Ständige Konferenz der
Innenminister und Senatoren der Länder

Arbeitsgruppe Cybersicherheit

20.11.2017

Sachstandsbericht: Intensivierung der Maßnahmen zur Verbesserung der Cybersicherheit bezogen auf das Internet der Dinge

Die 206. IMK hat die länderoffene Arbeitsgruppe Cybersicherheit mit Beschluss zu TOP 51 beauftragt, die Intensivierung der Maßnahmen zur Verbesserung der Cybersicherheit bezogen auf das Internet der Dinge umfassend zu prüfen:

1. Die IMK stellt fest, dass die massenhafte Verbreitung von mit dem Internet verbundenen Gebrauchsgeräten (Internet der Dinge) ohne ausreichende Sicherheitsvorkehrungen eine erhebliche Bedrohung für den Cyberraum darstellt.
2. Sie hält eine Intensivierung der Maßnahmen zur Verbesserung der Cybersicherheit bezogen auf das Internet der Dinge für erforderlich. Dies sollte im Rahmen eines umfassenden Handlungskonzepts erfolgen, das unter anderem folgende Themenfelder adressiert wie:
   a) Schaffung verbindlicher Produktsicherheitsstandards für mit dem Internet verbundene Geräte,
   b) Schaffung von Regelungen zur Produkthaftung für mit dem Internet verbundene Geräte unter Berücksichtigung von IT-spezifischen Schadensfällen.
3. Die IMK bittet die länderoffene Arbeitsgruppe Cybersicherheit, diese Thematik umfassend zu prüfen und hierbei den IT-Planungsrat im erforderlichen Umfang zu beteiligen.

Die Arbeitsebene der länderoffenen Arbeitsgruppe Cybersicherheit tagte am 9. und 10. November Wiesbaden. Schwerpunkt war die inhaltliche Bearbeitung der Aufträge aus der 206. IMK vom 12. bis 14. Juni 2017.

Auch im nationalen Cyber-Sicherheitsrat wurde das Thema Schaffung verbindlicher Produktsicherheitsstandards vor dem Hintergrund des Mirai-Bot-Netzes und des Angriffes auf die Internetzugangsrouter von Hunderttausenden Telekom-Kunden zweimal behandelt:
Bereits in der Sitzung am 9. März 2017 hat Herr StS Vitt (BMI) vorgetragen, dass die Bundesregierung sich mit Gütesiegeln, Mindestsicherheitsstandards für mit dem Internet verbundene Geräte und Fragen der Produkthaftung befasst:

> (Auszug Protokoll NCSR 9. März 2017)
> „Um eine angemessene Verteilung von Verantwortlichkeiten und Sicherheitsrisiken im Netz zu erreichen, prüft BMI die Einführung eines freiwilligen Gütesiegels für IT-Sicherheit. Die Abstimmung mit BMJV und BMWi läuft derzeit und ein entsprechendes Grobkonzept wird vorbereitet.

Mindest-IT-Sicherheitsstandards, auf denen das Gütesiegel aufbauen könnte, oder IT-Sicherheitszertifizierungen könnten später auch als Grundlage zur Bewertung von Haftungsfragen herangezogen werden.

In einem weiteren Schritt wäre daher zu prüfen, ob Gütesiegel und Zertifikate als Grundlage geeignet sein könnten, für mehr Rechtssicherheit bei der Umsetzung von haftungsrechtlichen Ansprüchen beizutragen, oder ob weitere Rechtsänderungen (z. B. im Bereich der Produkt- und Produzentenhaftung) erforderlich sind."

(Auszug Protokoll NCSR 26. Juni 2017)
„Mit einem Entschließungsantrag fordern die Regierungsfraktionen darüber hinaus die Bundesregierung auf, die IT-Sicherheit internetfähiger Geräte zu erhöhen. Die Bundesregierung soll sich in Brüssel für verpflichtende Vorgaben im europäischen Binnenmarkt einsetzen. Eine angemessene Verteilung von Verantwortlichkeiten und Sicherheitsrisiken im Netz zu erreichen ist ein wichtiges Ziel der neuen Cyber-Sicherheitsstrategie der Bundesregierung. In diesem Kontext prüfen wir auch die Einführung eines Gütesiegels für IT-Sicherheit. Ein entsprechendes Konzept wird in Zusammenarbeit mit BMWi und BMJV derzeit vorbereitet. Es sieht unter anderem eine Pilotierung im Produktbereich „Internetzugangsrouter" vor. Eine Beteiligung von Herstellern, Wirtschaftsvertretern, Verbraucherschützern und anderen Interessensvereinigungen am Planungsprozess ist vorgesehen.

Mindest-IT-Sicherheitsstandards, auf denen das Gütesiegel aufbaut, oder elaborierte IT-Sicherheitszertifizierungen können später als Grundlage zur Bewertung von Haftungsfragen herangezogen werden. Die zugrundeliegenden Mindest-IT-Sicherheitsstandards (idR Technische Richtlinien des BSI zu einzelnen Produktklassen) können auch im Zusammenhang mit Cyber-Versicherungen von Bedeutung sein.

Ob Gütesiegel und Zertifikate als Grundlage geeignet sind, für mehr Rechtssicherheit bei der Umsetzung von haftungsrechtlichen Ansprüchen beizutragen, oder vielmehr weitere Rechtsänderungen - etwa im Bereich der Produkt- und Produzentenhaftung - erforderlich sind, wird geprüft."

Die Arbeitsebene der länderoffenen Arbeitsgruppe Cybersicherheit hat sich in ihrer Sitzung mit Blick auf die Aktivitäten der Bundesregierung und die Aktivitäten der EU-Kommission (COM 2017 477 final: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die "EU Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik ("Rechtsakt zur Cybersicherheit") zunächst auf die Erörterung grundsätzlicher Aspekte beschränkt.

Es bestand zwischen den Vertretern der Länder Einvernehmen, dass nationale Maßnahmen nur marginale Effekte auf das von mit dem Internet verbundenen Geräten ausgehende Risiko für die Verwaltung und die nationale informationstechnische Infrastruktur haben.

Dies begründet sich darin, dass es sich überwiegend um Geräte in der Betriebsverantwortung von privaten Endanwendern handelt, die erfahrungsgemäß im Zweifelsfall ihre Kaufentscheidungen am Preis, am Komfort und den Leistungsdaten des Produktes und nicht an seinen Sicherheitseigenschaften ausrichten. Erschwerend kommt hinzu, dass bei diesen Geräten in der Regel nicht die Gesundheit oder die Vermögenswerte des Benutzers gefährdet

werden, sondern die Dritter. In der Praxis werden die Angriffe über diese Geräte so gestaltet, dass der Besitzer diese gar nicht bemerkt; die ungestörte Funktion der Geräte ist eine conditio sine qua non. In diesen Fällen greift der Ansatz der Produkthaftung nicht.

Ob die Besitzer als Störer in Haftung genommen werden könnten oder ob Import und Verkauf reguliert werden könnten, ist rechtlich wie politisch fragwürdig. Zumal auch im außereuropäischen Ausland betriebene Geräte zu Angriffen auf deutsche Ziele missbraucht werden können.

Die Arbeitsebene der länderoffenen Arbeitsgruppe Cybersicherheit wird den Bund bitten, in ihrer nächsten Sitzung in der zweiten Hälfte des Januar 2018 zum Stand der Aktivitäten der Bundesregierung zu berichten und den Fortgang des Vorhabens der EU-Kommission beobachten, weitere Maßnahmen prüfen und in 2018 einen Bericht zu den Ergebnissen vorlegen.