20. April 2021

Antrag

der Fraktionen der CDU/CSU und SPD
auf eine Entschließung des
4. Ausschusses des Deutschen Bundestages
- Ausschuss für Inneres Heimat -

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)812

Deutschlands Cybersicherheit stärken

I. Der Ausschuss für Inneres und Heimat des Deutschen Bundestages stellt fest:

Der Gesetzentwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme („IT-Sicherheitsgesetz 2.0“) ist ein wesentlicher Schritt für die Stärkung der Netz- und Informationssicherheit in Deutschland. Mit dem IT-Sicherheitsgesetz 2.0 wird der rechtliche Rahmen gestärkt. Der Gesetzentwurf umfasst Maßnahmen im Bereich der Wirtschaft zum Schutz Kritischer Infrastrukturen einschließlich kritischer Komponenten und weiterer Unternehmen im besonderen öffentlichen Interesse, zum Schutz der Verbraucherinnen und Verbraucher sowie zum Schutz der Bundesverwaltung.

Die digitale Transformation wird durch eine weiter steigende Durchdringung von Informations- und Kommunikationstechnologie ermöglicht. Unvermeidbare Folge der Digitalisierung ist dabei, dass die Anzahl der Schwachstellen in Soft- wie Hardware weiter ansteigt. Fehlerfreie Produkte können nicht gewährleistet werden – auch bei intensiven Tests ist es nicht möglich, alle Fehler zu entdecken. Die Information der betreffenden Stellen und Unternehmen über Sicherheitslücken ist daher ein wichtiger Baustein bei der Gewährleistung von IT-Sicherheit: insbesondere die Sicherheit von IT-Produkten kann verbessert werden, wenn Hersteller Informationen über entdeckte Sicherheitslücken erhalten und diese die Informationen nutzen, um Fehler zu beheben.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist auf Bundesebene die kompetente nationale Stelle zur Förderung der Sicherheit in der Informationstechnik. Zu den Aufgaben des BSI gehört es, Informationen über Sicherheitsrisiken zu sammeln, auszuwerten und die gewonnenen Erkenntnisse anderen Stellen zur Verfügung zu stellen (§ 3 Absatz 1 Satz 2 Nummer 2 BSI-Gesetz). Ferner berät und warnt das Bundesamt Hersteller, Vertreiber und Anwender in Fragen der IT-Sicherheit (§ 3 Absatz 1 Satz 2 Nummer 14 BSI-Gesetz). Mit § 7 Absatz 1 Satz 1 Buchstabe a BSI-Gesetz hat das BSI die Befugnis, die Öffentlichkeit und betroffene Fachkreise, insbesondere Hersteller, vor Sicherheitslücken in informationstechnischen Produkten und Diensten zu warnen.

Mit dem IT-Sicherheitsgesetz 2.0 wird die Kompetenz des BSI, über Sicherheitslücken oder andere Sicherheitsrisiken zu informieren, gestärkt. Das BSI darf auf Grundlage von § 7 BSI-Gesetz künftig nicht nur Warnungen aussprechen, sondern auch allgemeine Informationen übermitteln. Diese Befugnis soll nunmehr ausdrücklich auch dem Verbraucherschutz und der Verbraucherinformation dienen.

Mit Blick darauf sind nach § 7 Absatz 1 Satz 1 Nummer 1 Buchstabe d des Gesetzentwurfs auch Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten Gegenstand der Warn- und Informationsbefugnis. Zudem wird das BSI als allgemeine Meldestelle für die IT-Sicherheit ausgestaltet (§ 4b BSI-Gesetz des Gesetzentwurfs). Informationen über Sicherheitslücken, Schadprogramme oder sonstige Informationen können dem BSI anonym gemeldet werden. Diese Informationen soll das BSI nutzen, um die Öffentlichkeit und betroffene Kreise, wozu Hersteller, Vertreiber oder Anwender gehören, zu warnen und zu informieren. Im Sinne einer verantwortungsbewussten Offenlegung (Responsible Disclosure) sind Hersteller rechtzeitig vor Veröffentlichung einer Warnung zu informieren.

Es besteht ein anhaltender Trend, dass Angreifer modulare Schadprogramme für cyber-kriminelle Massenaufgriffe auf Privatpersonen, Unternehmen und andere Institutionen nutzen (vgl. Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2020, S. 9). Typischerweise besteht diese Software aus einer initialen „Hintertür“, die genutzt wird, um weitere Schadfunktionen nachzuladen. Das Verhalten dieser Software lässt sich aus der Ferne steuern. Insbesondere in Verbindung mit Erpressungs-Software (Ransomware) enthält diese Schadsoftware auch Funktionen zu ihrer eigenen Deinstallation, aber auch Funktionalitäten eines Bot-Netzes sind häufig in derartiger Software enthalten. Ein bekanntes Beispiel der jüngeren Vergangenheit ist die „Emotet“ genannte Schadsoftware. Diese diente sowohl als Türöffner für Erpressung durch Verschlüsselung als auch zum unberechtigten Kopieren von Daten. Insbesondere der Bekämpfung solcher Schadprogramme dient die Anordnungsbefugnis nach § 7c Absatz 1 Satz 1 Nummer 2 des Entwurfs des BSI-Gesetzes. Auf Grundlage dieser Befugnis kann das BSI Telekommunikationsdiensteanbieter zur Mitwirkung bei der Bereinigung betroffener Datenverarbeitungssysteme von einem konkret benannten Schadprogramm verpflichten. Dabei knüpft die Befugnis an hohe tatbestandliche Hürden an. Das BSI kann Maßnahmen nur zur Abwehr konkreter erheblicher Gefahren für die Verfügbarkeit, Unversehrtheit und Vertraulichkeit der in § 7c Absatz 2 des Entwurfs des BSI-Gesetzes genannten Informations- und Kommunikationssysteme und -dienste anordnen. Zur Verfahrenssicherung ist vor Anordnung einer etwaigen Maßnahme das Einvernehmen mit der Bundesnetzagentur und dem oder der Beauftragten für den Datenschutz und die Informationsfreiheit herzustellen. Aufgrund des Zwecks und der technischen Durchführung sind Maßnahmen auf Grundlage von § 7c Absatz 1 Satz 2 Nummer 2 des Entwurfs des BSI-Gesetzes wertungsmäßig und technisch nicht mit Maßnahmen zu vergleichen, die dem Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung zugrunde liegen (BVerfG, Urteil vom 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07). Während es in dem Urteil um heimliche Infiltration eines informationstechnischen Systems ging, um sich Kenntnisse von Kommunikationsinhalten zu verschaffen, geht es bei der Befugnis nach § 7c Absatz 1 Satz 1 Nummer 2 des Entwurfs des BSI-Gesetzes darum, Schadprogramme zu deaktivieren, die sich – unter Verletzung der Integrität und Vertraulichkeit – auf einem befallenen IT-System befinden. Zudem werden weder zur Durchführung von Maßnahmen Zugangsbeschränkungen überwunden, noch werden Systeme manipuliert, um in den aus dem Persönlichkeitsrecht abgeleiteten Schutzbereich der Integrität und Vertraulichkeit informationstechnischer Systeme einzugreifen. Vielmehr wird die vorangehend von Cyber-Kriminellen durch Aufbringen einer Schadsoftware beeinträchtigte Integrität und Vertraulichkeit der informationstechnischen Systeme durch Maßnahmen nach § 7c Absatz 1 Satz 1 Nummer 2 des Entwurfs des BSI-Gesetzes wiederhergestellt.

Zum Schutz der IT-Sicherheit Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse gehört neben technischen und organisatorischen Vorkehrungen auch der Einsatz vertrauenswürdiger Mitarbeiter in den sicher-

heitsrelevanten Bereichen. Den Unternehmen stehen derzeit häufig keine geeigneten Mittel zur Verfügung, die Vertrauenswürdigkeit des Personals zum Beispiel im Rahmen des Einstellungsprozesses zu überprüfen.

Als zentrale Meldestelle für Betreiber Kritischer Infrastrukturen erstellt das BSI ein Lagebild zur Sicherheit in der Informationstechnik Kritischer Infrastrukturen gemäß § 8b Absatz 2 Nummer 3 BSIG und unterrichtet die Betreiber über die sie betreffenden Informationen. Der Informationsfluss besteht aus allgemeinen Informationen in Form von Lagebildern sowie speziellen Handlungsanweisungen zu Prävention, Detektion und Reaktion zu Cyber-Angriffen, die den Betreibern Kritischer Infrastrukturen durch das BSI zur Verfügung gestellt werden. Damit das BSI die Lagebilder und spezialisierten Handlungsanweisungen erstellen kann, ist es auch auf Meldungen der Betreiber Kritischer Infrastrukturen z.B. zu Cyber-Angriffen angewiesen.

Der sichere und souveräne Betrieb Kritischer Infrastrukturen hängt auf Grund der voranschreitenden Digitalisierung und Vernetzung zunehmend von bestimmten kritischen Komponenten und damit auch von deren Herstellern ab. Dies gilt gerade für die zukünftigen Mobilfunknetze, die zunehmend das Rückgrat der digitalen Gesellschaft bilden werden. Damit spielen auch die „Vertrauenswürdigkeit“ der Hersteller und mithin Gefahren, die aus der Sphäre der Hersteller kritischer Komponenten stammen können, eine besondere Rolle beim Schutz der öffentlichen Ordnung und Sicherheit. Im IT-Sicherheitsgesetz 2.0 wird mit dem neuen § 9b BSIG erstmals eine Möglichkeit geschaffen, den Einsatz kritischer Komponenten bestimmter Hersteller durch Anordnungen einzuschränken oder als Ultima Ratio zu untersagen, sofern der Einsatz voraussichtlich eine Gefahr für die öffentliche Ordnung und Sicherheit der Bundesrepublik Deutschland darstellt. Damit wird eine der Kernforderungen der sog. EU 5G Toolbox („Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures“) umgesetzt, welche ausdrücklich Begrenzungen des Einsatzes sog. „high risk suppliers“ in den 5G-Netzen fordert („Strategic measure 03“).

Die Verabschiedung des IT-Sicherheitsgesetzes wird begleitet durch weitere wesentliche Maßnahmen zur Sicherstellung der Integrität von Mobilfunknetzen an anderer Stelle. So ist eine weitere Kernforderung der EU Toolbox die Verhinderung von Monokulturen in der Netztopologie („Strategic measure 05“). Dies ist durch den Einsatz von Komponenten möglichst vieler Hersteller sicherzustellen.

Vor diesem Hintergrund ist die Entscheidung der Bundesregierung, im Rahmen des Konjunktur- und Zukunftspaketes zwei Milliarden Euro in die Entwicklung künftiger Netztechnologien zu investieren, nicht nur als eine wirtschaftspolitische Maßnahme, sondern auch als ein Beitrag zur Sicherheit unserer Mobilfunknetze zu begrüßen.

Maßnahmen nach § 9b BSIG können im Einzelfall dazu führen, dass die betroffenen Betreiber Kritischer Infrastrukturen kritische Komponenten nicht wie beabsichtigt – oder nicht wie bereits erfolgt weiter – in ihren Kritischen Infrastrukturen einsetzen können. Damit handelt es sich bei Maßnahmen nach § 9b BSIG im Einzelfall um Begrenzungen der Eigentümerbefugnisse in Form von Inhalts- und Schrankenbestimmungen. Im Rahmen der Ausarbeitung des § 9b BSIG wurde daher sorgfältig und umfangreich geprüft, ob sich diese Regelung in den Grenzen hält, bei denen die Begrenzungen der Eigentümerbefugnisse als Ausfluss der Sozialgebundenheit des Eigentums (Artikel 14 Absatz 2 GG) entschädigungslos hinzunehmen sind.

In Anbetracht der möglichen Szenarien, in denen es zu einer Anordnung oder einer Untersagung in Bezug auf den Einsatz kritischer Komponenten kommen kann, und unter Berücksichtigung und Abwägung der Interessen der betroffenen Unternehmen sowie den Interessen der Allgemeinheit an dem sicheren Betrieb

Kritischer Infrastruktur und deren Rolle für das Gemeinwohl ist eine Entschädigung im Rahmen der verfassungsrechtlichen Vorgaben nicht notwendig.

Dabei wurden auch die zurechenbaren Verantwortungssphären mit in die Abwägung einbezogen. Die Betreiber der Kritischen Infrastrukturen haben jeweils die Gesamtverantwortung für den sicheren Betrieb inne. Da die Betreiber dazu verpflichtet sind, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, strahlt diese Pflicht auch auf die angemessene Auswahl der Zulieferer der eingesetzten Komponenten aus. Derartige Abwägungen und Prüfungen bei Auswahl der Komponenten sind bei dem Betrieb Kritischer Infrastrukturen, die im Interesse der Allgemeinheit – und des Schutzguts der öffentlichen Sicherheit und Ordnung – „sicher“ zu betreiben sind, auch aus eigenem wirtschaftlichen Interesse immer zu machen.

Für den Sektor der „öffentlichen Telekommunikationsnetze“ – und nur für diesen Bereich wird mit dem IT-Sicherheitsgesetz 2.0 die Möglichkeit geschaffen, auch kritische Komponenten festzulegen - wurde bereits der Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz aktualisiert und um neue Anforderungen an den sicheren Betrieb der Netze erweitert (Bearbeitungsstand 29. April 2020, in Kraft seit dem 23. Dezember 2020; die Betroffenen hatten ab dem 11. August 2020 Gelegenheit zur Stellungnahme). Darin wird unter Punkt 3.1.3 des Kataloges ausdrücklich aufgeführt, dass die Bereitstellung von Telekommunikationsdiensten oft nur unter Rückgriff auf Dritte erfolgen kann und Lieferanten und Erfüllungsgehilfen vor diesem Hintergrund eine wichtige Rolle einnehmen. Aus diesem Grund wird explizit gefordert, dass das pflichtige Unternehmen daher eine Bewertung der Zuverlässigkeit, Vertrauenswürdigkeit und Qualität des Erfüllungsgehilfen oder Lieferanten vornehmen muss.

Ferner wurde im Rahmen der Abwägung berücksichtigt, dass es die Regelung ermöglicht, dass neben der Untersagung des Einsatzes auch sonstige Anordnungen erlassen werden können, um die erkannten Gefahren – sofern als milderes Mittel ausreichend – abzuwehren. Im Rahmen der Ermessensentscheidung muss zudem auch die verfassungsimmanente Grenze der Verhältnismäßigkeit beachtet werden. Unverhältnismäßige Maßnahmen scheiden daher aus. Diese Ausgestaltung sorgt dafür, dass alle Aspekte des Betriebs der Kritischen Infrastruktur im Rahmen der Entscheidung nach § 9b BSIG-E in ausreichender Weise beachtet werden können.

Bei der Anwendung des § 9b – insbesondere bei der Untersagung des Einsatzes bereits eingebauter Komponenten – sind von der Bundesregierung die Auswirkungen auf die Funktionalität der betroffenen Kritischen Infrastruktur sowie volkswirtschaftliche und gesellschaftliche Folgewirkungen zu berücksichtigen. Dazu können u.a. die Auswirkungen auf die Ausbauziele im Mobilfunk sowie auf die Entwicklung von digitalen Innovationen in unserem Land zählen.

Da die technologische Entwicklung der kritischen Komponenten in dynamischer Weise voranschreitet und sich dadurch auch die Gefährdungslage mit Blick auf Kritische Infrastrukturen ändern kann, sollte aber auch fortlaufend geprüft werden, ob die zur Verfügung stehenden Maßnahmen weiterhin angemessen sind, um Gefahren für die öffentliche Ordnung und Sicherheit wirksam abzuwenden.

Auch kommt dem Staat die Aufgabe zu, den Einsatz von sicheren und vertrauenswürdigen kritischen Komponenten in geeigneter Weise zu fördern.

II. Der Ausschuss für Inneres und Heimat des Deutschen Bundestages fordert die Bundesregierung auf,

1. a) das BSI organisatorisch so aufzustellen, dass es die bestehenden und durch das IT-Sicherheitsgesetz 2.0 erweiterten Aufgaben und Befugnisse so nutzen kann, dass Hersteller effektiv über gemeldete oder detektierte IT-Schwachstellen durch das BSI informiert werden;

   b) zu prüfen, ob die für Hersteller bestehenden (insbesondere zivilrechtlichen) Pflichten zum Schließen von durch das BSI gemeldeten Sicherheitslücken ausreichen, damit Hersteller ihrer Verantwortung zur Behebung von Fehlern in IT-Produkten entsprechen.

2. im BSI technisch und organisatorisch sicherzustellen, dass bei der Durchführung von Maßnahmen auf Grundlage der Befugnis von § 7c Absatz 1 Satz 1 Nummer 2 des Entwurfs des BSI-Gesetzes rechtwidrige Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme von vornherein ausgeschlossen sind.

3. die gesetzliche Einführung weiterer Möglichkeiten zur Überprüfung der Vertrauenswürdigkeit von Beschäftigten in besonders sicherheitskritischen Bereichen bei Betreibern Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse zu prüfen.

4. zur Stärkung des Informationsflusses in beide Richtungen und zur Verbesserung des Lagebilds des BSI zu Kritischen Infrastrukturen, in der nächsten Legislaturperiode ein geeignetes System zu entwickeln und umzusetzen, mit dem spezialisierte technische Informationen zu Prävention, Detektion und Reaktion effizient und effektiv zwischen den zuständigen Behörden und den Betreibern Kritischer Infrastrukturen automatisiert ausgetauscht werden können.

5. a) die Anwendung des § 9b BSIG fortlaufend zu überwachen und zu prüfen, ob die Erfahrungen aus der Verwaltungspraxis Anlass zu einer Anpassung der gesetzlichen Rahmenbedingungen geben. Dabei ist auch zu prüfen, ob infolge solcher Anpassungen Entschädigungsregelungen geboten sind und gegebenenfalls, wie solche umgesetzt werden können;

   b) die Bundesregierung soll ferner zur Stärkung der digitalen Souveränität der Bundesrepublik Deutschland den Einsatz von sicheren kritischen Komponenten in Kritischen Infrastrukturen, insb. in Telekommunikationsnetzen, im Einklang mit den Empfehlungen der EU 5G Toolbox, mit geeigneten Mitteln fördern.