Beschluss

des Bundesfachausschusses Innenpolitik vom 8. September 2016

Abwehrfähigkeit gegen Cybergefahren stärken

Nahezu alle Lebensbereiche in unserem Land sind von fortschreitender Digitalisierung durchdrungen. Zunehmend werden auch hochsensible Prozesse vernetzten IT-Systemen überantwortet – vom Gesundheitswesen über den Straßenverkehr, der industriellen Produktion bis hin zur Energieversorgung. Die Abhängigkeit von der Sicherheit und Zuverlässigkeit dieser Systeme ist in den vergangenen Jahren deutlich gestiegen.

Zugleich ist die Bedrohungslage unverändert ernst: Die IT-Systeme in Deutschland sind fortlaufend Angriffen ausgesetzt. Die Vorgehensweise der Angreifer reicht dabei von simplen Attacken bis hin zu hochentwickelten und lang andauernden Angriffen. Diese Entwicklung stellt unser Land vor besondere Herausforderungen.

Widerstandsfähige IT-Infrastrukturen und Netze sind angesichts dieser Bedrohungslage unverzichtbar. Unsere Sicherheitsbehörden in Bund und Ländern müssen im Kampf gegen die Gefahren aus dem Cyberraum gut aufgestellt sein. Sie brauchen die erforderlichen Befugnisse sowie ausreichende technische und personelle Ausstattung.

Informationssicherheit ist eine wesentliche Voraussetzung für das Gelingen der großen Digitalisierungsprojekte in Deutschland, wie etwa für die Energiewende, für Industrie 4.0 oder für das autonome Fahren. Mit der IT-Sicherheitsstrategie haben wir eine gute Grundlage gelegt, um Sicherheit auf einem angemessenen Niveau zu gewährleisten, ohne die Chancen der Digitalisierung zu beeinträchtigen. Darauf wollen wir weiter aufbauen.

Der Bundesfachausschuss Innenpolitik der CDU Deutschlands fordert eine Reihe von Maßnahmen, um die Informationssicherheit weiter zu stärken. Entscheidend dabei ist: Akteure aus Staat, Wirtschaft und Gesellschaft müssen eng miteinander verzahnt sein. Es muss intensiver für IT-Sicherheitsfragen sensibilisiert sowie die Aufklärung darüber verstärkt werden, um so die Abwehrfähigkeit gegen Cybergefahren und die Handlungsfähigkeit in akuten Bedrohungslagen zu erhöhen.

1. Das Internet darf kein Schutzraum für Kriminelle sein. Aus diesem Grund treten wir dafür ein, die technischen Fähigkeiten der Cyberaufklärung in einer „Zentralen Stelle für Informationstechnik im Sicherheitsbereich“ (ZITiS) organisatorisch zu bündeln. ZITiS soll die Sicherheitsbehörden als Forschungs- und Entwicklungsstelle unterstützen sowie Methoden, Produkte und Strategien zur Bekämpfung von Kriminalität und Terrorismus im Internet erarbeiten und bereitstellen.

2. Der Schutz kritischer Infrastrukturen in unserem Land muss weiter verbessert werden. Das IT-Sicherheitsgesetz und die mit der NIS-Richtlinie erfolgte europäische Gesetzgebung müssen der aktuellen Bedrohungslage angepasst werden.

3. Die Wettbewerbsfähigkeit der deutschen Wirtschaft wird durch gezielte Spähangriffe fremder Nachrichtendienste und internationaler Konkurrenz schwer geschädigt. Wichtige Forschungs- und Entwicklungsergebnisse werden so ausgespäht; insbesondere kleine und mittelständische Unternehmen sind häufig nur unzureichend geschützt.

Den Standort Deutschland und damit Arbeitsplätze in unserem Land wollen wir besser schützen. Mit der Initiative Wirtschaftsschutz der obersten deutschen Sicherheitsbehörden und der großen Wirtschaftsverbände ist hierzu ein verbindlicher Rahmen der gemeinsamen Aktivitäten geschaffen worden. Diese Zusammenarbeit muss weiter gestärkt werden. Es braucht zusätzliche finanzielle Anreize für Staat, Wirtschaft und Gesellschaft zur Verbesserung der Informationssicherheit – etwa in Form eines „Digitalbonus“, der die Umsetzung sinnvoller Maßnahmen belohnt.

4. Bewährte deutsche und europäische IT- und Datensicherheitsstandards müssen in der globalisierten Welt gestärkt werden. IT-Produkte müssen standardmäßig sicher hergestellt und konfiguriert sein. Hierfür sollten Anreize und eine faire Risikoverteilung für Staat, Wirtschaft und Gesellschaft geschaffen werden – bis hin zur Haftung für unsichere Produkte.

5. Deutschland braucht mehr Fachkräfte auf dem Gebiet der Informationstechnik. Um diese zu gewinnen, sollte auch an Wege außerhalb formaler Abschlüsse und festgelegter

Besoldungsstrukturen gedacht werden. Informationssicherheit und Cybersicherheit müssen zentrale Bestandteile einer zeitgemäßen Bildungs- und Forschungspolitik sein. Sie müssen in Schule und Hochschule – auch in Studiengängen jenseits der klassischen Informatik – einen angemessenen Platz bekommen.

6. Sicherheit im Netz ist ein entscheidender Standortfaktor der Zukunft. Deshalb setzen wir uns dafür ein, den europäischen Datenstandort zu stärken sowie die IT-Sicherheitsforschung weiter voranzutreiben, innovative Projekte zu fördern und dies auf staatlicher Ebene besser zu koordinieren.

Insbesondere bei der Entwicklung von Hard- und Software müssen wir in Deutschland und Europa mehr technologische Souveränität erlangen, um unabhängiger von Ländern außerhalb Europas zu werden. Immer mehr Unternehmen entwickeln neuartige Sicherheitslösungen. Dabei ist die Vertrauenswürdigkeit dieser Lösungen von deutschen und europäischen Anbietern ein wichtiges Alleinstellungsmerkmal. Diese Initiativen müssen gestärkt werden. Durch die richtigen Anreize – etwa durch Privilegierungen für Unternehmen im Vergaberecht – wollen wir Deutschland zum Marktführer für Sicherheitslösungen im Netz entwickeln.

7. Deutschland braucht eine zentrale Stelle für Fragen der Informations- und Cybersicherheit. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sollte zu dieser zentralen Stelle ausgebaut und ausreichend ausgestattet werden. Es sollte prägender Gestalter der deutschen Informations- und Cyber-Sicherheitsarchitektur in der Digitalisierung für Staat, Wirtschaft und Gesellschaft werden. Hierzu ist eine Öffnung des BSI notwendig, um zusätzlich zur Bundesverwaltung auch weitere staatliche Stellen zu erfassen, die Wirtschaft insgesamt zu adressieren und mit der erforderlichen Breitenwirkung in die Gesellschaft hinein präsent zu sein.

8. Mit dem Zusammenwirken des Bundesamts für Verfassungsschutz, des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe, des Bundeskriminalamts, der Bundespolizei, des Zollkriminalamts, des Bundesnachrichtendiensts und der Bundeswehr im Nationalen Cyber-Abwehrzentrum unter der Federführung des BSI haben wir die Schlagkraft der Sicherheitsbehörden gestärkt. Diesen erfolgreichen Ansatz wollen wir weiter ausbauen. Im BSI sollte der besondere Sachverstand des Bundes gebündelt und durch Zusammenarbeit

mit anderen Institutionen in Bund und Ländern sowie in Wirtschaft und Gesellschaft nutzbar gemacht werden.