Leipzig, den 22.04.2015

Stellungnahme des Händlerbundes e.V.

zum

Regierungsentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Die Mitglieder des Händlerbundes e.V. als größtem Onlinehandelsverband Europas sind von dem Regierungsentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) betroffen. Deshalb nimmt der Verband nachstehend Stellung:

Grundsätzlich wird die mit dem Gesetzentwurf beabsichtigte Verbesserung der Sicherheit informationstechnischer Systeme positiv bewertet, soweit diese zu einem besseren Schutz vor digitalen Übergriffen auf Bürger, Unternehmen und staatliche Stellen führt. Denn externe Sicherheitsrisiken haben zuletzt massiv zugenommen und dazu geführt, dass rund zwei Drittel aller deutschen Unternehmen bereits Opfer von Cyber-Attacken geworden sind.
Abgesehen davon besteht allerdings besonders im Bereich der vorgeschlagenen Änderung des Telemediengesetzes erheblicher Nachbesserungsbedarf, da die aktuelle Fassung des Entwurfs zu einer unangemessenen Verlagerung der Haftung auf die Telemedienanbieter führt. Zudem bedarf es der Klarstellung bei einer Reihe unbestimmter Rechtsbegriffe und vorgesehener Berichtspflichten. Dies wird der Händlerbund e.V. im Folgenden darlegen.

Zum Gesetzestext und der Begründung zu der mit Artikel 1 vorgesehenen Änderung des BSI-Gesetzes

Mit dieser Norm soll § 2 des BSI-Gesetzes ein neuer Absatz 10 beigefügt werden. Dieser hat folgenden Wortlaut:

„(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die
1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.
Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt. Kommunikationstechnik im Sinne des Absatzes 3 *gehört nicht zu den Kritischen Infrastrukturen im Sinne dieses Gesetzes.“*

Problematisch ist in diesem Zusammenhang zunächst die Frage, was im Einzelnen unter den unbestimmten Rechtsbegriff der „kritischen Infrastrukturen“ zu subsumieren ist. Denn diese werden im Gesetzentwurf selbst nicht definiert, sondern sollen erst im Nachhinein durch ministerielle Verordnung konkretisieret werden. Auch die Auflistung der relevanten Wirtschaftsbereiche, in denen an solche Infrastrukturen angeknüpft werden soll, hilft bei der

Konkretisierung nicht weiter. Dies ist schon wegen der erheblichen Berichts- und Sicherungspflichten, die den Betreibern „kritischer Infrastrukturen“ zugewiesen werden, nicht hinnehmbar und sollte im Zuge der weiteren Bearbeitung des Referentenentwurfs durch das Bundesministerium des Inneren unbedingt korrigiert werden. Eine möglichst konkrete Ausgestaltung dient der Rechtssicherheit und ist für eine transparente Anwendung des Gesetzes durch die Unternehmen der Digitalen Wirtschaft unerlässlich. Die konkrete Definition des Begriffes „kritischer Infrastrukturen“ im Gesetz ist deshalb unbedingt erforderlich und könnte unter anderem z.B. auf die Größe der Infrastruktur, den Zweck der Infrastruktur, die Anzahl der User der Infrastruktur und/oder die Art der Daten, die mit der Infrastruktur gespeichert werden, Bezug nehmen.

Darüber hinaus sollen mit dem neu einzuführenden § 8a des BSI-Gesetzes eine Reihe von Schutz- und Berichtspflichten eingeführt werden. Die Norm hat folgenden Wortlaut:

„(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei ist der Stand der Technik zu berücksichtigen. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.
(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten.
(3) Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und, soweit erforderlich, im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.“

Der vorgeschlagene Gesetzestext macht deutlich, dass Betreiber kritischer Infrastrukturen dazu verpflichtet werden, für einen angemessenen Schutz dieser Infrastruktur zu sorgen. Dies wird unter den Vorbehalt der Verhältnismäßigkeit gestellt. Damit werden auch hier erhebliche Unschärfen in der Formulierung des Gesetzestexts deutlich, die in der Konsequenz zu einer Klärung durch die Gerichte führen werden. Darüber hinaus birgt die Regelung die Gefahr, dass besonders kleine und mittlere Unternehmen der Digitalen Wirtschaft im Verhältnis zu großen Unternehmen benachteiligt werden – denn diesen stehen erheblich Mittel zur Erfüllung der Sicherungs- und Berichtspflichten zur Verfügung als kleineren Marktteilnehmern. Dieses Problem wird auch nicht dadurch entschärft, dass den Branchenverbänden das Recht zuerkannt wird, spezifische Standards für organisatorische und technische Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme vorzuschlagen. Diese Vorschläge sind nämlich für die mit der Überprüfung dieser Maßnahmen betrauten Behörden nicht bindend.

Zum Gesetzestext und der Begründung zu der mit Artikel 2 vorgesehenen Änderung des Telemediengesetzes (TMG)

Mit dieser Norm soll zunächst in § 13 TMG ein neuer Absatz 7 eingefügt werden. Dieser hat folgenden Wortlaut:

„(7) Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass
1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und
2. diese
a) gegen Verletzungen des Schutzes personenbezogener Daten und
b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.“

Mit dieser Norm sollen Diensteanbieter von Telemedien einerseits erforderliche technische und organisatorische Vorkehrungen ergreifen, um Zugriffe Unberechtigter auf TK- und DV-Anlagen zu vermeiden. Zum anderen sollen personalisierte Telemediendienste mit sicheren Authentifizierungsverfahren angeboten werden. Auffallend ist auch hier die Häufung unbestimmter Rechtsbegriffe, die kaum geeignet sein wird, in der Unternehmenspraxis eine rechtssichere Anwendung des Gesetzes zu gewährleisten. Aus diesem Grund ist auch hier eine Konkretisierung des Texts geboten.

Davon abgesehen ist allerdings die in § 13 Abs. 7 TMG n.F. in der hier vorgeschlagenen Fassung enthaltene Verlagerung der Verantwortlichkeit auf den Diensteanbieter unverhältnismäßig und ist daher abzulehnen. Im Ergebnis sollen die Unternehmen nämlich sicherstellen, dass nicht nur über eigene Inhalte, sondern auch über externe Inhalte Dritter – etwa Online-Werbung – keine Schadsoftware transportiert werden kann. In der Konsequenz bedeutet dies, dass der Diensteanbieter dafür einzustehen hat, dass auf diesem Weg weder direkt noch indirekt oder durch weitere Verlinkung potentiell gefährliche Inhalte oder Schadsoftware zugänglich sind. Diese Form der umfassenden Ergebnisverantwortlichkeit des Diensteanbieters geht haftungsrechtlich zu weit – und ist technisch kaum durchzusetzen.

Daran ändert auch die in der Gesetzesbegründung kundgetane Einsicht der Entwurfsverfasser nichts, wonach kompromittierende Inhalte auch über Werbebanner transportiert werden können, die über Affiliate-Netzwerke ausgespielt werden. Diese Ausspielung ist Teil eines hochkomplexen technischen Verfahrens, das integraler Teil der Wertschöpfungskette ist und auf das der Diensteanbieter kaum Einfluss hat – und dies unabhängig davon, ob er ein Medienangebot, eine Partnerbörse oder einen Online-shop betreibt.

Die in der Gesetzesbegründung vorgeschlagene Lösung, wonach das Unternehmen etwa mit vertraglichen Schutzklauseln oder technischen Schutzmaßnahmen, absichern solle, wird dem gesetzten Haftungstatbestand nicht gerecht. Auch ein Unternehmen, das sich beispielsweise von Affiliate-Netzwerken oder einem Werbetreibenden vertraglich zusichern lässt, dass die geschaltete Werbung selbst keine kompromittierenden Inhalte enthält, bleibt angesichts der gewählten Formulierung in § 13 Abs. 7 Satz 1 TMG n.F. im Ergebnis haftbar,

wenn die vertragliche Zusicherung durch den Verantwortlichen der Werbung nicht eingehalten wird. Der Shop-Betreiber wird damit einerseits in eine Ergebnishaftung genommen, andererseits sind die Möglichkeiten den Risiken wirksam entgegenzutreten, höchst begrenzt.

Die vorgesehene Risikoverlagerung auf den Diensteanbieter ist daher auch aus diesem Grund abzulehnen und sollte entsprechend geändert werden.

Über den Händlerbund e.V.

Als größter Onlinehandelsverband Europas ist der Händlerbund Sprachrohr und Partner der E-Commerce-Branche. Der Verband fördert den Austausch zwischen Händlern und Dienstleistern, um den digitalen als auch stationären Handel nachhaltig zu unterstützen und zukunftsfähig auszurichten. Durch die europaweite Interessenvertretung und Bündelung verschiedener Dienstleistungen gestaltet der Händlerbund mit seinen Mitgliedern und Partnern aktiv die Branche.
Ihr Ansprechpartner: Florian Seikel, florian.seikel@haendlerbund.de