BUNDESVERBAND

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)721

Stellungnahme des

AOK-Bundesverbandes

zum

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

Bundestags-Drucksache 19/26106

Stand 04.02.2021

AOK-Bundesverband
Rosenthaler Straße 31
10178 Berlin

Tel. 030/ 3 46 46 - 2299

Inhaltsverzeichnis:

I. Zusammenfassung ..... - 3 -

II. Stellungnahme zu einzelnen Regelungen des Gesetzentwurfs ..... - 4 -

Artikel 1 Änderung des BSI-Gesetzes ..... - 4 -

§ 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden ..... - 4 -

§ 8a Anschaffung von Systemen zur Angriffserkennung ..... - 5 -

§ 9b Untersagung des Einsatzes kritischer Komponenten..... - 6 -

I. Zusammenfassung

Es ist zu begrüßen, dass mit diesem Gesetzentwurf die sicherheitstechnischen IT-Fortschritte und die damit verbundenen Risiken aufgegriffen werden.

Anzuerkennen ist, dass die Anregungen der betroffenen Betreiber kritischer Infrastrukturen und Unternehmen im öffentlichen Interesse im Rahmen der Verbändebeteiligung zum Referentenentwurf in wesentlichen Punkten in diesem Gesetzentwurf aufgegriffen wurden. Gleichwohl bestehen weiterhin wirtschaftliche und betriebliche Risiken für die Betreiber kritischer Infrastrukturen durch fehlende Konkretisierungen, ambitioniert gefasste Befugnisse und Vorlaufzeiten in den vorgesehenen Regelungen.

II. Stellungnahme zu einzelnen Regelungen des Gesetzentwurfs

Artikel 1 Änderung des BSI-Gesetzes

§ 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden

A Beabsichtigte Neuregelung

Die ergänzende Regelung in Absatz 1 eröffnet dem Bundesamt die Möglichkeit, sogenannte Portscans zur Ermittlung von Sicherheitslücken und anderen Sicherheitsrisiken in der Informationstechnik bei dem Bund, den Betreibern kritischer Infrastrukturen sowie Unternehmen im besonderen öffentlichen Interesse auch ohne Kenntnis der jeweiligen Betreiber durchzuführen.

B Stellungnahme

Es ist anzunehmen, dass mit der Durchführung von Portscans Schwachstellen bei Betreibern kritischer Infrastrukturen ermittelt werden sollen.

Der Nutzen dieses Vorgehens ist jedoch zweifelhaft und bindet in der beschriebenen Form zusätzliche Ressourcen bei den Betreibern, da die Netzwerkaktivitäten ohne vorherige Abstimmung als Angriffsversuch interpretiert werden könnten.

Die bloße Ermittlung von potenziell risikobehafteten Ports lässt darüber hinaus keine verlässliche Auskunft über die dahinterliegende Anwendung zu und kann somit auch nicht zuverlässig einer Sicherheitslücke und oder einem anderen Sicherheitsrisiko zugeordnet werden. Ein systematisches Vorgehen zur Ermittlung von Risiken ist daher in Abstimmung mit den Betreibern, bei denen die Durchführung von Portscans erfolgen soll, zu bevorzugen.

C Änderungsvorschlag

Einfügen des nachfolgenden Satz nach Satz 4 im Absatz 1:

„Maßnahmen nach Satz 1 dürfen nur im Einvernehmen mit den jeweiligen Betreibern kritischer Infrastrukturen oder Unternehmen im besonderen öffentlichen Interesse durchgeführt werden.“

§ 8a Anschaffung von Systemen zur Angriffserkennung

A Beabsichtigte Neuregelung

Betreiber Kritischer Infrastrukturen müssen Systeme zur Angriffserkennung nach dem vom Bundesamt festgelegten Standards vorhalten.

B Stellungnahme

Je nach Größe des Betreibers bzw. Netzwerkdurchsatzes kann die geplante Regelung zu regelmäßigen erheblichen Investitionen und Betriebsaufwänden führen. Die hierfür erforderlichen Aufwände müssen daher durch Mittel des Bundes gegenfinanziert werden.

Gleichzeitig bedarf die Verpflichtung der KRITIS-Betreiber zur Anschaffung von Produkten für die Angriffserkennung einer deutlichen und präzisen Definition der erforderlichen Mindestfunktionen sowie die realistische Verfügbarkeit solcher Produkte am Markt.

Die Regelung zur Speicherung von Daten über einen Zeitraum von vier Jahren muss präzisiert werden. Es ist unklar, ob der Gesetzgeber für Protokollierungsdaten vier Jahre vorsieht. Falls dies der Fall ist, sind Aufwand und Kosten für die Speicherung erheblich, ohne dass diese anonymisierten Daten nach vier Jahren noch einen besonderen Nutzen für die Ziele der Gesetzgebung und der IT-Sicherheit darstellen. Eine Speicherdauer von maximal einem Jahr wäre angemessen.

C Änderungsvorschlag

§ 8a Abs. 1b wird wie folgt geändert:

„Betreiber Kritischer Infrastrukturen müssen für die Angriffserkennung und Angriffsnachverfolgung relevante, nicht personenbezogene Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, mindestens ein Jahr speichern.“

§ 9b Untersagung des Einsatzes kritischer Komponenten

A Beabsichtigte Neuregelung

Es wird eine Anzeigepflicht gegenüber dem Bundesministerium des Innern, Bau und Heimat für kritische Komponenten eingeführt. Der Betrieb von kritischen Komponenten kann durch die Behörde untersagt werden.

B Stellungnahme

Bei einer Untersagung des Einsatzes von kritischen Komponenten, die vom Betreiber nicht vorhersehbar waren, müssen die hierfür erforderlichen Aufwände durch Mittel des Bundes gegenfinanziert werden. Es muss sichergestellt sein, dass getätigte Investitionen der KRITIS-Betreiber geschützt werden. Eine nachträgliche Untersagung von eingesetzten Komponenten führt zu unverhältnismäßigen wirtschaftlichen und betrieblichen Risiken.

Die geforderten Fristen sind in der Praxis unverhältnismäßig und müssen unter Berücksichtigung der Schutzziele der Informationssicherheit gegenüber Schadensausmaß abgewogen werden. Die Untersagung des Einsatzes von kritischen Komponenten muss das Risiko in der jeweiligen Betriebsumgebung berücksichtigen.

C Änderungsvorschlag

Streichung des 2. Satzes im Absatz 3 und Anfügen der folgenden Sätze nach Satz 1:

„Die Frist zum Weiterbetrieb der kritischen Komponente ist im Einvernehmen mit dem jeweiligen Betreiber unter Berücksichtigung des Risikos für die öffentlichen Interessen festzulegen.

Wird die Untersagung einer in Betrieb befindlichen kritischen Komponente angeordnet, müssen die Kosten durch Mittel des Bundes gegenfinanziert werden.“