Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)740

Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

Die Versicherungswirtschaft begrüßt das Vorhaben der Bundesregierung, die Cyberresilienz Deutschlands zu stärken. Die zunehmende Digitalisierung von Staat, Wirtschaft und Gesellschaft baut auf Cyber- und IT-Sicherheit auf und erfordert eine Kooperation aller Akteure.

Nachfolgende Punkte zur Verbesserung des von der Bundesregierung vorgelegten Gesetzentwurfs schlagen wir vor:

Festlegen des Standes der Technik (§ 3 Absatz 1 Nummer 20)

Der Gesetzentwurf sieht vor, dass das BSI die Entwicklung des Standes der Technik bzgl. Sicherheit von IT-Produkten übernehmen soll.

Dabei ist jedoch zu bedenken:

- Der Stand der Technik entsteht durch Agieren der Entwickler, Hersteller und Nutzer und ist einer sich ständig ändernden Dynamik ausgesetzt, die der Gesetzgeber bzw. eine Behörde nicht beeinflussen sollte.
- Es gibt bereits ausreichend kompetente Akteure am Markt, die sich laufend einer Beschreibung widmen und zum Stand der Technik veröffentlichen.
- Ein festgelegter Stand der Technik könnte Hersteller und deren Produkte ausschließen, die vor dem Festlegen genutzt werden konnten. Dadurch würde nur noch die Nutzung von Produkten gewisser Hersteller ermöglicht werden.

Daher sollte der Stand der Technik nicht durch das BSI festgelegt werden, sondern vielmehr – wie in der Praxis bewährt - dessen Beschreibung durch kompetente Institutionen erfolgen und so ohne bürokratische Aufwände den aktuellen Gegebenheiten angepasst werden.

Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden (§ 7b)

Das BSI soll durch § 7b BSIG-E in die Lage versetzt werden, zur „Detektion von Sicherheitslücken und anderen Sicherheitsrisiken an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen Maßnahmen (Portscans) durchzuführen, …“.

Dabei ist jedoch zu bedenken:

- Die Sicherheit und Verfügbarkeit der Systeme könnte durch den Scan gefährdet werden, da dem BSI im Vorfeld nicht klar sein kann, wie weit es durch die Detektion in die Systeme eindringt. Zudem ist die Haftung für Schäden nicht geregelt, die durch die Detektion verursacht werden.
- Neben den Haftungsfragen muss auch geklärt werden, wie die betroffenen Betreiber im Vorfeld über Umfang, Form und Zeitraum der Detektion informiert werden, wie das BSI die Detektion nachvollziehbar dokumentiert und garantiert, dass keine Hintertür verbleibt.

Die Maßnahmen müssen sich auf das absolut Notwendige zur Detektion der Sicherheitslücken beschränken, dürfen nicht über einen Portscan hinausgehen, und eine Kompromittierung der Systeme muss ausgeschlossen sein.

Untersagung des Einsatzes kritischer Komponenten (§ 9b)

Nach § 9b BSIG-E ist vorgesehen, Betreiber Kritischer Infrastrukturen zu verpflichten, dem BMI den Einsatz kritischer Komponenten anzuzeigen und nur kritische Komponenten von Herstellern einzusetzen, die eine Garantieerklärung der Vertrauenswürdigkeit über die gesamte Lieferkette hinweg abgeben (Abs. 2). Während der einmonatigen Prüfung der Komponenten soll deren Einsatz nicht gestattet sein (Abs.3). Zudem ist vorgesehen, dass da BMI den Einsatz bereits eingebaute kritischer Komponenten untersagen kann (Abs. 3).

Dabei ist jedoch zu bedenken:

- Gerade bei global hergestellten, komplexen Produkten ist die Lieferkette nicht immer zurückverfolgbar, eine Garantieerklärung über die gesamte Lieferkette daher nicht möglich.
- Die Möglichkeit einer nachträglichen Untersagung durch den Entzug der Vertrauenswürdigkeit und damit verbundene Rückbauverpflichtungen von bereits eingesetzten IT-Produkten sorgt für Rechtsunsicherheit und könnte im Extremfall eine Bedrohung der unternehmerischen Existenz darstellen.
- Die Betreiber müssten das Kostenrisiko eines angeordneten Rückbaus allein tragen und hierfür erhebliche Rückstellungen bilden. Daher müssten mindestens klare Verantwortlichkeiten, Ausstiegsszenarien und Übergangsfristen Rechtssicherheit garantieren, da es sonst zu erheblichen negativen Auswirkungen sowie rechtlichen Unsicherheiten kommen könnte.
- Ebenfalls berücksichtigt der Gesetzentwurf nicht, dass die Sicherheit technischer Produkte bereits durch das Ergreifen zusätzlicher organisatorischer und technischer Maßnahmen nachjustiert werden kann.
- Zudem sind die Folgen für die Versicherer und deren Geschäftsprozesse im Falle der Weigerung der Hersteller, eine Garantieerklärung abzugeben, unabsehbar. Darüber hinaus besteht die Gefahr einer Marktverzerrung, falls nur eine gewisse Anzahl an Herstellern eine solche Garantieerklärung für die gesamte Lieferkette abgeben. Dies könnte dazu führen, dass Versicherer sich in eine Abhängigkeit von diesen Herstellern begeben müssten.

Angesichts der aufgezeigten erheblichen Unsicherheiten, Konzentrationsrisiken und Mehraufwendungen sollte § 9b des BSIG-E in seiner jetzigen Form erheblich angepasst werden.

Der GDV hatte bereits zum Referentenentwurf eine Stellungnahme abgegeben, die Sie unter folgendem Link finden können:
[Stellungnahme]

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, D-10117 Berlin
Postfach 08 02 64, D-10002 Berlin
Tel.: +49 30 2020-5000
Fax: +49 30 2020-6000

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +49 30 2020-6140
ID-Nummer 6437280268-55

Ansprechpartner:
Patrik Maeyer
Gabriele Sieck

E-Mail: **g.sieck@gdv.de**

www.gdv.de