Das Sprachrohr für 1.000 IT-Mittelständler

BITMi Stellungnahme zum

Referentenentwurf des Bundesministeriums des Innern zum "Entwurf eines Gesetzes zur Erhöhung der Sicherheit Informationstechnischer Systeme (IT-Sicherheitsgesetz)“

Bundesverband IT-Mittelstand e.V.
Augustastrasse 78, 52070 Aachen
www.bitmi.de

Bundesverband
IT-Mittelstand e.V.

Zusammenfassung des Gesetzes:

Mit dem IT-Sicherheitsgesetz soll die IT-Infrastruktur der Bundesrepublik Deutschland auf Bundesebene besser gegen Hackerangriffe vorbereitet werden und es sollen Strukturen eingerichtet werden, die schnellere Reaktionen auf Hackerangriffe und Datendiebstahl ermöglichen.

Darüber hinaus soll außerdem der Schutz sog. „kritischer Infrastrukturen“ verbessert werden. Die daraus abgeleiteten Forderungen gelten damit auch für die Betreiber der „kritischen Infrastrukturen“ in der Wirtschaft, sowie durch einige Spezialregelungen für die IT-Wirtschaft in Deutschland.

Deswegen soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit zusätzlichen Kompetenzen ausgestattet werden und der Informationsaustausch zwischen dem BSI, der Bundesnetzagentur (BNetzA) und den Betreibern sog. „kritischer Infrastrukturen“ (KRITIS) verbessert werden.

Durch das IT-Sicherheitsgesetz werden Änderungen im BSI-Gesetz, im Telemediengesetz (TMG), im Telekommunikationsgesetz (TKG), im Außenwirtschaftsgesetz (AWG), sowie im Gesetz über das Bundeskriminalamt […] (BKA-Gesetz) durchgeführt.

Bedeutung des Gesetzes für den deutschen IT-Mittelstand

Durch das IT-Sicherheitsgesetz entsteht der deutschen IT-Wirtschaft – und hier insbesondere dem deutschen IT-Mittelstand – ein nicht näher quantifizierbarer organisatorischer und personeller Aufwand.

Bewertung des Gesetzes

Mit der Veröffentlichung eines überarbeiteten Referentenentwurfs des IT-Sicherheitsgesetzes möchte die Bundesregierung, insbesondere das Bundesministerium des Innern, die Reaktionsfähigkeit Deutschlands auf Hackerangriffe und Datendiebstahl verbessern.

Die Absicht, Bürger, Wirtschaft und den Staat besser vor digitalen Übergriffen zu schützen und digital bedingte Verwundbarkeiten zu reduzieren, erkennt der BITMi als ein begrüßenswertes Ziel der Bundespolitik an. Auch der grundsätzliche Ansatz des Bundesministeriums des Innern (BMI), auf eine großflächige Regulierung zu verzichten und den Schwerpunkt auf systemrelevante Faktoren wie die

digitale Infrastruktur, die Gesundheitsversorgung und den Bevölkerungs- und Katastrophenschutz zu legen, hält der BITMi für grundsätzlich richtig[1].

Dennoch enthält der vorliegende Gesetzesentwurf eine Reihe von Formulierungen, die aus Sicht des BITMi weitere Verbesserungen im Zuge der Ressortabstimmung sowie im parlamentarischen Verfahren erforderlich machen.

1. **Kritische Infrastrukturen**

   Der vorliegende Gesetzesentwurf bezieht sich zum großen Teil auf die Betreiber kritischer Infrastrukturen. Diese werden allerdings nicht im Gesetz selbst dargelegt oder beschrieben, sondern es wird auf eine noch vom BMI zu erlassende Ordnung verwiesen (IT-Sicherheitsgesetz RefE, Artikel 1 Abs. 2 und 9). Es wird lediglich auf *„Anlagen […] bzw. Teile von Anlagen der Bereiche Energie, Informationstechnik, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, sowie Finanz- und Versicherungswesen“* verwiesen, *„die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind.“*

   Die hier getroffene Aussage lässt den Kreis der betroffenen Wirtschaftsbereiche ebenso im Unbestimmten, wie die Tiefe, die eine solche Regulierung besitzt. Der Geltungsbereich und die Verbindlichkeit von Regulierungen, die mit diesem Gesetz getroffen sind, schafft für den deutschen IT-Mittelstand ein enormes Maß an Unsicherheit.

2. **Berichtspflichten und Anpassung von Strukturen:**

   Betreiber kritischer Infrastrukturen werden mit dem vorliegenden Gesetz dazu verpflichtet, für einen angemessenen Schutz der kritischen Infrastruktur zu sorgen (IT-Sicherheitsgesetz RefE, Artikel 1 Abs. 8). Dabei sollen sie die Verhältnismäßigkeit ihrer Mittel berücksichtigen. Auch hier zeigt sich eine erhebliche Unschärfe bei den gesetzlichen Vorgaben, die zu einer nachgelagerten Unsicherheit und vermutlich einer letzten Endes gerichtlich auszutragenden Debatte für die Betreiber kritischer Infrastrukturen führen wird. Darüber hinaus enthält dieser Passus enormes Diskriminierungspotential für kleine und mittelständische IT-Unternehmen, die in ihrer Personal- und Ressourcenplanung nicht immer mit großen, am Markt etablierten Anbietern von Software konkurrieren können. Ein Vorschlagrecht für die Betreiber und deren Branchenverbände mag hier vielleicht etwas Abhilfe schaffen und die Hoffnung wecken, dass

[1] Eine entsprechende Bemerkung enthält die Begründung des Gesetzesentwurfs.

Anforderungen konkretisiert werden. Da diese jedoch für die umsetzenden Behörden nicht bindend sind, bleibt auch hier viel Raum für Spekulationen.

Die zusätzlich auferlegte Berichtspflicht für Betreiber kritischer Infrastrukturen alle (mindestens) zwei Jahre (vgl. IT-Sicherheitsgesetz Art. 1 Abs. 8) ist mit Blick auf die Aktualität, Schnelllebigkeit und die Lebenszyklen von insbesondere Software aus Sicht des BITMi vor allem eine unnötige bürokratische Maßnahme, welche den Betreibern von KRITIS zusätzliche Berichtspflichten auferlegt und beim BSI zusätzlichen Arbeits- und Personalaufwand generiert. Die pauschale Regelung von (mindestens) zwei Jahren wird den einzelnen Bereichen von KRITIS wie Maschinenteilen, Computerhardware, Software und deren spezifischen Wartungs- und Lebenszyklen nicht gerecht.

3. Einrichtung einer zentralen Meldestelle für Störungen in KRITIS

Um die Kommunikation zwischen den Bundesbehörden und den Betreibern von KRITIS zu gewährleisten, soll eine zentrale Meldestelle beim BSI eingerichtet werden. Grundsätzlich ist eine solche Meldestelle für die Betreiber von KRITIS als zentraler Ansprechpartner begrüßenswert. Konkrete Schwierigkeiten ergeben sich an dieser Stelle vor allem durch die Einrichtung von Kommunikationsstrukturen, die eine 24/7 Verfügbarkeit eines Ansprechpartners der KRITIS erfordert. Dieser Passus beinhaltet Diskriminierungspotential für kleine und mittelständische IT-Unternehmen, die ggf. nicht die personellen Ressourcen vorhalten können, um eine solche Erreichbarkeit zu gewährleisten. Auch ist hier fraglich, ob eine solche Erreichbarkeit tatsächlich zwingend notwendig ist, oder ob die Benachrichtigung auf einer „Need-to-Know“ Basis auch bspw. rechtzeitig vor Wartungs- oder Reperaturzyklen erfolgen kann und daher die 24/7 Erreichbarkeit der Ansprechpartner nicht zwingend gewährleistet sein muss. Auch der Umstand, dass so genannte „Kleinstunternehmen“ (bis 10 Mitarbeiter und maximal 2 Mio. Euro Umsatz) von der Meldepflicht ausgenommen sind, vereinfacht die Situation speziell für diese Unternehmen nur bedingt, da sie durch die Abgabe von Erklärungen mit zusätzlichem bürokratischen Aufwand belastet werden.

4. Einführung einer Meldepflicht für Störungen in KRITIS

Die durch den vorliegenden Referentenentwurf angedachte „anonymisierte“ Meldepflicht für die Betreiber KRITIS, sowie den Schutz vor Auskunft gegenüber Dritten (geregelt. Durch Art. 1 Abs. 8) sieht der BITMi vor dem Hintergrund der Ausführungen in „3. Einrichtung einer zentralen Meldestelle für Störungen in KRITIS“ entsprechend kritisch. Darüber hinaus hinterfragt er den Sinn einer solchen Meldepflicht, die primär der Erstellung eines Lagebildes

zu dienen scheint und weniger darauf abzielt, IT-Infrastrukturen vor Angriffen zu schützen. Hier stellt sich die Frage, ob durch die Meldepflicht nicht wichtige Unternehmensressourcen, die für die Abwehr eines Angriffs oder die Beseitigung einer Störung benötigt werden, auf den Austausch mit anderen Stellen genutzt werden müssen. Zuguterletzt bezweifelt der BITMi, dass im Falle der Meldung einer Störung und der damit verbundenen Berichtspflicht des BSI die Anonymität der Meldung und damit letzten Endes die Integrität der beteiligten Unternehmen tatsächlich gewährleistet werden kann. Dies gilt umso mehr für kleine Marktsektoren, auf denen nur sehr wenige spezialisierte Anbieter aktiv sind. Der BITMi hat bereits in der Vergangenheit deutlich zum Ausdruck gebracht, dass er sowohl die Meldepflicht als auch die damit einhergehenden Ansprechpartner ablehnt. Er hält trotz einiger vordergründiger Verbesserungen im Gesetzestext an dieser Position fest.

5. Schutzmaßnahmen von IT-Angeboten durch kommerzielle Anbieter

In Artikel 2 des IT-Sicherheitsgesetzes wird darauf abgehoben, dass *„Diensteanbieter im Sinne von §7 Absatz 1 und § 10 Absatz 1 [des TMG]“* für *„geschäftsmäßig in der Regel gegen Entgelt angebotene Telemedien“* durch *„erforderliche technische und organisatorische Vorkehrungen“* gewährleisten sollen, dass der Zugriff *auf „Telekommunikations- und Datenverarbeitungssysteme nur für Berechtigte“* möglich ist, *„soweit dies technisch möglich und zumutbar“* ist.

Dieser Passus enthält gleich mehrere problematische Formulierungen und unbestimmte Rechtsbegriffe, die für erhebliche Rechtsunsicherheit bei IT-Mittelständlern und Startups sorgen.

Durch die Formulierung *„geschäftsmäßig in der Regel gegen Entgelt“* wird ein Bezug zu kommerziellen Diensten, die Daten erheben, speichern oder verarbeiten hergestellt. Allerdings wird durch die Erweiterung um die Entgeltfrage dieser Bereich nahezu unbegrenzt ausgeweitet, so dass der tatsächliche Geltungsbereich dieses Passus sowohl für Unternehmen als auch für Privatpersonen ein enormes Maß an Unsicherheit mit sich bringt. Vor allem vor dem Hintergrund der Frage, ob der Betreiber des Telemediendienstes auch der Anbieter der IT-Infrastruktur ist, besteht an dieser Stelle ein erhebliches Maß an Rechtsunsicherheit speziell für Unternehmen im Onlinebereich.

Auch die Regelung des Zugriffs für Berechtigte durch organisatorische und technische Maßnahmen im Rahmen der Zumutbarkeit schafft enorme Rechtsunsicherheit für Anbieter von Diensten und Software. Es wird einerseits dabei außer Acht gelassen, dass für bestimmte

Angebote – insbesondere im Öffentlichen Sektor – bereits heute sehr präzise Vorgaben für Zugriffs- und Administrationsrechte, sowie gesetzliche Vorgaben wie das Bundesdatenschutzgesetz (BDSG) bestehen, die den Anbietern entsprechender Dienste bspw. DE-Mail enormen bürokratischen und technischen Aufwand verursachen. Andererseits wird durch die Zumutbarkeitsklausel ein möglicher Klageweg neben dem in der Regel bei Diensten bestehenden Vertragsverhältnis zwischen Nutzern und Anbietern eröffnet, der insbesondere für kleine und mittelständische IT-Unternehmen und Startups von enorm schädlicher Wirkung für die Etablierung am Markt oder die Erprobung neuer Geschäftsmodelle sein kann.

Zuguterletzt bleibt an dieser Stelle offen, inwieweit der vorliegende Paragraf im Referentenentwurf mit den sehr konkreten Vorgaben aus der EU-Datenschutzrahmenrichtlinie zum Umgang mit personenbezogenen Daten (Verschlüsselung) Rechnung trägt. Hier sind sehr detaillierte Regeln für KMU, Großunternehmen beschrieben, welche Maßnahmen und Berichtspflichten zum Schutz und zur Verarbeitung personenbezogener Daten getroffen werden müssen, sowie welche Meldepflichten im Falle eines Verlusts bestehen. Der Referentenentwurf des IT-Sicherheitsgesetzes geht aus Sicht des BITMi weit über die von der EU vorgeschriebenen Maßgaben hinaus.

Der BITMi lehnt die vorliegende Ergänzung des TMG um diesen Paragrafen ab.

6. **Mitteilungspflicht über Störung in Telekommunikationsdiensten**

Das IT-Sicherheitsgesetz regelt außerdem die Berichtspflichten über aufgetretene Störungen in Kommunikationsnetzen neu.
Kritisch zu betrachten ist hier die Berichtspflicht bei Störungen von Telekommunikationsdiensten, die möglicherweise den unerlaubten Zugriff auf Nutzerdaten ermöglichen. Durch die fakultative Formulierung besteht das Risiko eines inflationären Einsatzes der Alarmmeldung. Darüber hinaus ist hier die anonymisierte Meldung nicht vorgesehen. Ein Schaden in der Reputation des Access Providers mithin nicht vermeidbar. Der BITMi lehnt diese Regelung daher als nicht sinnvoll ab.
Darüber hinaus soll der Betreiber eines Telekommunikationsdienstes den Nutzer darüber in Kenntnis setzen, wenn von dessen Rechner eine Störung des Dienstes ausgeht. Dies setzt voraus, dass der Diensteanbieter seinen Nutzer kennt und ggf. auch über eine geeignete Kontaktmöglichkeit verfügt. Die Anbietung von anonymen Diensten ist somit nicht mehr möglich. Dies könnte sich negativ auf das Innovationspotential der deutschen IT-Wirtschaft im Bereich der Datensicherheit auswirken. Der BITMi lehnt diese Regelung daher ab.

Zusammenfassung und Fazit

Insgesamt enthält das IT-Sicherheitsgesetz sehr viele unbestimmte Rechtsbegriffe und Unklarheiten, die für den deutschen IT-Mittelstand das Risiko rechtlicher Schritte gegen die Unternehmen ermöglichen bzw. den Unternehmen mögliche Berichtspflichten auferlegen, die für große Unsicherheit sorgt. Darüber hinaus stellt dieses Gesetz einen nationalen Alleingang dar, der sich in Zukunft und insbesondere bei der genaueren Ausgestaltung der Regeln durch die Verordnung des BMI zu einer doppelten Belastung für den international tätigen IT-Mittelstand erweisen könnte. Dies gilt insbesondere für die neu eingeführten Melde- und Berichtspflichten, sowie für die Schaffung von Strukturen, die das IT-Sicherheitsgesetz zwingend vorschreibt.

Vor diesem Hintergrund fordert der BITMi:

- Die Harmonisierung des Gesetzgebungsprozesses um das IT-Sicherheitsgesetz mit der korrespondierenden Richtlinie der Europäischen Union über „Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union“ (KOM 2013/48) und deren gemeinsame Implementierung. Die stärkere Berücksichtigung der geplanten EU-Datenschutz-Grundverordnung im Bereich des Telemedien- und Telekommunikationsgesetzes.

- Die Vermeidung der doppelten Belastung des deutschen IT-Mittelstands durch doppelte Berichts- und Meldepflichten.

- Die genaue Überprüfung über Anforderungen an Strukturen in KRITIS und die Berücksichtigung der branchen- und wirtschaftlich bedingten Rahmenbedingungen für die Betreiber.

- Die Rücknahme rechtlich unpräziser Auflagen über angenommene Datenverluste und zumutbare Maßnahmen in TKG und TMG