

Bundesinnenministerin Faeser will Grundgesetzänderung für Cybersicherheit

13 Juli 2022 22:19 Uhr

Nancy Faeser will das Grundgesetz für die Cybersicherheit ändern. Derzeit liegt die Kompetenz für die Cybersicherheit bei den Ländern. Nun will die Bundesinnenministerin das Bundesamt für Sicherheit in der Informationstechnik zur Zentralstelle für Cybersicherheit ausbauen.



Quelle: Gettyimages.ru © Bernd von Jutrczenka/picture alliance
Bundesinnenministerin Nancy Faeser (SPD)

Bundesinnenministerin Nancy Faeser (SPD) hat eine Grundgesetzänderung vorgeschlagen, um das ihrem Haus unterstellte Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Zentralstelle für den Kampf gegen Cyberattacken auf Ziele in Deutschland zu machen. Eine vergleichbare Konstruktion gibt es jetzt schon beim Bundeskriminalamt (BKA) und beim Bundesamt für Verfassungsschutz, die eng mit den jeweiligen Landesbehörden zusammenarbeiten.

Die Verantwortung für Cybersicherheit im Inland liegt aktuell noch bei den Ländern, das BSI könne daher bislang nur Amtshilfe leisten, sagte die Ministerin am Dienstag in Berlin. Angesichts der gewachsenen Bedrohung sei dies jedoch nicht mehr zeitgemäß. Die Länder seien mit dieser Aufgabe langfristig "überfordert". Sie habe zu ihrem Vorschlag einer Grundgesetzänderung sehr positive Signale aus den Ländern erhalten. Für eine Grundgesetzänderung bräuhete die Ampel-Regierung im Bundestag jedoch auch Stimmen aus der Opposition, da dafür eine Zwei-Drittel-Mehrheit erforderlich ist.

In den vergangenen zwei Jahren hatten mehrere Cyberattacken auf Kliniken und staatliche Stellen für Probleme gesorgt. Insgesamt nahm die Zahl der bislang bekannt gewordenen Angriffe zu. Infolge eines Cyberangriffs auf die Kreisverwaltung im Landkreis Anhalt-Bitterfeld wurde dort am 9. Juli 2021 der Katastrophenfall ausgerufen. Mehrere Server waren mit sogenannter Ransomware infiziert worden. Dabei werden durch eine Schadsoftware Daten auf den Rechnern der Behörden verschlüsselt. Nach der Zahlung eines Lösegelds sollen diese dann wieder freigegeben werden. Der Landkreis lehnte die Geldzahlung ab und konnte daraufhin etliche Dienstleistungen nicht mehr erbringen.

FDP-Fraktionsvize Konstantin Kuhle mahnte, vor einer Grundgesetzänderung müsse das Aufgabenprofil des BSI klar umrissen und dessen Unabhängigkeit gestärkt werden. "Dazu gehört auch die Einrichtung eines funktionierenden Schwachstellenmanagements für alle Sicherheitsbehörden." Im Fokus stehen dabei Sicherheitslücken in der Hard- und Software, die bewusst nicht geschlossen werden, damit sich staatliche Stellen für Aufklärung oder Ermittlungen zu schweren Straftaten Zugang zu Handys und anderen Kommunikationsmitteln verschaffen können.

Angesichts der russischen Militäroperation in der Ukraine stellte das Bundesinnenministerium weitere Maßnahmen für mehr Cybersicherheit vor. Dazu gehört die Einführung eines zentralen Videokonferenzsystems für die Bundesverwaltung, das höchsten Sicherheitsanforderungen entspricht. Beim BSI soll für Unternehmen eine Plattform für den Austausch von Informationen zu Cyberangriffen entstehen.

Darüber hinaus sollen Investitionen in sogenannte Cyber-Resilienzmaßnahmen bei kleinen und mittleren Unternehmen gefördert werden, wenn diese zur "kritischen Infrastruktur" gehören. Dazu zählen etwa die Bereiche Verkehr, Ernährung, Gesundheit, Energie und Wasserversorgung. Zudem hat sich Faeser die Modernisierung der IT-

Infrastruktur des Bundesamtes für Verfassungsschutz vorgenommen. Dieses soll auch mehr Befugnisse zur "Aufklärung technischer Sachverhalte bei Cyberangriffen fremder Mächte" erhalten.

Abstimmungsbedarf gibt es im Bereich Cybersicherheit allerdings nicht nur mit den Ländern, sondern auch innerhalb der Bundesregierung. Für Digitales ist Verkehrsminister Volker Wissing (FDP) verantwortlich. Mit dem Kommando Cyber- und Informationsraum gibt es in der Bundeswehr einen Organisationsbereich zur Abwehr von Cyberangriffen. Faeser erläuterte:

"Die Schnittstelle zum BMVg (Bundesverteidigungsministerium) werden wir immer haben müssen."

Der Koalitionsvertrag von SPD, Grünen und FDP sieht ein neues Gesetz vor, in dem Vorschriften zum Schutz der kritischen Infrastruktur gebündelt werden sollen. Dieses müsse schnellstmöglich umgesetzt werden, sagte der stellvertretende Grünen-Fraktionsvorsitzende Konstantin von Notz. Er erklärte:

"Auch bedarf es dringend einer Abstimmung mit den von anderen Häusern derzeit in Erarbeitung befindlichen Strategien."

Der innenpolitische Sprecher der Unionsfraktion, Alexander Throm (CDU), wandte ein, die neue Cybersicherheitsagenda lasse entscheidende Fragen unbeantwortet – beispielsweise welche konkreten Befugnisse das Bundeskriminalamt, das Bundesamt für Verfassungsschutz und die Bundespolizei zur Abwehr von Cyberangriffen erhalten sollen. Er fügte hinzu:

"Auch fehlt ein Konzept für eine aktive Cyberabwehr, das sich gefahrenabwehrend gegen den Cyberangriff richtet."

Ein entsprechendes Konzept sei während der Amtszeit von Faesers Vorgänger Horst Seehofer (CSU) am Widerstand der SPD gescheitert.

Ein weiterer Schwerpunkt von Faesers Cybersicherheitsagenda liege bei Maßnahmen, die auf die Verhinderung der Verbreitung strafbarer Inhalte im Internet abzielen – insbesondere Darstellungen des sexuellen Missbrauchs von Kindern. Dazu soll ein durch das BKA koordinierter, bundesweit abgestimmter Melde- und Löschprozess etabliert werden. Auf EU-Ebene will sich Faeser für einen Rechtsrahmen zur Verhinderung der Verbreitung solcher Darstellungen einsetzen. Ein vom BKA koordiniertes Lösungsverfahren, könne "dafür sorgen, dass entsprechende Darstellungen schneller aus dem Internet verschwinden", erklärte der Branchenverband Bitkom. Der SPD-Innenpolitiker Uli Grötsch warnte seinerseits:

"Die Gefahren im Cyberraum nehmen stetig zu."

Daher sei gut, dass Faeser "effektiver gegen Cyberkriminalität vorgehen" wolle. Im vergangenen Jahr registrierte die Polizei laut BKA im Bereich Cybercrime bundesweit 146.363 Delikte – ein Anstieg um mehr als zwölf Prozent gegenüber dem Vorjahr.

(rt/dpa)