Berlin, 13.04.2021

Stellungnahme
und Handlungsempfehlungen

zum Eckpunktepapier "Fortschreibung der Cyber-Sicherheits-strategie für Deutschland"

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Ansprechpartner für Rückfragen:

Dr. Holger Mühlbauer
Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Geschäftsführer
holger.muehlbauer@teletrust.de

Zu Handlungsfeld 1 - Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung

("Sichere "elektronische Identitäten" sind als elementarer Grundstein der Cyber-Sicherheit Voraussetzung für das hoheitliche Handeln des Staates im digitalen Zeitalter. Die Festlegung von Anforderungen an eID-Verfahren, sowie deren Absicherung sollten daher durch den Staat erfolgen.")

Kommentar TeleTrusT: Dies sollte auf solche Bereiche beschränkt bleiben, wo hoheitliches Handeln des Staates wirklich erforderlich ist. Nicht jeder Log-in oder Account erfordert eine Regulierung durch den Staat.

Zu Handlungsfeld 2 - Gemeinsamer Auftrag von Staat und Wirtschaft

Kommentar TeleTrusT: Die Wirtschaft erscheint in diesem Handlungsfeld als Objekt dargestellt, nicht als souveränes Subjekt - d.h. der Staat bestimmt und die Wirtschaft führt aus. Gemeinsames Handeln sollte dagegen auf Augenhöhe erfolgen. Es geht um die gemeinsame Umsetzung gemeinsamer Ziele. Das setzt gegenseitiges Vertrauen und gegenseitigen Respekt voraus.

Zu Handlungsfeld 3 - Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur

("Es soll eine ausgewogene, behördenübergreifende Strategie zum Umgang mit Schwachstellen nach den jeweils geltenden gesetzlichen Vorgaben bei den Strafverfolgungs- und Sicherheitsbehörden, geschaffen werden. Damit sollen auch in Zukunft über bereits vorhandene interne Behördenvorgaben hinaus die Interessen der Cyber- und Informationssicherheit sowie der Strafverfolgungs- und Sicherheitsbehörden in einen angemessenen Ausgleich gebracht werden.")

Kommentar TeleTrusT: Sofern das bedeutet, dass auch zukünftig die Möglichkeit besteht, erkannte Schwachstellen nicht öffentlich zu machen, sondern für Zwecke der Strafverfolgungs- und Sicherheitsbehörden geheim zu halten, konterkariert dies die Bemühungen für mehr IT-Sicherheit und ist nicht akzeptabel.

("Um die Verwundbarkeit des zunehmend digitalisierten Wahlumfelds und der Wahlinfrastruktur zu reduzieren, soll die Cyber-Sicherheit im Umfeld von Wahlen erhöht werden.")

Kommentar TeleTrusT: Der Schutz der Wahlen hat sicherlich hohe Bedeutung. Dennoch ist das zu kurz gesprungen. Beeinflussung von Stimmungen und Meinung durch gezielte Manipulation und Falschinformation über Online-Foren und soziale Netze, auch aus dem Ausland, finden auch ganz unabhängig von Wahlen statt und sollte unabhängig von Wahlen bekämpft werden. Das ist keine eigentliche Aufgabe von IT-Sicherheit, da die Bedrohung aber aus dem Cyberraum kommt, gehören Gegenmaßnahmen in die Cyber-Sicherheitsstrategie.

("Der Einsatz quantentechnologischer Systeme zur Gewährleistung eines hohen IT-Sicherheitsniveaus soll vorangetrieben werden.")

Kommentar TeleTrusT: Auch der Einsatz von Post-Quantum Cryptography ist ein wichtiges zukünftiges Element zur Sicherstellung der digitalen Souveränität an und sollte mit aufgenommen werden.

Zu Steuerung der CSS 2021

Kommentar TeleTrusT: Es wird unterschieden zwischen Strategischem Controlling (Aufgabe des BMI) und der operativen Umsetzung, die "eigenständig in der Verantwortung der zuständigen Stellen" erfolgen soll. Wer verantwortet die Umsetzung von ressortübergreifenden Strategischen Zielen? Das BMI koordiniert nur. Falls ressortbezogen, bedeutet dies geteilte Verantwortung, was in aller Regel nicht gut funktioniert. Hier wäre eine zentrale Aufgabe für ein Digitalministerium.