Deutscher Bundestag **Drucksache 18/5127**

18. Wahlperiode 10.06.2015

Entschließungsantrag

der Abgeordneten Dr. Konstantin von Notz, Hans-Christian Ströbele, Luise Amtsberg, Volker Beck (Köln), Kai Gehring, Dieter Janecek, Katja Keul, Renate Künast, Monika Lazar, Irene Mihalic, Özcan Mutlu, Tabea Rößner und der Fraktion BÜNDNIS 90/DIE GRÜNEN

zur dritten Beratung des Gesetzentwurfs der Bundesregierung

– Drucksachen 18/4096, 18/5121 –

Entwurfs eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

(IT-Sicherheitsgesetz)

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Die Digitalisierung und Vernetzung von Gesellschaft, Wirtschaft und Staat schreitet weiter voran und damit auch die die Abhängigkeit von IT-Systemen. Zugleich ist nicht erst seit dem durch Edward Snowden bekannt gewordenen Überwachungs- und Abhörskandal westlicher Geheimdienste klar, dass digitale Infrastrukturen auch durch staatliche Behörden bedroht sind. Beinahe täglich erfahren wir von gravierenden Sicherheitslücken in Software und von zahlreichen Hackerangriffen auf private als auch öffentliche IT-Strukturen. Die IT-Sicherheitslage in Deutschland ist weiterhin angespannt, wie der Lagebericht zur IT-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik (BSI) nachweist.

Das gesellschaftliche Vertrauen und das Vertrauen der Wirtschaft in die Integrität der digitalen Infrastruktur sind wesentliche Grundlagen für die digitale Zukunft. Eine Stärkung und Verbesserung der IT-Sicherheit ist aber vor allem auch dringend geboten, um den Menschen – auch vor dem Hintergrund des NSA-Überwachungsskandals - Schutz vor der Verletzung ihrer Grundrechte, insbesondere ihres Grundrechts auf Vertraulichkeit und Integrität der von Ihnen genutzten informationstechnischen Systeme zu bieten.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. einen Gesetzentwurf vorzulegen, der das neu geschaffene IT-Sicherheitsgesetz zurücknimmt und stattdessen weitergehende, insbesondere grundrechts- und rechtsstaatskonforme Regelungen zur IT-Sicherheit enthält,
   a. der nicht allein den Schutz Kritischer Infrastrukturen, sondern auch die Schutzpflicht des Grundrechts der Menschen auf Vertraulichkeit und Integrität ihrer informationstechnischen Systeme zum Ziel hat, sowie den grundlegenden datenschutzrechtlichen Anforderungen und dem Fernmeldegeheimnis gerecht wird,
   b. dessen Anwendungsbereich auch öffentliche Stellen umfasst,
   c. der hinreichend bestimmte und normenklare gesetzliche Regelungen zur Bestimmung der betroffenen Wirtschaftsbereiche und Betreiber sowie des Begriffs der kritischen Infrastruktur enthält,
   d. der konkret, eng und unter strenger Beachtung des Grundsatzes der Zweckbindung regelt, von wem und zu welchen Zwecken die im Rahmen der Meldepflichten übermittelten personenbeziehbaren Daten verarbeitet werden dürfen; der Meldepflichten für Sicherheitsvorfälle nicht erst im Falle „erheblichen Störungen“ vorsieht, sondern bereits zu einem Zeitpunkt, in dem noch kein Schaden eingetreten ist“,
   e. der Massenspeicherungen von Daten (Bestandsdaten, Verkehrsdaten oder Inhaltsdaten) allein für Zwecke der IT-Sicherheit ausschließt,
   f. der positive und wettbewerbsrelevante Anreize für die Wirtschaft setzt, ihre IT-Sicherheitskonzepte stetig und proaktiv fortzuentwickeln und zu pflegen, und hierzu insbesondere zu prüfen, ob ein System der unabhängigen Auditierung und Zertifizierung von Produkten und Verfahren einen effizienteren Ansatz bietet,
   g. der sicherstellt, dass die Qualität von IT-Sicherheitskonzepten in Behörden und Unternehmen durch zu auditierende Sicherheitsprüfungen wie zum Beispiel sog. Penetrationstests qualitativ verbessert werden, der ein Verfahren zur unabhängigen Festsetzung von Standards der IT-Sicherheit nach gesetzlich festgelegten Kriterien vorsieht,
   h. der für die gesetzlichen Vorgaben für technische Schutzstandards nicht nur den „Stand der Technik „berücksichtigt“, sondern auch Standards, die auf der Basis von Risikoanalysen und konkretisierbaren Gefahrenlagen (Szenarien) ermittelt werden, einhält,
   i. der eine Kontrolle der Einhaltung durch ein zumindest für diesen Aufgabenbereich unabhängig gestelltes Bundesamt für Sicherheit in der Informationstechnik (BSI) vorsieht,
   j. der klarstellt, dass neu zu regelnde Meldepflichten unbeschadet der in § 42a BDSG und § 109a TKG zum Zwecke des Datenschutzes geregelten Meldepflichten bestehen,
   k. der die Vorgaben der höchstrichterlichen Rechtsprechung des Bundesverfassungsgerichts (Urteil vom 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08) und des Europäischen Gerichtshofs (Urteil vom 08.04.2014 - C-293/12 und C-594/12) zur Vorratsdatenspeicherung beachtet,
   l. der wirksame Sanktionen bei Zuwiderhandlungen, insbesondere gegen gesetzliche Vorgaben für einzuhaltende Sicherheitsstandards vorsieht,

m. der insbesondere im Hinblick auf personenbezogene Daten ausdrücklich regelt, an wen und zu welchen konkreten Zwecken das BSI die durch die Meldungen erlangten Informationen übermitteln darf und unter welchen Voraussetzungen deren Weiterverarbeitung erfolgt,

n. der anlassbezogene Informationspflichten über Verletzungen der IT-Sicherheit gegenüber betroffenen Unternehmen und Öffentlichkeit differenzierend regelt,

o. der die Weitergabe von Erkenntnissen aus dem Lagebild des BSI sowie Erkenntnissen aus der Erweiterung der Aufgaben des BSI zur Untersuchung von informationstechnischer Systeme, normenklar regelt und Erkenntnisse der Öffentlichkeit verpflichtend und unmittelbar zur Verfügung stellt und eine grundsätzliche Pflicht zur unverzüglichen Veröffentlichung von Sicherheitslücken enthält,

p. der die Einbeziehung der Datenschutzbeauftragten des Bundes und der Länder in die Festlegung von Informationssicherheitsstandards und in die vorgesehenen Meldewege mit vorsieht,

q. der, entgegen des im IT-Sicherheitsgesetz vorgesehenen und mangelhaft begründeten Stellenaufbaus bei Nachrichtendiensten, keine Stellenaufwüchse und keine neuen Überwachungsbefugnisse der Nachrichtendienste im Zusammenhang mit der IT-Sicherheit vorsieht, solange die von den Nachrichtendiensten dabei zu verwendenden Methoden und Instrumente, somit auch die dadurch zu erwartenden Grundrechtsbeeinträchtigungen für den Gesetzgeber und die Öffentlichkeit nicht nachvollziehbar gemacht werden können, und

r. der das IT-Sicherheitsgesetz auf die parallel in Verhandlung befindliche EU-Richtlinie zur Netz- und Informationssicherheit (NIS) hin anpasst

2. sich auf EU-Ebene insbesondere in den laufenden Verhandlungen und die NIS-Richtlinie für einheitliche und hohe Standards der IT-Sicherheit einzusetzen;

3. mittelfristig gesetzlich dafür Sorge zu tragen, dass

a. der Aufbau, Betrieb und das Angebot von Ende-zu-Ende-Verschlüsselungen gefördert und zum Kernstück eines umfassenderen Regelungsansatzes gemacht wird,

b. eine langfristige Strategie zur Prüfung und Sicherstellung von Bausteinen einer sicheren Hard- und Softwareinfrastruktur auf der Grundlage etwa von Open Source-Elementen (offene und überprüfbare Quelltexte) erarbeitet und umgesetzt wird, beispielsweise durch die Finanzierung von regelmäßigen und unabhängigen Überprüfungen von sicherheitsrelevanter Software („bug bountys“),

c. in einer ganzheitlichen Perspektive die Hersteller von Hard- und Software (nicht nur Betreiber) berücksichtigt und Anreize zur Qualitätssicherung durch Haftungsverpflichtungen geschaffen werden,(beispielsweise für die fahrlässige Implementierung oder Nichtbeseitigung von Sicherheitslücken),

d. das Vergaberecht der öffentlichen Hand angepasst wird, so dass grundsätzlich nur auditierte, zertifizierte sowie open source gemäße Produkte berücksichtigt werden,

e. eine Beförderung des Schwarzmarktes für Sicherheitslücken durch den staatlichen Aufkauf und die Zurückhaltung von Sicherheitslücken (bspw.

zero-day-exploits), welche die Integrität digitaler Infrastrukturen gefährden, zu verbieten und stattdessen auf die konsequente Beseitigung von Sicherheitslücken hinzuwirken,

f. mittels eines übergreifenden Regelungsansatzes für einen hohen Datenschutz durch Technik gesorgt wird, beispielsweise durch Verpflichtungen zu „Security and Privacy by Design and Default“

g. der Schutz von Whistleblowern (Hinweisgebern) gesetzlich gestärkt wird.

Berlin, den 9. Juni 2015

Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion