Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)728

BUNDESVERBAND PAKET & EXPRESS LOGISTIK BIEK

Stellungnahme

BSI-Gesetz – Sicherheit erhöhen ohne Bürokratie auszubauen

Der Deutsche Bundestag ist mit der ersten Lesung des IT-Sicherheitsgesetzes 2.0 (IT-SiG 2.0) in das Gesetzgebungsverfahren eingetreten. Wir möchten mit dieser Stellungnahme auf Aspekte aufmerksam machen, die aus unserer Sicht im parlamentarischen Verfahren nachgebessert werden sollten, um das Gesetz rechtssicher und effektiver zu gestalten.

Der Bundesverband Paket und Expresslogistik vertritt bundesweit tätige Paketdienstleister. Im Zusammenhang mit der aktuellen Sicherheitsdiskussion halten wir es für möglich, dass eine Diskussion auftritt, den Anwendungsbereich über den in der Begründung genannten Bereich hinaus auszudehnen, auch wenn hierfür kein Anlass besteht.

Eine grundsätzliche Anmerkung betrifft die Evaluierung bestehender Regelungen. Der Gesetzgeber hat eine Evaluierung des IT-Sicherheitsgesetzes im Gesetz selbst vorgesehen. Dennoch ist diese Evaluierung durch das Bundesministerium des Inneren, für Bau und Heimat (BMI) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterblieben, zumindest ist uns keine Berichterstattung dazu bekannt.

Wir weisen in diesem Zusammenhang auf die Empfehlungen des UP-KRITIS hin. Es ist grundsätzlich fragwürdig, eine Verpflichtung zur Evaluierung im Gesetz vorzunehmen, sie dann aber nicht erkennbar vorzunehmen, Empfehlungen zur Weiterentwicklung zu ignorieren, aber dennoch eine Neuregelung vorzunehmen.

Konkrete Ansatzpunkte sehen wir bei den folgenden Aspekten:

1. Risikobezug

Weder das BMI noch das BSI haben eine Gefährdungsanalyse des Mobilitäts- und Logistiksektors vorgelegt, mit dem die Risiken aufzeigt, bewertet und darauf ausgerichtete gezielte Maßnahmen vorgeschlagen werden. Ziel muss es sein, die begrenzten Mittel zur Abwehr von Gefahren so gezielt einzusetzen, dass ein sehr hoher Sicherheitsstandard erlangt werden kann. Dafür müssen die größten Gefahren ermittelt und anschließend regulatorische Maßnahmen auf Basis eines risikobasierten Ansatzes entwickelt werden.

2. Verwendung unbestimmter Rechtsbegriffe

Im Gesetzentwurf werden unbestimmte Rechtsbegriffe verwendet, die im Ergebnis zu einseitig hohen Kostenrisiken der Wirtschaft führen, ohne den gewünschten Sicherheitseffekt erzielen zu können. So sind die im aktuellen Gesetzentwurf neu eingefügten Begriffe „Unternehmen im besonderen öffentlichen Interesse" sowie „erhebliche volkswirtschaftliche Schäden" näher zu bestimmen. Der Versuch einer näheren Bestimmung von „Wertschöpfung" bezieht sich z. B. nur auf deutsche

Unternehmen, nicht aber, was dem Zweck des Gesetzes eher entspräche, auf die Wertschöpfung auf dem Gebiet der Bundesrepublik Deutschland. Es gibt einen Klärungsbedarf bei der Definition, die in diesem Fall ein Maß (Wertschöpfung) ohne Bezug zum originären Schutzzweck der Vorschriften (Versorgungssicherheit der Bevölkerung in Deutschland) einführt. Auch die Vorgabe, IT-Systeme nach dem „Stand der Technik" vorzuhalten, ist genauer festzulegen. Hierbei muss die Gleichbehandlung aller vom Gesetz betroffenen Unternehmen und die EU-Harmonisierung (keine Wettbewerbsnachteile) berücksichtigt werden.

3. Unverhältnismäßige Sanktionsdrohungen

Unternehmen, die in den Anwendungsbereich des Gesetzes fallen, werden mit der Androhung hoher Strafzahlungen konfrontiert. Welche Unternehmen betroffen sein könnten, ist jedoch unklar, sodass der Großteil der deutschen Wirtschaft vorauseilend tätig werden müsste, um die hohen Bußgelddrohungen zu vermeiden. Der in den Bußgeldvorschiften neu eingeführte Verweis auf das Ordnungswidrigkeitengesetz kann das aktuelle Sanktionsmaß von 100.000 Euro auf 20 Millionen Euro, also um das 200-Fache erhöhen. Das halten wir für unverhältnismäßig und korrekturbedürftig.

Die Paketdienste investieren laufend in Digitalisierung und in sichere IT-Systeme, die schon im eigenen Interesse auch geprüft werden. Die mit dem Entwurf vorgeschlagenen Vorschriften und der pauschale Ansatz des Gesetzentwurfes verursachen jedoch einen erheblichen zusätzlichen Verwaltungsaufwand zudem werden personelle und finanzielle Kapazitäten gebunden, die dringend für die weitere Optimierung der Systeme gebraucht werden.

Vier Beispiele hierzu:

- Stand der Technik: Die pauschale Vorgabe, den „Stand der Technik" einzusetzen verpflichtet, immer das neueste Betriebssystem zu erwerben, auch wenn für die Vorgängerversion Sicherheitsupdates verfügbar und ihre Anwendung vereinbart ist. Das ist unwirtschaftlich und bindet unnötige Ressourcen.

- Anwenderhaftung: Durch die Ausrichtung auf Anwender und nicht auf Systemanbieter verlagert das Gesetz das Risiko auf die Nutzer von Soft- und Hardware, statt auf die Anbieter. Bei Fehlern des Soft- oder Hardwareanbieters können diese nicht in Haftung genommen werden. Sinnvoller ist der Ansatz „Security by Design", bei dem sichere Systembausteine zertifiziert und geprüft und deren Anbieter in Haftung genommen werden können. Betreiber kritischer Infrastrukturen, die beispielsweise Opfer des Mitte Dezember 2020 bekannt gewordenen Hackerangriffs auf den amerikanischen IT-Dienstleister SolarWinds wurden, müssen für den entstandenen Schaden selbst aufkommen. Solange im IT-Sicherheitsgesetz kein Verursacherprinzip hinterlegt ist, fehlt der Druck auf Hersteller Sicherheitslücken zu schließen.

- Meldeverfahren: Sobald eine Sicherheitslücke bekannt wird, sollten Betreiber kritischer Infrastrukturen schnellstmöglich darüber informiert werden, um eventuell nötige Vorkehrungen treffen zu können. Allerdings teilt das BSI scheinbar nur verzögert und nur ausgewählte Informationen. Damit bleibt die Schutzfunktion das BSI für die betroffene Wirtschaft lückenhaft.

- Bürokratieaufbau: Im Gesetzesentwurf wird der Anwendungsbereich des Gesetzes auf 2.000 Unternehmen geschätzt. Dem stehen auf der Verwaltungsseite alleine im BSI bis zu 200 zusätzliche Stellen gegenüber, was einem „Betreuungsverhältnis" alleine für das Melde- und Berichtswesen von 1 Mitarbeiter*in zu 10 Unternehmen entspricht.

Abschließend verweisen wir auf die zuvor genannten, bereits frühzeitig gegenüber dem BMI kommunizierten Vorschläge des UP KRITIS-Wirtschaftsrats zur Verbesserung des Gesetzentwurfs, denen wir uns anschließen.

Berlin, 10. Februar 2021