" erachtet werden.

Für einen etwas weiteren Blickwinkel als bisher von dem Papier eingenommen, spricht auch die Gesetzesbegründung für § 8a BSIG. Für die Bestimmung des Standes der Technik wird hier gefordert, insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen und vergleichbare Verfahren, Einrichtungen und Betriebsweisen zu analysieren, die sich in der Praxis erprobt haben.[10] Dieser Hinweis könnte vom BSI dahingehend für die Auslegung des § 13 Abs. 7 S. 2 TMG umgesetzt werden, nicht ausschließlich den Katalog und die Richtlinien des BSI selbst zu nennen, sondern ebenfalls internationale und europäische Normen und Verfahren einzubeziehen und auszuwerten. Gerade die technologische Entwicklung sowie auch die Angriffe, vor denen geschützt werden soll, machen nicht an der Landesgrenze halt, so dass ein internationaler Ansatz wünschenswert wäre.

Im Rahmen der konkreten Maßnahmen wäre es zudem wichtig, darauf einzugehen, dass das Gesetz selbst in § 13 Abs. 7 S. 3 TMG als Maßnahme im Sinne des Satzes 1 insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens nennt. Als einzige Maßnahme auf die gesetzliche Ebene gehoben, müsste diesem Punkt in der Ausarbeitung des BSI ebenfalls eine eigene Bedeutung zukommen.

5 Grenzen der Pflichten

Auch wenn das Hauptaugenmerk der Ausarbeitung des BSI auf der Konkretisierung des Terminus‘ "Stand der Technik" liegt, so müsste sie dennoch aus systematischen Erwägungen auch eine Stellungnahme zu den Grenzen im Rahmen der Verhältnismäßigkeitsprüfung enthalten.

§ 13 Abs. 7 TMG begrenzt die Verpflichtung der Telemedienanbieter, technische und organisatorische Vorkehrungen zu schaffen, in dreifacher Weise: Zunächst ist der Stand der Technik "zu berücksichtigen" und "soll" nicht wie bei § 8a BSIG "eingehalten werden". Was darunter zu verstehen ist, also wann der Stand der Technik bewusst unterschritten werden darf, weil er berücksichtigt, aber nicht eingehalten wurde, ist für die Adressaten der Norm äußerst relevant. Es ist davon auszugehen, dass die Regelung so gemeint ist, dass ein "Berücksichtigen" dann anzunehmen ist, wenn der Stand der Technik in die Bewertung der technischen oder organisatorischen Vorkehrungen einbezogen wird, ohne dass jede dem Stand der Technik entsprechende Vorkehrung tatsächlich umgesetzt wird.[11] An dieser Stelle wäre es praxisrelevant, durch ein paar konkretisierende Ausführungen die Rechtsunsicherheit und Unklarheit etwas einzudämmen.

Weiterhin sind die Anbieter von Telemedien zur Anwendung der ermittelten technischen und organisatorischen Vorkehrungen nur verpflichtet, soweit dies technisch möglich und wirtschaftlich zumutbar ist, § 13 Abs. 7 S. 1 TMG.[12] Auch hierzu ist eine Stellungnahme des BSI deshalb unabdingbar, weil es für die Adressaten gerade nicht ausreicht, zu erfahren, welche Verschlüsselungsmethode (zu diesem Zeitpunkt) dem Stand der Technik entspricht, sondern er einen Leitfaden oder eine Anleitung benötigt, zu ermitteln, ob er diese Verschlüsselung auch tatsächlich für seinen Telemediendienst umsetzen muss oder dies etwa im Einzelfall als unverhältnismäßig bewertet werden darf. Die Verhältnismäßigkeitsgrenzen des § 13 Abs. 7 TMG werden für viele Unternehmen, vor allem kleiner und mittlerer Größe, sogar als das Maß der Dinge zu bezeichnen sein. Es wird die zentrale Frage darstellen, unter welchen Voraussetzungen vom objektiv zu bestimmenden Stand der Technik, der - wie oben herausgearbeitet - das beste und effektivste Schutzniveau meint, welches auf dem Markt erhältlich ist, nach unten aus subjektiven Gründen (technische subjektive Unmöglichkeit und wirtschaftliche Zumutbarkeit) abgewichen werden kann.

In diesem Zusammenhang wären aus praktischer Sicht ebenfalls Ausführungen zu einer Dokumentation der Umsetzung/ Unterlassung bestimmter technischer und organisatorischer Maßnahmen hilfreich. Aus dem Gesetz geht eine solche Dokumentationspflicht der Telemediendienste zwar nicht hervor; auf Grund der Fülle der Einzelmaßnahmen und Maßnahmenbündel kann jedoch ohne eine Dokumentation eine eventuelle Kontrolle

[9] BT Drs. 18/4096, S. 34
[10] BT Drs. 18/4096, S. 26
[11] Siehe ausführlich Bartels/Backer, ITSiG-konforme Telemedien, DuD 2016, S. 22 ff. (27).
[12] Ausführlich zur Auslegung der technischen Möglichkeit und wirtschaftlichen Zumutbarkeit siehe Bartels/Backer, ITSiG-konforme Telemedien, DuD 2016, S. 22 ff. (27)

nicht bewältigt werden. Sie stellt deshalb vielmehr eine Obliegenheit für den Anbieter dar.[13] Insbesondere die Auseinandersetzung mit Fragen zur Tiefe oder Detailliertheit der Dokumentation im Falle einer eventuellen Kontrolle wären wünschenswert.

Ansprechpartner für Rückfragen:

Rechtsanwalt Karsten U. Bartels LL.M.,
TeleTrusT - Bundesverband IT-Sicherheit e.V.
Mitglied des Vorstandes
Leiter der TeleTrusT-AG "Recht"

[13] Bartels/Backer, ITSiG-konforme Telemedien, DuD 2016, S. 22 ff. (28)