PRESSEMITTEILUNG

Anforderungen an einen künftigen Europäischen Zertifizierungs- und Kennzeichnungsrahmen für IKT-Sicherheit: TeleTrusT - Bundesverband IT-Sicherheit e.V. kritisiert Pläne der EU-Kommission und fordert Änderungen

Berlin, 04.10.2017 - Die Europäische Kommission hat einen Regulierungsvorschlag veröffentlicht, der auch einen künftigen Europäischen Zertifizierungs- und Kennzeichnungsrahmen für IKT-Sicherheit betrifft. Er soll die Sicherheitseigenschaften von Produkten, Systemen und Diensten, die bereits in der Entwurfsphase ("security by design") integriert sind, verbessern. Die gute Absicht ist erkennbar, zumal ein erhöhter Schutz der Bürger und Unternehmen durch bessere Cybersicherheits-Vorkehrungen erstrebenswert ist. Dennoch hat der Vorschlag erhebliche fachliche Mängel. Darüber hinaus fehlt es an Offenheit und Transparenz, wie man sie von Normensetzung erwarten kann, die der Unterstützung der EU-Gesetzgebung dienen soll.

https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF

TeleTrusT-Positionen:

Der Vorschlag wird als notwendiger und grundlegender Beitrag zur Cyber-Sicherheit in digitalen Infrastrukturen angesehen. Die Entwicklung und der Einsatz der neuen Digitaltechnologien mit ihren erhöhten inhärenten Risiken bedürfen eines nachhaltigen Rahmenplans, der einschlägige technische Normen und Zertifizierungsdienste im "Digitalen Binnenmarkt" bereitstellt. Dies führt zu sicheren Produkten, Systemen und Diensten bereits vor Markteintritt und während ihres gesamten Lebenszyklus. Der Vorschlag orientiert auf umfassende Befugnisse für die EU-Kommission, zu entscheiden, welche Cybersicherheits-Schemata innerhalb der EU erforderlich sind, welche Normen für ein Schema gelten und welche Produkt- oder Dienstetypen erfasst werden. Ein Schema kann Smart Meters, IoT-tragbare Geräte, Datenbanken, Cloud-Dienste, Smartphones etc. umfassen, in der Tat also jedes IKT-Produkt. Sollten keine anwendbaren Normen für ein Schema vorhanden sein, werden die Anforderungen, die zur Zertifizierung eines Schemas erfüllt werden müssen, ohne Konsultation in das Schema integriert.

Der EU-Agentur für Network and Information Security (ENISA) wird das Vorschlagsrecht für Schemata zugeschrieben, aber die endgültige Entscheidung, wann ein neues EU-Schema erforderlich ist und welche Produkte und Dienste erfasst werden, bleibt ausschließlich in der Hand der EU-Kommission. Es gibt keine Beteiligung der Mitgliedstaaten, des Europäischen Rates, des Europäischen Parlaments, nationaler Normenorganisationen, gesellschaftlicher Interessengruppen oder der Industrie. Dass ein Schema zunächst freiwillig anzuwenden ist, ist ein schwaches Argument zur Verteidigung einer Verordnung, die der EU-Kommission zu viel Macht verleiht.

Der neue Rahmenplan kann nur unter folgenden Voraussetzungen gelingen:

1. Der Rahmenplan migriert vorhandene Zertifizierungsinfrastrukturen ohne Betriebsunterbrechung, besonders SOGIS-MRA ("Senior Officials Group Information Systems Security - Mutual Recognition Arrangement", aktuell mit 14 Mitgliedstaaten, kompetenten Schemata und privaten Prüfstellen; initiiert Anfang der neunziger Jahre durch die EU-Kommission, große Industrieanerkennung und Weltmarktposition).

2. Zertifizierung muss auf offene Normen setzen, die Wettbewerb zwischen Prüfstellen bzw. Schemata sowie zwischen den geeignetsten Sicherheitslösungen für ein festgelegtes Sicherheitsproblem ermöglichen.

3. Der Rahmenplan kann Ergebnisse analog zum rasanten Tempo technologischer Änderungen erzielen und die Marktbedürfnisse rechtzeitig und wirtschaftlich befriedigen.

4. Eine leistungsstarke Beziehung zwischen dem Rahmenplan und den Europäischen Normungsorganisationen (ESO) kann aufgebaut werden.

5. Was die IKT-Sicherheitsaspekte betrifft, werden die Richtlinien und Verordnungen der EU-Kommission für jeden vertikalen Digitalmarkt die Anforderungen an geeignete technische Sicherheitsnormen und Zertifizierungen prüfen und das Certification Board entsprechend regelmäßig einbeziehen. Falls ein Vertikalsektor nicht harmonisiert werden kann, wird die Vereinheitlichung der technischen Normen und Zertifizierungen schwer erreichbar sein. IT-Sicherheit betrifft auch Netzwerksicherheit, die öffentliche bzw. nationale Sicherheit sowie die digitale Souveränität. IT-Sicherheit ist nicht nur Anliegen des Digitalbinnenmarktes, sondern auch der Mitgliedsstaaten. Das gilt insbesondere für Kryptonormen und die Qualifikation der Prüfstellen.

Deshalb muss ein künftiges Europäisches IKT-Zertifizierungs- und Kennzeichnungsrahmenwerk

- ein "European Cyber Security Certification Board" etablieren, besetzt mit Vertretern der Mitgliedsstaaten in Abstimmung mit den ESO und dem European Data Protection Board (EDPB), mit der Verantwortung, seine Themenbereiche sowie Arbeitsgruppen aufzubauen,
- die Generaldirektionen der EU-Kommission bei der Entwicklung der Kommunikationen, Richtlinien und Verordnungen für Vertikalsektoren unterstützen, so dass Standardisierung und Zertifizierung in einer sehr frühen Phase vorbereitet werden und Synergien zwischen den vertikalen Digitalisierungssektoren erzeugt werden können,
- SOGIS-MRA von einer Aktivität einzelner Mitgliedsstaaten in eine gesamteuropäische Aktivität migrieren,
- die Unabhängigkeit der Standardisierung und Auswertung gewährleisten, indem ein geeignetes Akkreditierungssystem für Prüfstellen bereitgestellt wird und die Akkreditierungsverordnung mit Hilfe einer zusätzlichen sektorspezifischen Ausnahmeregelung gemäß Erwägungsgrund Nr. 5 in 765/2008 verbessern,
- eine Rolle für die ENISA etablieren, um die Sekretariats- und organisatorische Infrastruktur für das (neue) European Cyber Security Certification Board bereitzustellen,
- Mitgliedsstaaten und Industrie unterstützen, um Innovationen für bessere IT-Sicherheit einzuleiten und Wettbewerbsgleichheit für die europäische Industrie im Weltmarkt zu schaffen.