GESELLSCHAFT
FÜR INFORMATIK

Berlin, 22. Mai 2019

Stellungnahme

der Fachgruppe „ADA – Zuverlässige Software-Systeme“
der Gesellschaft für Informatik e.V.

zum Entwurf des des Bundesministeriums des Innern, für Bau und Heimat

für ein „IT-Sicherheitsgesetz 2.0“

GESELLSCHAFT
FÜR INFORMATIK

Vorbermerkung

Das IT-Sicherheitsgesetz soll den Rahmen schaffen innerhalb dessen sichere Systeme mit IT Bestandteilen (u.a. IoT) geprüft, zertifiziert, zugelassen und bei einem IT Sicherheitsvorfall (Unfall, Systemfehlverhalten, Hack) analysiert werden können, um den Fehler zu finden, der zum Vorfall geführt hat. Das Gesetz soll dem Bürger ein gutes Gefühl geben, dass es nach dem Stand der Technik sicher ist, wenn er ein Gerät mit Sicherheitszertifikat benutzt.

Um Interessenkonflikte zu vermeiden, wie sie uns in der Automobilindustrie durch die Dieselaffäre vor Augen geführt wurden, empfehlen wir aus der Luftfahrtindustrie schon lange bewährte Strukturen zur Gewaltenteilung aufzusetzen. Wir haben entsprechende Entitäten der Luftfahrt in Deutschland und USA beispielhaft in Klammern unten hinzugefügt, um zu zeigen, welche bereits bewährte Strukturen es dort gibt.

Stellungnahme der Fachgruppe ADA – Zuverlässige Software-Systeme

Wir sehen einen Mangel an Gewaltenteilung beim Thema IT Sicherheit!
Analog zur Luftfahrt fordern wir eine Aufteilung der Verantwortung in voneinander gänzlich unabhängige Entitäten:

1. Hersteller (Beispiele aus der Luftfahrt: Airbus, Boeing): Sie stellen Produkte her, die Sicherheitskriterien erfüllen sollen. Damit sie vom Markt akzeptiert werden, müssen sie Sicherheitsstandards genügen und sich einer Zulassung unterziehen.

2. Zulassungsbehörde (Beispiele aus der Luftfahrt: Luftfahrt-Bundesamt LBA, FAA): Sie definiert welche Standards erfüllt werden müssen, um ein Sicherheitszertifikat oder eine Gebrauchszulassung zu erhalten. Sie akkreditiert die unabhängigen Gutachter/Testlabore, die die Produkte gemäß den Standards zertifizieren.
Die Gutachter dürfen in keinem Abhängigkeitsverhältnis zum Hersteller oder der Organisation für die Untersuchung von IT Sicherheitsvorfällen stehen. Aufgrund des Gutachterzertifikats erteilt dann die Zulassungsbehörde das Sicherheitszertifikat oder die Gebrauchszulassung.

3. Organisation für die Untersuchung von IT Sicherheitsvorfällen (Beispiele aus der Luftfahrt: Bundesstelle für Flugunfalluntersuchung BFU, NTSB): Sie führt Buch über alle entdeckten IT Sicherheitsvorfälle. Sie veröffentlicht diese nach gesetzlich zu definierender Vorgabe und sie untersucht die Ursachen dieser Vorfälle. Letzteres kann zur Aufdeckung von Schwächen der Standards, Fehlern der Implementierung oder Mängeln bei der Zulassungsprüfung führen. Daraus kann sie Empfehlungen für die Änderung der Standards und Vorschriften ableiten. Deswegen muss diese Organisation gänzlich unabhängig von Hersteller und Zulassungsbehörde sein. Die

Auswertung des jeweils untersuchten Vorkommnisses sowie die daraus resultierende Schlussfolgerung und Sicherheitsempfehlung sollen nicht der Klärung der Schuld-bzw. Haftungsfrage dienen. Vielmehr hat die technische Untersuchung einzig das Ziel, Erkenntnisse zu gewinnen, mit denen künftige Vorfälle und Störungen verhütet werden können.

4. Die IT Sicherheitsstandards können gemeinsam von allen interessierten Seiten entwickelt und nach öffentlicher Diskussion verabschiedet werden zu dem Zwecke, dass sie von der Zulassungsbehörde als anzuwendende Standards definiert werden. In der Luftfahrt gibt es dazu die gemeinnützigen Organisationen EUROCAE in Europe und RTCA in den USA.

Das BMI soll für die Finanzierung der Zulassungsbehörde zuständig sein. Das BMWi soll für die Finanzierung der Organisation für die Untersuchung von IT Sicherheitsvorfällen zuständig sein.

Beide Bundesministerien müssen für eine ausreichende Finanzierung der Entitäten sorgen, damit sie ihre Aufgabe unabhängig und vollumfänglich erfüllen können.
Damit sind die beiden Entitäten aus unterschiedlichen Lagern und unterliegen keinem ministeriellen Interessenskonflikt.