Sichere Lieferketten sind Grundlage für vertrauenswürdige IT als Element der digitalen Souveränität

Zusammenfassung des Ideenpapiers „Etablierung und Aufrechterhaltung sicherer Lieferketten für vertrauenswürdige IT der Bundeswehr“ des Expertenkreises 2 im Gesprächskreis 4 des strategischen Industriedialogs

Im Rahmen des strategischen Industriedialogs hat das BMVg gemeinsam mit dem BDSV und dem Bitkom im Expertenkreis 2 *„Nationale Schlüsseltechnologien und -fähigkeiten für Entwicklung, Realisierung und Lebenszyklusunterstützung vertrauenswürdiger IT der Bundeswehr“ (Kurzform: „Vertrauenswürdige IT“)* einen offenen und unverbindlichen Dialog ermöglicht, der sich außerhalb konkreter Beschaffungsabsichten befindet und keine als Verschlusssache oder kommerziell-vertraulich eingestuften Informationen behandelt.

Kernaussage:

Sichere zuverlässige Lieferketten sind unerlässliche Schlüsselfähigkeiten[1], um vertrauenswürdige IT herstellen, bereitstellen und über den Lebenszyklus hinweg aufrecht erhalten zu können. Die Fähigkeit zur Etablierung und Aufrechterhaltung sicherer Lieferketten als Schlüsselfähigkeit sollte im Rahmen der nationalen Anstrengungen analog zu den nationalen Schlüsseltechnologien[2] angemessen Berücksichtigung finden.

<u>Weitere Ideen und Empfehlungen</u>

- *Für die Absicherung der Lieferkette über den gesamten Produktlebenszyklus sind der Einbezug spezifischer Rahmenbedingungen für Einsatz und Nutzung sowie gemeinsame Standards und Methoden zwischen GB BMVg und Industrie unerlässlich. Hierbei sind neben einzelnen IT-Technologieprodukten auch komplexe Gesamtsysteme und Dienstleistungen mit Technologieanteil (z.B. *as a Service) zu betrachten.*
- *Die in den Detailbetrachtungen identifizierten spezifischen Handlungsfelder (z.B. Operationalisierung und Regulierung, ggf. Erstellen einer Metrik) sollten weiter betrachtet werden. Hierzu sind geplante sowie bereits laufende Forschungs- und Entwicklungsvorhaben im nationalen und internationalen Bereich mit einzubeziehen.*
- *Eine Etablierung und Aufrechterhaltung sicherer Lieferketten inklusive vollständiger Transparenz zu Herkunft und Eigenschaften aller Elemente (einschließlich der einzelnen elektronischen Bauteile) stellt eine enorme Herausforderung dar. Für bereits vorhandene Systeme erscheint eine „nachträgliche“ Berücksichtigung dieser Aspekte z.B. bis zu den einzelnen elektronischen Bausteinen unrealistisch. Deshalb sind stattdessen im Rahmen des Lebenszyklus Maßnahmen einzuführen mit denen Risiken jeweils erkannt, bewertet und mitigiert werden können.*
- *Die für sichere Lieferketten relevanten technischen Informationen sollten digital erfasst, zwischen den beteiligten Stellen unter Nutzung offener Standards ausgetauscht und über den Lebenszyklus hinweg verwendet werden.*

Es kommt auch zukünftig darauf an, die Herausforderungen bzgl. der Verfügbarkeit ausreichend vertrauenswürdiger IT zur Sicherstellung der „digitalen Souveränität“ für alle Beteiligten nachhaltig mit der notwendigen Qualität und Agilität, aber auch wirtschaftlich und synergetisch zu lösen. Hierbei sind die jeweiligen Kompetenzen und Rahmenbedingungen sowie Sachzwänge/Interessen aller Beteiligten stets angemessen transparent zu machen und zu berücksichtigen.

Die Ergebnisse des fachlichen Ideenaustauschs und der Diskussionen im EK 2 spiegeln die teils komplementären Fähigkeiten und Schwerpunkte wider, die sich durch die Rolle als potenzieller Auftraggeber/Forderer (BMVg/GB BMVg) bzw. potenzieller Auftragnehmer/Bereitsteller (Industrie) im Bereich Cyber/IT herausbilden.

Weitere Details und begleitende Informationen können dem durch die Leitung BMVg und den Industrieverbänden gebilligten Ideenpapier entnommen werden. Das vollständige Dokument ist abrufbar unter:

---

[1] Definition Schlüsselfähigkeiten gem. Ideenpapier „Nationale Schlüsseltechnologien und -fähigkeiten für Entwicklung, Realisierung und Lebenszyklusunterstützung vertrauenswürdiger IT der Bundeswehr“: Unter Schlüsselfähigkeiten im Kontext Cyber/IT werden die Fähigkeiten verstanden, welche unter Nutzung von Technologieelementen (sowohl Schlüsseltechnologien als auch Nicht-Schlüsseltechnologien) elementar für die Konzeption, Realisierung und Nutzung sowie Lebenszyklusunterstützung von vertrauenswürdigen Informationssystemen, einzelnen Systemkomponenten oder Systemfunktionalitäten sind.

[2] Definition Schlüsseltechnologien: Schlüsseltechnologien sind Technologien, die aus den außen-, sicherheits- und europapolitischen Interessen Deutschlands, dem militärischen Bedarf der Bundeswehr, den Bündnisverpflichtungen sowie der Verantwortung Deutschlands abgeleitet und regelmäßig überprüft werden.
(siehe auch Ideenpapier „Vertrauenswürdige IT“ https://www.bmvg.de/de/aktuelles/vertrauenswuerdige-it-bundeswehr-140710)

https://www.bmvg.de/de/aktuelles/vertrauenswuerdige-it-bundeswehr-140710
https://www.bdsv.eu/aktuelles/aktuelle-meldungen.html
https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Verteidigung/index.jsp

Über den Gesprächskreis Innovation Cyber/ IT im Strategischen Industriedialog

Auf Initiative der Leitung BMVg vom Juni 2017 ist der strukturierte Dialog zwischen dem BMVg und dem Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie (BDSV) zum Strategischen Industriedialog (SID) weiterentwickelt worden. Dessen Kern besteht aus sechs Gesprächskreisen (GK). Der GK 4 „Innovation Cyber/IT“, wird von Seiten der Industrie gleichberechtigt zum BMVg durch den Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) und BDSV betreut, wobei die industrielle Leitung vom Bitkom und die BMVg seitige Leitung durch Abteilungsleiter CIT gestellt wird. Der GK 4 „Innovation Cyber/IT“ hat auf Fachebene in einem Expertenkreis 2 (EK 2) einen Ideenaustausch zum Thema „vertrauenswürdige IT“ mandatiert. Die thematische Schwerpunktsetzung des EK 2 greift die zunehmende Abhängigkeit sämtlicher Lebensbereiche von Informationstechnologie (IT) und die Notwendigkeit der Stärkung der digitalen Souveränität auf.