Stellungnahme

der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

I. Ausgangslage und Ziele:

Das Bundesministerium des Innern hat seinen Referentenentwurf für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme Mitte August vorgestellt.

Der Gesetzesentwurf konkretisiert und erweitert, den bereits im Koalitionsvertrag zur 18. Legislaturperiode vereinbarten Grundgedanken Mindestanforderungen an die IT-Sicherheit für kritische Infrastrukturen zu schaffen und eine Verpflichtung zur Meldung erheblicher IT-Sicherheitsvorfälle einzuführen. Erklärtes Ziel ist die weltweite Führungsrolle in Bezug auf die Sicherheit von IT-Systemen und digitalen Strukturen in Deutschland, ohne den Schutz der Bürgerinnen und Bürger aus dem Blickfeld zu verlieren.

Vor dem Hintergrund der Tatsache, dass wesentliche Teile unseres Gemeinwesens miteinander vernetzt sind, Arbeits- und Geschäftswelt von der Funktionsfähigkeit der IT und des Internet abhängen, begrüßt die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. das Vorhaben der Bundesregierung generell, sowohl die Resilienz als auch die Schutzmaßnahmen bei den Betreibern kritischer Infrastrukturen durch Kooperation und gesetzliche Vorgaben weiter zu verbessern und auch die Sensibilisierung für die IT-Sicherheit bei den Bürgerinnen und Bürgern voranzutreiben.

Der Entwurf sieht Änderungen in fünf verschiedenen Themenfeldern vor:

1. **Verbesserung der IT-Sicherheit bei Unternehmen - insbesondere bei kritischen Infrastrukturen**
2. **Schutz der Bürgerinnen und Bürger in einem sicheren Netz**
3. **Schutz der IT des Bundes**

4. **Stärkung des BSI**

5. **Zuständigkeitserweiterung des BKA**

II. Bewertung

1. Klare Adressierung erforderlich

Nach einer gem. § 2 Abs. 10 BSIG-E i.V.m § 10 Abs. 1 BSIG-E noch zu erlassenden Rechtsverordnung soll bestimmt werden, welche Einrichtungen, Anlagen oder Teile davon in den genannten Sektoren der Regulierung unterliegen.
Betreiber Kritischer Infrastrukturen sollen verpflichtet werden, binnen zwei Jahren nach Inkrafttreten dieser Rechtsverordnung angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen zum Schutz derjenigen informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Diese Vorkehrungen sollen dann mindestens alle zwei Jahre hinsichtlich der Erfüllung der Anforderungen einer Überprüfung unterzogen werden. Das Gesetz spricht insoweit von der Möglichkeit, die Anforderungen auf geeignete Weise nachzuweisen.

Als gangbare Möglichkeit werden Sicherheitsaudits, Prüfungen und Zertifizierungen genannt.

Nach § 8b Abs. 5 BSIG-E sind Betreiber kritischer Infrastrukturen nur dann unter Nennung des Betreibernamens unverzüglich zu einer Meldung an das BSI verpflichtet, wenn die Beeinträchtigung der informationstechnischen Systeme, Komponenten oder Prozesse zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastruktur führen würde.

Nach § 8b Abs. 4 BSIG-E kann die Meldung durch die Betreiber kritischer Infrastrukturen anonym erfolgen, soweit die Beeinträchtigungen der informationstechnischen Systeme, Komponenten oder Prozesse, (lediglich) Auswirkungen auf ihre eigene Funktionsfähigkeit haben können. Angaben zu den technischen Rahmenbedingungen sowie zur Branche des Betreibers müssen jedoch enthalten sein.

Das IT-Sicherheitsgesetz basiert auf dem Konzept, dass derjenige, der durch den Einsatz von IT, Risiken für andere schafft, auch die Verantwortung für den Schutz vor diesen Risiken trägt. Bislang existiert aber eine Unschärfe bezüglich der Adressaten dieser Regelung, so dass die Frage der Verantwortung unklar bleibt.

Die Absätze 10 und 11 des § 2 BSIG-E versuchen zwar eine Legaldefinition des Begriffs „kritische Infrastrukturen“ und des Begriffs „Betreiber kritischer Infrastrukturen“ aufzustellen, jedoch bleibt im Sinne einer besseren Planungssicherheit für die möglicherweise betroffenen Unternehmen die Forderung, dass die Änderung des § 10 BSIG-E unmissverständlich aufzeigen muss, welche Unternehmen unter diesen Begriff zu subsumieren sein werden.

Forderung:

Die Adressaten der Meldepflicht müssen eindeutig feststehen.

2. Rechtsunsicherheit durch Doppelvorschriften vermeiden

In der Koalitionsvereinbarung sprach sich die Bundesregierung für eine europäische Sicherheitsstrategie und die Gestaltung der Internet-Infrastruktur zu einem deutsch-europäischem „Vertrauensraum“ aus.

In wie weit ein nationales IT-Sicherheitsgesetz mit dem auf europäischer Ebene vorgestellten Richtlinienentwurf („NIS-Richtlinie“), dessen Ziel die Verbesserung der Netzwerk und Informationssicherheit in der EU ist, harmonisiert werden kann und muss, ist ein weiterer Aspekt dem Beachtung geschenkt werden sollte.

Forderung:

Nationale Regelungen zur IT-Sicherheit sollten mit langfristig angestrebten europäischen Regelungen mit ähnlichen Zielvorstellungen im Einklang stehen. Die Rechtsunsicherheit vergrößernde Doppelvorschriften sollten vermieden werden.

3. Verwendungsverbot für Meldungen

Nach § 8b Abs. 5 BSIG-E hat im Falle einer Beeinträchtigung der informationstechnischen Systeme oder im Falle der Beeinträchtigung der kritischen Infrastruktur unverzüglich eine Meldung an das BSI zu erfolgen. Diese Meldung wird durch den Betreiber der kritischen Infrastruktur über die Warn- und Alarmierungskontakte unter Nennung des Betreibers erstattet.

Hierbei hält die GDD eine strikte Zweckbindung und ein Verwendungsverbot mit Fernwirkung ähnlich § 42a Satz 6 BDSG für erforderlich. Die Freiheit, sich selbst nicht bezichtigen zu müssen, besitzt Verfassungsrang und stellt eine notwendige Prämisse des Strafprozesses dar.

Aus dem sog. nemo-tenetur-Grundsatz ergibt sich das Erfordernis, in Anlehnung an § 42a S. 6 BDSG, auch im Rahmen der Benachrichtigungspflicht im Sinne des IT-Sicherheitsgesetzes eine verfassungskonforme Auslegung dahingehend zu fordern, dass die mitgeteilten Tatsachen in keiner Form für ein straf- oder ordnungswidrigkeitenrechtliches Verfahren nutzbar gemacht werden dürfen.

Das Verwendungsverbot sollte auch gelten, wenn die verantwortliche Stelle irrtümlicherweise eine Meldung abgibt, etwa weil die Kritikalität zu hoch eingeschätzt wurde.

Forderung:

Die Meldungspflicht bedarf einer verfassungskonformen Auslegung im Sinne des nemo-tenetur-Grundsatzes.

4. Bewährte Prozesse beibehalten

In § 8a Abs. 2 BSIG-E schlägt der Entwurf ausdrücklich vor, dass Betreiber kritischer Infrastrukturen und ihre Branchenverbände branchenspezifische Sicherheitsstandards vorschlagen können. Das Bundesamt erkennt die branchenspezifischen Sicherheitsstandards im Benehmen mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe auf Antrag an, wenn diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten.

Die GDD Die GDD regt an, dass auch hinsichtlich der Warn- und Meldekontakte auf branchenintern bestehende Strukturen zurückgegriffen wird, um effiziente Meldewege zu gewährleisten und über Jahre hinweg erworbene Best Practices nutzbringend einzusetzen.
Des Weiteren regt die GDD an, dass eine Evaluation und Rückmeldung der Ergebnisse an die Meldeverpflichteten implementiert wird.

Forderung:

Bewährte Best Practices weiterhin nutzen und eine Evaluation implementieren.

5. Datenschutzkonformer Umgang mit Meldedaten

Es ist aus Sicht der GDD nicht abwegig, dass mit dem geplanten Vorhaben bei allen Anbietern von Telemediendiensten Strukturen zum Vorhalten von umfangreichen Nutzerdaten geschaffen werden.
Der sich im Gesetzentwurf befindliche Gedanke, Daten von Nutzern zum Erkennen von Störungen zu erheben, trägt das Prinzip der Vorratsdatenspeicherung in sich. Die GDD sieht es daher als unabdingbar an strenge Regelungen zur Zweckbindung dieser Daten sowie eine zeitliche Befristung der Erhebung und Verwendung im Gesetz zu verankern.

Forderung:
Der datenschutzkonforme Umgang mit den anfallenden Meldedaten muss im Gesetz bedacht werden.

Eine ausführlichere Kommentierung des Entwurfs eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme finden Sie in der RDV 5/2014.

Bonn, den 11. September 2014