Bundesverband

Positionspapier

IT-Sicherheitsgesetz

Grundrichtung stimmt – viele Details noch offen

Stand: 11. November 2014

Der ASW Bundesverband sieht die Ansätze des IT-Sicherheitsgesetzes positiv, gleichzeitig jedoch wichtigen Verbesserungsbedarf in den Details.

Branchenspezifische Mindestanforderungen an die IT-Sicherheit

Der ASW Bundesverband begrüßt die Einführung branchenspezifischer Mindestanforderungen an die IT-Sicherheit, wenn diese von den Branchenverbänden festgelegt werden. Wir wollen keine Situation, in der Unternehmen, die verantwortungsvoll in Sicherheit investieren, einen Kosten- und somit Wettbewerbsnachteil gegenüber denjenigen haben, die sich der Verantwortung entziehen und diese notwendigen Investitionen sparen.

Die zu definierenden Standards sollten sich nach gängigen nationalen und internationalen Standards richten. **Doppelanforderungen** gilt es dabei zu vermeiden – der Gesetzentwurf geht auf diese mögliche Problematik bereits abschnittsweise ein.

Den aktuellen Gesetzesentwurf verstehen wir so, dass die jeweilige Branche und das BSI sich auf einen Standard einigen müssen. Offen bleibt jedoch die Frage, was passiert, wenn keine Einigung erzielt werden kann. Der ASW Bundesverband regt daher die Einrichtung einer **Schiedsstelle** bestehend aus Vertretern der Behörden, der Wirtschaft und der Wissenschaft an, um ggf. langwierige Rechtsstreitigkeiten zu vermeiden.

Eine schnelle Umsetzung der Sicherheitsstandards erachtet der Verband als sinnvoll. Gleichwohl erscheint eine **Umsetzungsfrist** in vielen Bereichen nicht realistisch. Der ASW Bundesverband schlägt daher vor, dass zwar grundsätzlich eine Frist von 2 Jahren einzuhalten ist. Sollte dieses Ziel jedoch für einzelne Branchen nicht erreicht werden können, kann die Frist, bei Nachweis bislang vertretbar großer Anstrengungen zur Zielerreichung, um ein Jahr verlängert werden.

Der im Gesetzesentwurf vorgesehene **Überprüfungszeitraum** von 2 Jahren sollte nochmals überdacht werden. Der ASW Bundesverband empfiehlt, dass Vertreter der Spitzenverbände und des BSI gemeinsam branchenspezifische Prüfmechanismen erarbeiten. Die Forderung des Gesetzes nach Übermittlung aller detaillierter Auditergebnisse etc. für den Fall vorliegender Sicherheitsmängel wird als zu weitgehend erachtet. Zumindest sollte dies erst bei wiederholter und andauernder Existenz schwerwiegender Sicherheitsmängel gelten. Dies entspricht auch dem Geist der pseudonymisierten Meldung bei nicht-kritischen Sicherheitsvorfällen.

Meldepflicht für IT-Sicherheitsvorfälle

Der Gesetzentwurf sieht eine pseudonymisierte Meldepflicht bereits für **Vorfälle** vor, **die kritisch sein könnten**. Der ASW Bundesverband sieht hierbei die Gefahr, dass Unternehmen, um rechtmäßig zu handeln, unzählige Vorfälle werden melden müssen, da oftmals nicht sofort erkennbar ist, ob hier eine potenzielle Gefährdung vorliegt. Das BSI könnte damit in einer Flut von Meldungen ertrinken und dabei ggf. solche übersehen, die tatsächlich wichtig sind.

Wenn der Zwang zur Meldung bleiben soll, dann müsste zumindest in der Gesetzeserläuterung festgehalten werden, dass Unternehmen kein Gesetzesverstoß vorzuhalten ist, wenn sie nachweislich nach bestem Wissen und Gewissen handeln und einzelne Vorfälle nicht melden, die sich nachträglich als potenziell gefährlich herausstellen. Hierdurch erhielten die Unternehmen die notwendige Rechtssicherheit.

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Bayerischer Platz 6 | 10779 Berlin
Telefon (030) 246 37 175 | Telefax (030) 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de

Kritische Vorfälle müssen laut Gesetzesentwurf ohne Pseudonymisierung „offen“ gemeldet werden. Der ASW Bundesverband schlägt vor, dass auch kritische Vorfälle pseudonymisiert gemeldet werden können sollten, wenn eine ständige Erreichbarkeit für Rückfragen gegeben ist. Hierdurch ergäbe sich kein Nachteil für das BSI. Gleichzeit kann die Sorge der Unternehmen, kritische Informationen könnten allzu leicht in Umlauf kommen, zu guten Teilen genommen werden. Grundsätzlich fehlt dem ASW Bundesverband auch eine frühzeitige Klarheit, welche Informationen in diesem Fall übermittelt werden müssen.

In dem Gesetzesentwurf wird für die Telekommunikationsbranche darauf eingegangen, dass keine **doppelten Meldepflichten** entstehen sollen. Zu klären bleibt, wie dies praktisch geschehen soll. Andere Institutionen müssten dann eine Meldepflicht gegenüber dem BSI erhalten. Darüber hinaus sollten analoge Regelungen auch für andere Branchen wie Energieversorgung getroffen werden.

Regelungen im Telekommunikations- und Telemediengesetz

Die Einführung des Zuverlässigkeitskriteriums des Anbieters im Telekommunikationsgesetz (§ 115 Abs.3) wird von uns begrüßt. Eine Konkretisierung durch Fallbeispiele in der Gesetzesbegründung wird jedoch empfohlen, da dies zu einer größeren Rechtsklarheit beiträgt. Beispielkriterien können auditierte Sicherheitskonzepte, Fristen für Updates und Sicherheitskontrollen sein.

Die neue Regelung im Telemediengesetz (§15, Abs.9), die erlaubt Nutzungsdaten sechs Monate zu speichern, wird von uns kritisch betrachtet. Mit dem Hintergrund der kontroversen öffentlichen Debatte zur Vorratsdatenspeicherung, empfehlen wir die derzeitige Regelung einer Speicherung von sieben Tagen beizubehalten.

Details in Verordnungen

Der Gesetzesentwurf sieht für zahlreiche Detailregelungen Verordnungen vor. Als Beispiel sei die genaue Definition der betroffenen Unternehmen genannt. Diese Verordnungen sollten in Zusammenarbeit mit den Branchenverbänden erarbeitet und dabei sichergestellt werden, dass hier ein gemeinsamer Konsens erreicht wird.

Das Wichtigste in Kürze

- Branchenspezifische Mindeststandards werden begrüßt
- Doppelanforderungen unterbinden, doppelte Meldepflichten ausschließen
- Orientierung an national und international anerkannten Standards essentiell
- Einrichtung einer Schiedsstelle notwendig
- Überprüfungszeitraum flexibler zu gestalten
- Empfehlung eines weitgehenden Verzichtes auf die Übermittlung von Schwachstellen bei Audits
- Rechtssicherheit für Meldung potenziell kritischer Vorfälle sichern
- Pseudonymisierung aller Meldungen
- Einbindung der Verbände in der Ausarbeitung der Verordnungen

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Bayerischer Platz 6 | 10779 Berlin
Telefon (030) 246 37 175 | Telefax (030) 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de