Ideenpapier

„Etablierung und Aufrechterhaltung sicherer Lieferketten für vertrauenswürdige IT der Bundeswehr“

Ergebnisse des Expertenkreises 2 (EK2)

im Rahmen des Gesprächskreises Innovationen Cyber/IT (GK4)
des strategischen Industriedialoges

zwischen
dem Bundesministerium der Verteidigung, Abteilung Cyber/Informationstechnik
und dem Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V.
und Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.

Version: Mitgeprüfte und mitgezeichnete Version zur Veröffentlichung
Stand: 08.06.2021

Einstufung: Offen –Zur freien Verwendung nach Maßgabe des strategischen Industriedialoges

Bundesministerium der Verteidigung
Abteilung Cyber/Informationstechnik

BDSV
Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V.

bitkom

BMVg
Bundesministerium der Verteidigung, Abteilung Cyber / Informationstechnik (CIT)
Stauffenbergstraße 18
10785 Berlin

BDSV e.V.
Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e. V.
Friedrichstraße 60
10117 Berlin

Bitkom e. V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10, 10117 Berlin

Hinweise

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung der Herausgeber zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers.

Inhaltsverzeichnis

Seite

1 Vorwort 5

2 Zielsetzung des Expertenkreises 6

3 Ergebnisse im Überblick 8

4 Detailbetrachtungen 11

4.1 Konkrete Gefährdungsszenarien hinsichtlich Etablierung und Aufrechterhaltung sicherer Lieferketten für vertrauenswürdige IT der Bundeswehr 18

4.1.1 Betrachtung des Produktlebenszyklus 22

4.1.2 Manipulationen/Fehler im Fertigungsprozess Mikroelektronik inkl. Firmware 23

4.1.3 Manipulationen/Fehler in COTS Hardware-Komponenten 26

4.1.4 Manipulationen/Fehler in weiterverwendeten Software-Komponenten Dritter und Software-Lieferketten 29

4.1.5 Manipulationen/Fehler in eigenentwickelten Software-Komponenten 33

4.1.6 Manipulationen/Fehler in Consumer-IT 35

4.2 Internationale und nationale Standards 37

5 Handlungsempfehlung 38

5.1 Analyse/Einordnung in internationalen Kontext 40

5.2 Nutzung offener Standards und Initiativen 41

5.2.1 Zertifizierung von Organisationen 42

5.2.2 Transparenz zu Produktbestandteilen 42

5.3 Vorschlag für eine Metrik „schutzbedarfsabhängige Anforderungen an Lieferkette und deren Absicherung" 43

5.4 Regulierungs- und Operationalisierungsbedarf 45

5.5 Umgang mit den Handlungsempfehlungen 47

6 Urheberschaftsnachweis 48

1 Vorwort

Gemeinsames Kapitel BMVg (BMVg CIT) / Industrieverbände (BDSV und Bitkom)

Im Rahmen des strategischen Industriedialoges, geführt zwischen BMVg und BDSV, zu den Themen der Agenda Rüstung wird seit Januar 2015 ein intensiver und konstruktiver Austausch zwischen der Amtsseite und der Industrie/Wirtschaft geführt. Mit dem am 29. Juni 2015 vorgelegten Ergebnisbericht wurden die initialen Ergebnisse vorgestellt und eine weiterhin enge Kooperation bei der Umsetzung der definierten Handlungsempfehlungen angekündigt.

Mit Tagung des verbändeübergreifenden Gesprächskreises 4 „Innovation in den Bereichen Cyber und Informationstechnologie der Bundeswehr“ vom 05. März 2020 wurde der bereits identifizierte Handlungsbedarf für den Themenbereich der Etablierung und Aufrechterhaltung sicherer Lieferkette vertrauenswürdige IT priorisiert und seitdem auf Fachebene im Expertenkreis „Nationale Schlüsseltechnologien und -Fähigkeiten für Entwicklung, Realisierung und Lebenszyklusunterstützung vertrauenswürdiger IT der Bundeswehr“ (EK2) diskutiert. Hierbei liegt der Fokus auf mittel bis langfristig wirkende Maßnahmen mit nachhaltigem Nutzen.

Für den Expertenkreis wurden vom BMVg und seinem Geschäftsbereich sowie von den Verbänden der Industrie/Wirtschaft ständige Vertreterinnen bzw. Vertreter benannt. Die Leitung des EK2 erfolgt gemeinsam durch eine Vertreterin des BMVg[1] und einen Vertreter der Verbände, der vom Bitkom gestellt wird. Die beiden beteiligten Verbände BDSV[2] und Bitkom[3] haben eine gemeinsame Position und Ideen in das vorliegende Dokument eingebracht.

Das vorliegende Dokument enthält die Ergebnisse des EK2 aus der Periode März 2020 bis März 2021 und basiert auf den Beiträgen der beteiligten Teilnehmenden. Dieses Dokument stellt den Gesamtbeitrag GK4 EK2 zur Fortführung und Detaillierung des Diskussionsprozesses dar und bildet eine unverbindliche Grundlage zur Anregung weiterer Schritte.

Berlin, im Juni 2021

Bundesministerium der Verteidigung (BMVg), Abteilung Cyber/Informationstechnik (CIT)

Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V. (BDSV)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom)

[1] Siehe https://www.bmvg.de/de/themen/cybersicherheit

[2] Siehe https://www.bdsv.eu/themen/cyber-it.html

[3] Siehe https://www.bitkom.org/Bitkom/Organisation/Gremien/Verteidigung.html

2 Zielsetzung des Expertenkreises

Gemeinsames Kapitel BMVg (BMVg CIT) / Industrieverbände (BDSV und Bitkom)

Im Rahmen der Digitalisierung werden alle Lebensbereiche zunehmend von Informationstechnologie (IT) durchdrungen (z.B. Internet of Things oder Industrie 4.0). Qualität und Quantität von Cyberangriffen nehmen in allen Bereichen zu. Das Eckpunktepapier zum Ausbau der digitalen Souveränität im GB BMVg vom 28. August 2020 definiert „digitale Souveränität" als die erforderlichen Kontroll- und Handlungsfähigkeiten im CIR, um den verfassungsgemäßen Auftrag der Bundeswehr sicher, selbstbestimmt und frei von ungewollter Einflussnahme durch Dritte ausüben zu können. Die Nutzung vertrauenswürdiger IT-Hard- und Software (inkl. Firmware) im Geschäftsbereich BMVg (GB BMVg) ist eine entscheidende Grundlage, um den zunehmenden Angriffen entgegen zu wirken und ein selbstbestimmtes staatliches Handeln im Cyber- und Informationsraum zu ermöglichen.[4]

Die Strategische Leitlinie Digitalisierung des BMVg vom 31. März 2017 führt im Zusammenhang mit dem Thema „digitale Souveränität" bezogen auf die Verteidigungsindustrie auf Seite 13 wie folgt aus: *„Die Bundesregierung hat sich im Rahmen der wachsenden Europäisierung der Verteidigungsindustrie zum Erhalt nationaler verteidigungsindustrieller Schlüsseltechnologien[5] bekannt. Diese Technologien sind besonders wichtig und erhaltenswert, deren Verfügbarkeit ist aus nationalem Sicherheitsinteresse zu gewährleisten, ggf. auch in Abstimmung und Zusammenarbeit mit den europäischen Partnern. Es gilt, definierte Schlüsseltechnologien im Schulterschluss mit anderen Ressorts und der Wirtschaft zu entwickeln oder zu erhalten. Hierdurch können eine eigene „digitale Souveränität" erreicht und erhalten sowie die erforderlichen militärischen Fähigkeiten und die Versorgungssicherheit der Bundeswehr sowie die Rolle Deutschlands als zuverlässiger Kooperations- und Bündnispartner technologisch und wirtschaftlich gesichert werden."*

Grundlage hierfür ist auch die Erkenntnis, dass keine einzelne Organisation - weder akademisch, behördlich noch industriell - die Herausforderungen der digitalen Souveränität sowie Informations- und Cybersicherheit allein lösen kann, sondern es hier der arbeitsteiligen Kooperation bedarf. Darüber hinaus werden Technologien und Fähigkeiten in Abhängigkeit von internationalen Standards und dem IT-Massenmarkt nur bedingt national bereitgestellt werden können, so dass nicht nur interdisziplinäre, sondern auch internationale Zusammenarbeit notwendig ist.

Der Expertenkreis 2 unterliegt den Rahmenbedingungen eines offenen Dialoges, befindet sich außerhalb konkreter Beschaffungsabsichten und behandelt keine als Verschlusssache oder kommerziell-vertraulich eingestuften Informationen. Unter diesen Rahmenbedingungen finden Diskussionen über die grundsätzlichen Vorstellungen und Planungen des BMVg (inkl. GB) und der Industrie (vertreten durch die genannten Verbände) hinsichtlich potenzieller nationaler Interessen in Bezug auf vertrauenswürdige IT beratend statt. Dabei treffen die beteiligten Organisationen und deren Vertreter grundsätzlich Aussagen für den eigenen Zuständigkeits- und Wirkungsbereich, mit der Zielsetzung der Formulierung gemeinsamer Ideen, soweit dies gemeinsam vertreten werden kann.

Im Fokus stehen daher nationale Schlüsseltechnologien und -Fähigkeiten für Entwicklung, Realisierung und Lebenszyklusunterstützung vertrauenswürdiger IT der Bundeswehr bei Schaffung eines

[4] Siehe dazu auch „Eckpunktepapier zum Ausbau der digitalen Souveränität im GB BMVg", Herausgeber: BMVg CIT I 1, vom 28.08.2020.
[5] 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)

gemeinsamen Verständnisses und darauf aufbauender Vorschläge zur Verbesserung der digitalen Souveränität.

Sichere zuverlässige Lieferketten sind unerlässlich, um vertrauenswürdige IT herstellen, aber auch um vertrauenswürdige IT-Systeme auf Basis von unterschiedlich vertrauenswürdigen IT-Komponenten bereitstellen und über den Lebenszyklus hinweg aufrecht erhalten zu können. Das Etablieren und Aufrechterhalten der sicheren Lieferkette, aber auch die entsprechend sichere Systemintegration, der Systembetrieb und die Lebenszyklusunterstützung sind unerlässliche Schlüsselfähigkeiten[6] zur Aufrechterhaltung und zum Ausbau der digitalen Souveränität.

Der Expertenkreis 2 beleuchtet die sich ergänzenden Sichtweisen der Amtsseite und der Industrie, um eine vollständige Gesamtschau zu erhalten und durch deren Bewertung eine Ableitung von Maßnahmen bzw. Handlungsempfehlungen zu ermöglichen. Während der Arbeit des Expertenkreises an diesem Thema wurden weitere erfolgreiche Angriffe auf Lieferketten öffentlich bekannt, die den Handlungsbedarf diesbezüglich unterstreichen.

Im Juni 2020 wurden durch das Landesamt für Verfassungsschutz Hamburg[7] und das Bundesamt für Verfassungsschutz[8] davor gewarnt, dass Digitalisierung in der maritimen Industrie Angriffsvektoren für Spionage und Sabotage durch fremde Staaten eröffnet. Hierbei steht das konkrete Risiko im Fokus, dass die Software maritimer Navigationssysteme bereits bei der Übergabe Malware enthalten bzw. diese auch in Update-Prozessen oder per Fernsteuerung gezielt eingespielt werden kann. Diese Software ist mit anderen sensitiven Systemen des Schiffs (z.B. Sensoren, Autopilot) vernetzt und hat somit Zugriff auf sensitive Informationen und kritische Funktionen. Hersteller von maritimen Navigationssystemen können in ihren Herkunftsländern weitreichender Einflussnahme der dortigen Nachrichtendienste ausgesetzt sein. Dies gilt insbesondere für Länder mit enger Verbindung zwischen Nachrichtendiensten und Wirtschaft.

In der Öffentlichkeit ab Dezember 2020 sichtbar wurde der Angriff auf das Produkt Orion des Softwareherstellers SolarWinds. In ein offizielles Update für diese weltweit häufig genutzte Netzwerkmanagementplattform wurde eine Malware eingeschleust, der bei der Installation des Updates auf das Zielsystem gelangte, wodurch Angreifende Zugriff auf die Systeme der nutzenden Organisationen erlangen konnten und diese Hintertür auch ausgenutzt haben.[9]

In einem anderen Beispiel vom Februar 2021 wurden mehrere Schwachstellen im weit verbreiteten Wifi-Modul RTL8195A[10] des Herstellers Realtek Semiconductor Corp. entdeckt, deren Ausnutzen einen Fernzugriff auf das Modul ermöglichen können.[11]

---

[6] 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.

[7] https://www.hamburg.de/innenbehoerde/schlagzeilen/13992656/spionage-sabotage-maritime-navigation

[8] https://www.wirtschaftsschutz.info/SharedDocs/Kurzmeldungen/DE/Spionage/Sensibilisierung_der_maritimen_Wirtschaft.html

[9] https://www.heise.de/news/Cyberangriffe-gegen-US-Ministerien-Moskau-unter-Verdacht-4988355.html
https://us-cert.cisa.gov/ncas/alerts/aa20-352a
https://amp-theguardiancom.cdn.ampproject.org/c/s/amp.theguardian.com/commentisfree/2020/dec/23/cyber-attack-us-security protocols

[10] https://www.realtek.com/en/products/communications-network-ics/item/rtl8195am

[11] https://www.vdoo.com/blog/realtek-rtl8195a-vulnerabilities-discovered
https://thehackernews.com/2021/02/critical-bugs-found-in-popular-realtek.html?m=1

3 Ergebnisse im Überblick

Gemeinsames Kapitel BMVg (CIT)/Industrieverbände (BDSV und Bitkom)

Zu Beginn der Arbeit des EK 2 zum Thema bestand im Gesprächskreis 4 „Innovation in den Bereichen Cyber und Informationstechnologie der Bundeswehr“ folgende Einschätzung hinsichtlich der Fähigkeiten für die Etablierung und Aufrechterhaltung sicherer Lieferketten für vertrauenswürdige IT der Bundeswehr: In Bezug auf vertrauenswürdige IT-Komponenten für IT der Bundeswehr sind national grundsätzlich ausreichende Fähigkeiten vorhanden, und dieser Teilbereich scheint entsprechend beherrschbar. Im Bereich der Integration von aus nationaler Fertigung stammenden Elementen in Elemente vom Weltmarkt (z.B. Hardware und Software) ist nationales Know-how grundsätzlich vorhanden, allerdings nicht in der notwendigen Kapazität querschnittlich über den gesamten Prozess hinweg ausgeprägt.

Das Vorhandensein sowie der Auf- und Abbau von Kompetenzen und Know-how und den notwendigen konzeptionellen und praktischen Fähigkeiten im Bereich der sicheren Lieferkette folgt – wie bei der IT - wesentlich der Beschaffenheit des Marktes, dabei sind Fähigkeiten zur Prüfung und Verifikation eingeschlossen. Die Anforderungen an die IT des Massenmarktes einerseits und die für den Bereich der staatlich zu schützenden Verschlusssachen sowie kritischer Infrastrukturen und missionskritischer Anwendungen andererseits unterscheiden sich erheblich. Dies bezieht sich sowohl auf die regulatorischen Vorgaben als auch auf das z.Zt. adressierbare Volumen der nationalen wie europäischen regulierten Märkte sowie auf die Einsatzumgebung, den Lebenszyklus und schließlich die Auswirkungen im Fall von Fehlfunktionen. Entsprechend diesen unterschiedlichen Anforderungen hat sich der Markt entwickelt.

Bestehende Regularien und Standards, und damit die Sicherheit der Produkte und Komponenten, werden als Anforderung verstanden und abhängig von der Ausrichtung auf Marktsegmente hinsichtlich Haftung und Regulierung in einem notwenigen Mindestmaß berücksichtigt. Hinsichtlich der Absicherung von Lieferketten bzw. Teilelementen der Lieferketten sind Regulierungen für spezifische Komponenten und etablierte Standards bzw. Best Practices für Teilaufgaben vorhanden.

Es gilt, die benötigten Kompetenzen zur querschnittlichen Etablierung und Aufrechterhaltung der sicheren Lieferkette ausgehend von z.Zt. vorhandenen Kompetenzen nachhaltig zu entwickeln. Vor dem Hintergrund auch längerfristig begrenzter Verfügbarkeit von Ressourcen (national sowie international) und der zunehmenden Auswirkungen digitaler Konvergenz und Abhängigkeiten von globalen Marktmechanismen müssen die Schwerpunkte mit Bedacht gewählt und im Vorgehen Prioritäten gesetzt werden. Durch sowohl die Fokussierung auf Schwerpunkte als auch die Priorisierung sollen grundsätzliche und regelmäßig zu aktualisierende Risikobetrachtungen berücksichtigt werden, um aktuelle und zukünftige Risiken angemessen adressieren zu können. Hierzu bedarf es gemeinsamer Methoden und Sichtweisen.

Deutsche Hersteller müssen ihre Lösungen und Produkte auf dem internationalen Markt absetzen können, um die notwendigen Investitionen zu finanzieren. Der Geschäftsbereich des BMVg ist darauf angewiesen neben nationalen Produkten und Lösungen auch auf das Angebot des Weltmarkts zur Deckung seines Bedarfs zurückgreifen zu können. Komplexe integrierte Systeme bestehen i.d.R. aus dem Verbund nationaler und internationaler Komponenten. Es sind sowohl solche Komponenten enthalten, die spezifisch für Hochsicherheit (z.B. VS-IT), missionskritische Funktionalität und militärische Anwendungen entwickelt wurden, als auch handelsübliche Komponenten vom Weltmarkt,

die jedoch regelmäßig auch in spezifischen Komponenten militärischer IT enthalten sind. Eine Konzentration der Betrachtungen zur Absicherung der Lieferketten nur auf den nationalen Markt ist deshalb nicht zielführend. Gleichzeitig ist festzustellen, dass die direkten Einflussmöglichkeiten auf den Weltmarkt begrenzt sind. Da allerdings auch die NATO[12] selber sowie NATO-Staaten-Partner und die europäische Gemeinschaft[13] sowie PESCO-Partner[14] vor konzeptionell und operationell ähnlichen Herausforderungen hinsichtlich der sicheren Lieferkette stehen, ist davon auszugehen, dass hier in der Zukunft ein internationaler Bedarf und damit auch ein entsprechendes Marktumfeld und Ökosystem mit Chancen entstehen werden.

Die Ergebnisse der Arbeiten des Expertenkreises 2 spiegeln die teils komplementären Fähigkeiten und Schwerpunkte wider, die sich durch die Rolle als Auftraggeber/Forderer bzw. Auftragnehmer/Bereitsteller zwangsläufig herausbilden. Hierbei ist zu berücksichtigen, dass es sich bei den Lösungen nicht nur um IT-Komponenten oder -Systeme handelt, sondern vielmehr um komplexe und hochintegrierte Systeme. Vor diesem Hintergrund kommt der EK2 zu folgenden Ergebnissen:

- Die zu Beginn der Arbeit durch den Gesprächskreis formulierte Selbsteinschätzung wird bestätigt: Grundsätzlich sind national ausreichende Fähigkeiten zur Herstellung von Komponenten und Aufrechterhaltung einer sicheren Lieferkette vorhanden. Auch das Know-How zur Integration von nicht-nationalen Komponenten ist grundsätzlich vorhanden. Allerdings sind die Kapazitäten zur Adressierung zukünftiger Herausforderungen nicht ausreichend ausgeprägt und die querschnittliche Betrachtung sicherer Lieferketten ist nicht ausreichend etabliert.

- Die Fähigkeit zur Etablierung und Aufrechterhaltung der sicheren Lieferkette als Schlüsselfähigkeit sollte im Rahmen der nationalen Anstrengungen angemessen Berücksichtigung finden. Siehe dazu auch die initialen Empfehlungen zur Etablierung und Aufrechterhaltenen Lieferketten im Ideenpapier „Vertrauenswürdige IT“[15].

- Die unterschiedlichen Anwendungsfälle für sichere Lieferketten und die jeweils benötigte spezifische Ausprägung sind derzeit noch nicht hinreichend konzeptionell erschlossen und entsprechend noch nicht umfänglich regulatorisch abgebildet. Zur Ermöglichung der nachhaltigen Handlungsfähigkeit und -sicherheit sollte hier präzisiert werden.

- 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.

- Bei der Absicherung der Lieferkette ist grundsätzlich der gesamte Produktlebenszyklus inklusive der Entwicklung, Produktion, Nutzung und Weiterentwicklung zu betrachten. Hierfür

[12] Siehe z.B. “TECHNICAL AND IMPLEMENTATION DIRECTIVE ON NATO SUPPLY CHAIN SECURITY REQUIREMENTS FOR COMMUNICATION AND INFORMATION SYSTEMS SECURITY ENFORCING PRODUCTS” (AC/322-D(2017)0016 (INV)) der NATO

[13] Siehe https://www.heise.de/news/Teures-Prestigeprojekt-Europas-souveraene-Chips-6010032.html

[14] Siehe z.B. https://eda.europa.eu/news-and-events/news/2020/11/05/exceed-defence-research-project-kicks-off

[15] https://www.bmvg.de/de/aktuelles/vertrauenswuerdige-it-bundeswehr-140710

sind realistische Zyklen und der Einbezug spezifischer Rahmenbedingungen sowie gemeinsame Standards und Methoden unerlässlich.

- Eine Etablierung und Aufrechterhaltung sicherer Lieferketten inklusive vollständiger Transparenz zu Herkunft und Eigenschaften aller Elemente sind wünschenswert, aber für bereits vorhandene Systeme „nachträglich“ bis z.B. zu den einzelnen elektronischen Bausteinen unrealistisch oder unwirtschaftlich. Hier sind im Rahmen des Lebenszyklus Maßnahmen vor zu sehen, um Risiken zu erkennen, zu bewerten und angemessen zu reagieren.

- Als Grundlage zur praktischen Etablierung, Aufrechterhaltung, Bewertung sowie Weiterentwicklung der sicheren Lieferkette und damit zusammenhängender Management Systeme (Prozesse, Kennzahlen) sollten die hierfür relevanten technischen Informationen (z.B. digitale Stücklisten mit notwendiger Granularität, Konfigurationsinformationen, Risikobewertung) durchgängig und digital erfasst, zwischen den beteiligten Stellen ausgetauscht und über den Lebenszyklus hinweg verwendet werden. Hierfür sollten nach Möglichkeit offene Standards und ein gemeinsamer Wortschatz zur Anwendung kommen, um von Anfang an interoperabel zu sein und den Aufwand zur Realisierung und Weiterentwicklung dieser Grundlagen für alle Beteiligten so gering wie möglich halten zu können.

Eine essentielle Maßnahme hierfür ist die Etablierung und Nutzung akkreditierter Prüfstellen und Prüfverfahren, die Tests und Prüfungen im Rahmen von Zertifizierungen, Akkreditierungen und Zulassungen durchführen. Diese Verfahren sind grundsätzlich aus dem Kontext vertrauenswürdiger IT-Komponenten aber auch der Eignungs- und Einsatzprüfungen komplexer Systeme bekannt. Generell ist nicht nur zu prüfen, ob die gewünschten Funktionen erfüllt werden, sondern auch darauf, ob weitere, gegebenenfalls unerwünschte oder sogar schädliche Funktionen erfüllt werden (können). Eine ernsthafte Durchführung solcher Prüfungen setzt allerdings voraus, dass die Prüfstelle über hinreichende Produktinformationen bis hin zum Quellcode verfügt, was in der Regel nur bei nationalen Herstellern gefordert und durchgesetzt werden kann. Zu beachten ist hier auch das gesamte Konfigurationsmanagement solcher Produkte und die Notwendigkeit erneuter Prüfungen nach Updates oder Konfigurationsänderungen. In der Praxis werden derartige Prüfungen derzeit nur für wenige Produkte ermöglicht, die in sicherheitskritischen Bereichen verwendet werden.

Die im vorherigen Abschnitt erwähnten Prüfungen bilden eine Momentaufnahme, zum Zeitpunkt der Durchführung, mit einer spezifischen Detailtiefe ab. Prüfungen können in der Regel erst dann stattfinden, wenn die Produkte einen entsprechenden Reifegrad aufweisen. Zur realistischen Etablierung sicherer Lieferketten und deren Aufrechterhaltung ist es aber notwendig, bereits deutlich früher im Lebenszyklus anzusetzen. Das heißt, dass entsprechende technischen Spezifikationen vorgegeben werden und ausreichende Prozess- und Methodenstandards in der Entwicklung und Integration von Produkten bzw. deren Elementen eingehalten werden müssen. Außerdem sind ein Risiko- und Konfigurationsmanagement sowie die Entwicklung/Produktion begleitende Tests notwendig. Diese Aktivitäten sind während des gesamten Lebenszyklus, das heißt auch bei Aktualisierungen oder Konfigurationsänderungen, erforderlich. Um dies zu ermöglichen ist eine gemeinsame Anstrengung von GB BMVg und Industrie unerlässlich.

4 Detailbetrachtungen

Gemeinsames Kapitel BMVg (CIT)/Industrieverbände (BDSV und Bitkom)

In diesem Kapitel erfolgen die Detailbetrachtungen sowohl anhand der Handlungsfelder (z.B. funktionaler Cluster) als auch der querschnittlichen prozessualen Anteile. Eine Lage wird erhoben und bewertet, auf deren Basis in Folge Handlungsbedarf und Lösungsansätze identifiziert werden.

Wesentlicher Ansatzpunkt zum Einsatz und Betrieb von vertrauenswürdiger IT (Komponenten, Systeme und Verfahren), auch als Bestandteil komplexer integrierter Systeme, ist die Betrachtung von sicheren Lieferketten einschließlich Produktion, Nutzung, Betriebsführung, betriebsbegleitender Weiterentwicklung sowie Außerdienststellung (im Folgenden auch als kompletter Lebenszyklus bezeichnet). Hierbei ist die Aufgabenstellung gesamtheitlich zu betrachten, das heißt nicht nur technisch oder organisatorisch. Perspektivisch sind auch komplexe Anwendungsfälle mit zusätzlichen Abstraktionsstufen wie z.B die Bereitstellung von Anwendungsplattformen (application Plattform as a Service, aPaaS), Software (Software as a Service, SaaS), Cloud-Kapazität (Cloud as a Service, CaaS) oder auch Infrastruktur (Infrastructure as a Service, IaaS) als bedarfsabhängige Dienstleistung zu berücksichtigen.

Jedes Element einer sicheren Lieferkette muss grundsätzlich auf o.a. Absicherungsarchitektur aufbauen, dies gilt z.B. für die Fertigung von Mikroelektronik, Firmware, Betriebssystem oder Software. Baut ein Element der Produktionskette auf einem nicht "vertrauenswürdigen" Produktionselement auf, so hat es sein Systemelement so weit wie irgend möglich abzukapseln. Beispiele:

- Integration einer nicht "vertrauenswürdig" produzierten Festplatte in einem "vertrauenswürdigen" IT-System: Jedwede Kommunikation des IT-Systems mit dem Festplattencontroller findet über eine standardisierte Schnittstelle inhaltsneutral statt. Daten des IT-Systems werden auf Grund der Kapselung nur verschlüsselt an den Festplattencontroller übergeben. (siehe z.B. SINA-Architektur[16])
- Realisierung eines vertrauenswürdigen APC auf Basis eines nicht vertrauenswürdig produzierten APC: Betrieb nur mit einem gekapselten Betriebssystem, welches eigens vertrauenswürdig entwickelt wurde. (siehe z.B. SINA-Architektur[16])

Eine vertrauenswürdige Produktions- und Lieferkette ist nur dann realistisch zu etablieren, wenn sie möglichst früh ansetzt und umfassend ist. Eine entsprechende (Ab-)Kapselung von nicht vertrauenswürdigen Systembausteinen ist umso einfacher, je einfacher die Funktionalität des einzelnen Bausteins gehalten ist.

Für jedes Element der Kette ist eine eigenständige und den Anforderungen an Vertrauenswürdigkeit und Leistungsfähigkeit nachweislich entsprechende Prüf- und Zertifizierungsinstanz zu etablieren, die über das notwendige konzeptionelle Wissen und die erforderlichen praktischen Fähigkeiten verfügt, die Produktionsinstanz kontrolliert und ihr die Vertrauenswürdigkeit als Bestandteil der Anforderungskonformität im notwendigen Umfang attestiert.

Durch die Nutzung von COTS-Produkten steigt die Chance, dass Dritte Fehler in der Software/Hardware finden und somit das Risiko, dass diese Fehler für schadhafte Zwecke ausgenutzt werden. Dies liegt

[16] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/SINA/sina_node.html

daran, dass COTS-Produkte am Markt weit verbreitet sind und die Bereitstellungszeit bis zur Verfügungstellung einer Aktualisierung und zur Beseitigung einer Sicherheitslücke unter Umständen länger ist als bei spezifischer Software/Hardware, die mit eigenen Wartungsverträgen ausgestattet ist.

Die Manipulation von Hardware (inkl. der in Hardware enthaltene Software) kann auch über Transportwege erfolgen und ist somit außerhalb des direkten Einflusses von Hersteller, Systemintegrator oder Nutzer.

Allgemein verfügbare Tools, die zur Überprüfung eingesetzt werden, können ebenfalls kompromittiert bzw. manipuliert sein. Bei marktüblichen Testverfahren wird vorwiegend die korrekte Funktion der Hardware bzw. Software getestet. Hierbei erfolgt aber i.d.R. keine Erkennung von oder Test hinsichtlich „Zusatzfunktionen“, die ohne Wissen des Nutzers oder auch endfertigenden Herstellers eingebracht wurden.

Eine Bedrohung kann auch dadurch entstehen, dass Hersteller gesetzlich verpflichtet werden, sog. Hintertüren (auch Backdoor genannt[17]) in Hardware oder Software einzubauen. Durch derlei Hintertüren kann die Angreifbarkeit von Hardware und Software erleichtert werden, ohne dass dies den Nutzenden bewusst oder bekannt sein muss bzw. durch diese effektiv verhindert werden kann.

Durch Kaskadierung von derlei Hintertüren bzw. Verwundbarkeiten können dann bspw. auch Angriffe auf nicht-vernetzte Systeme ermöglicht werden, so dass z.B. eine eingeschleuste Malware gemäß Parametrisierung autark und verschleiert Daten sammelt und jene gesammelten Daten – ebenfalls verschleiert - abfließen lassen kann sobald hierzu die Möglichkeit besteht. Neben dem reinen Sammeln von Daten ist auf diesem Wege auch der situationsabhängige Eingriff in Systeme möglich. Hierdurch entstehen reale Bedrohungsszenarien für z.B. autark arbeitende Waffen- und Steuersysteme ohne direkte bzw. permanente Vernetzung mit anderen Systemen.

Weitere Verwundbarkeiten können auch dadurch entstehen, dass (eigentlich) fehlerfreie Module in überarbeiteten/ aktualisierten Systemen wiederverwendet werden, sich dort auf Grund möglicher anderer Betriebsparameter aber anders als beabsichtigt verhalten und durch unvorhergesehene Fehlfunktionen Angriffsmöglichkeiten entstehen.

Aufgrund immer kürzerer Innovations-, Markt- und Produktionszyklen einiger technischer Komponenten, insbesondere Massenprodukte vom Weltmarkt die ursprünglich nicht für den Einsatz in z.B. Hochsicherheitsumgebungen oder dem missionskritischen Umfeld entwickelt wurden, ist davon auszugehen, dass ein durchgängig sicheres Design und vertrauenswürdige Fertigung nur bedingt ermöglicht werden kann. Höchstwahrscheinlich werden nicht alle erkannten Sicherheitslücken erkannt oder geschlossen werden können.

Im Kontext der sicheren Lieferkette ist ebenfalls zu berücksichtigen, dass die Verfügbarkeit einzelner IT-Komponenten – ohne weitere Maßnahmen – nicht über den gesamten Lebenszyklus der typischerweise langlebigen komplexen militärischen Systeme gegeben sein wird. Die Nachversorgung kann durch politische, gesellschaftliche oder wirtschaftliche Entwicklungen (z.B. Exportregulierung fertigender Nationen, Marktaustritt von Herstellern) sowie Naturkatastrophen und Krisenlagen[18],

[17] https://www.security-insider.de/was-ist-eine-backdoor-a-676126/

[18] Siehe z.B. https://www.heise.de/hintergrund/Autoindustrie-Chip-Mangel-problematisch-bis-ins-zweite-Halbjahr-5078850.html

gestört werden. Das notwendige Maß an Resilienz muss somit essenzielle Ausprägung der sicheren Lieferkette sein.

Eine rein nationale Betrachtung der Absicherung von Lieferketten ist in der überwiegenden Anzahl der Anwendungsfälle praktisch weder möglich noch zielführend. Vielmehr muss die Absicherung der Lieferkette analog zu globalisierten Wertschöpfungs- und Fertigungsprozessen (z.B. im Bereich Mikroelektronik) global betrachtet werden, so dass übergreifende Lösungsansätze gefunden werden können.

Die inhärente Sicherheit als Eigenschaft eines IT-Systems wird nicht nur durch die bei der Nutzung des Systems getätigten Handlungen, sondern auch durch die bei der Entwicklung, Fertigung und Lieferung des Systems definierten und gegebenenfalls böswillig manipulierten Eigenschaften bestimmt. Die zunehmend erfolgte Spezialisierung der einzelnen Unternehmen in der Vergangenheit hat zu einer Fragmentierung und Internationalisierung der Fertigungs- und Lieferkette geführt.

Diese Kette besteht aus den Schritten vor und nach der Lieferung und Inbetriebnahme eines Systems. Die wesentlichen Schritte der Wertschöpfungs- und Lieferkette vor der Auslieferung sind:

- Entwicklung: Systementwicklung, Produktentwicklung (HW und SW), Erstellung der Betriebsdokumentation, Wartungsplanung- und Dokumentation, Qualitätsplanung
- Planung: „Make or Buy“-Entscheidung, Fertigungskonstruktion, -planung und -vorbereitung, Einkauf
- Fertigung: Produktion von Subsystemen aus Halbzeugen und Rohprodukten
- Integration: Integration des Gesamtsystems aus eigenen und zugelieferten Subsystemen
- Qualitätssicherung: Prüfung und Dokumentation des Bauzustandes
- Lieferung: Transport des Systems an den Ort des Eigentumsübergangs

Nach der Auslieferung sind weitere Schritte der Lieferkette bzw. Nutzungsphase zu berücksichtigen:

- Inbetriebnahme und Nutzung
- Betrieb und Wartung: Sicherstellung der Funktionsfähigkeit durch Prüfung und Austausch von Subsystemen
- Entsorgung: Recycling des Systems, Nutzung von Subsystemen zur Wartung anderer Systeme

An jedem Übergang zwischen Schritten in der Lieferkette werden Informationen und gegebenenfalls Systeme zwischen Verantwortlichkeiten übergeben. Diese können sowohl innerhalb einer Organisation – z.B. zwischen Entwicklungsabteilung und Fertigungsabteilung – als auch zwischen Organisationen – z.B. zwischen zwei Konsortialpartnern oder einem Entwicklungsdienstleister und einem Plattformlieferanten – stattfinden. Jede Übergabe von Informationen oder Systemkomponenten birgt die Gefahr von Manipulation, Informationsabfluss oder Störung des Ablaufs. Ein besonderes Risiko besteht bei der Übergabe vom Zulieferer an den Integrator und der Übergabe vom Integrator oder Ersatzteilhersteller zum Nutzer. Hier sind in der Regel die Transportwege lang und es kommen verschiedene Dienstleister zum Einsatz, was die Angriffsfläche für eine Manipulation vergrößert und die Nachvollziehbarkeit einer Manipulation erschwert.
Im Wesentlichen werden zwischen zwei Arbeitsschritten in der Lieferkette von IT-Systemen drei verschiedene Elemente übergeben:

- HW-Systeme: physikalische Produkte (Systeme oder Komponenten)

- SW-Systeme: Informationen als in HW eingebrachte (embedded) Software oder als Software auf Datenträgern
- Informationen: Basisdaten zur Verwendung durch Software oder Informationen zur Bedienung und Wartung des IT-Systems

Am Beispiel eines Lagebildsystems wären das:

- HW-Systeme: z.B. Endgeräte und Peripherie
- SW-Systeme: z.B. Betriebssysteme und Funktionssoftware (z.B. Datenbanken, Middleware etc.), virtuelle Appliances (z.B. Embedded Software), Anwendungssoftware, Unterstützungssoftware auf Datenträger(n)
- Informationen: z.B. logistische und geographische Informationen für Lagebild und Betriebsführung, Konfigurationsparameter, Benutzer- und Betriebsdokumentation auf Datenträger(n)

Für eine Absicherung der Lieferketten sind also die inneren Lieferketten, d.h. die Transporte von Teilen und Informationen zwischen den Entwicklungs- und Fertigungsschritten beim Hersteller, genauso zu betrachten wie die äußere Lieferkette, also die Transportstrecke des fertigen Produktes zum Nutzer und die weitere Handhabung in der Nutzer-Organisation inkl. Betriebsführung über den Lebenszyklus des Systems hinweg. Des Weiteren müssen auch die inneren und äußeren Lieferketten der Zulieferer von Herstellern berücksichtigt werden. Jedes dieser Elemente unterliegt im Übergang zwischen den Prozessschritten der Lieferkette möglichen Risikofaktoren. Diese sind beispielhaft:

- HW-Systeme können hinsichtlich der Verfügbarkeit z.B. in kritischen Situationen so manipuliert werden, dass sie beim Eintreten bestimmter Bedingungen (z.B. nach 24 Stunden kontinuierlicher Nutzung ausfallen. SW-Systeme können so manipuliert werden, dass unberechtigte Zugriffe möglich sind, oder Informationen nicht vollständig angezeigt werden, z.B. Schaffung von blind spots im Lagebild, oder verfälscht werden, z.B. Entfernung oder Verfremdung von Geodaten.

- Komplette Systeme oder deren Komponenten können ausgetauscht werden, z.B. Speichermedien auf Versionen mit kleiner MTBF (Mean Time Between Failures, mittlere Betriebsdauer zwischen Ausfällen), oder SW-Systeme durch manipulierte, mit Backdoors versehene, Versionen.

- Durch Analyse der Entwicklungsunterlagen oder durch Reverse Engineering von Systemen und Informationen können Dritte Kenntnis über Fähigkeiten und Einschränkungen der einzusetzenden Systeme erhalten und gegebenenfalls einen eigenen Fähigkeitsaufwuchs einleiten.

- In den Systemen gespeicherte Informationen können von Dritten ausgelesen werden. Diese erhalten somit Kenntnis über den aktuellen Informationsstand sowie – insbesondere beim Austausch von Subsystemen im Kontext der Wartung – Kenntnis über gespeicherte Abläufe.

Ein übergreifendes Sicherheitskonzept zur Absicherung der Lieferkette ist somit unerlässlich und sollte zwei Themenkomplexe abdecken: die Absicherung der einzelnen Arbeitsschritte der Lieferkette sowie die Absicherung des Übergangs und Transportes zwischen zwei Schritten der Lieferkette.

Im Folgenden liegt der Fokus auf die Absicherung des Übergangs und des Transportes zwischen zwei Arbeitsschritten sowie dem Arbeitsschritt „Lieferung“, um die Herausforderungen und Handlungsoptionen grundlegend zu erläutern.

Im Rahmen einer Sicherheitsbetrachtung ist grundsätzlich davon auszugehen, dass die Beschaffung von Systemen über autorisierte Vertriebswege erfolgt. Die Nutzung sogenannter Grau- oder Reimporte, die nicht vom Hersteller kontrolliert werden können, verhindert die Aufrechterhaltung durchgängiger Sicherheitsketten.

Zur Umsetzung und Ausgestaltung eines Sicherheitskonzeptes zur Absicherung der Lieferkette sind zumindest die folgenden Sicherheitsziele durch die Umsetzung von Sicherheitsmaßnahmen zu realisieren

- Definition und Dokumentation der sicherheitsbedürftigen Subsysteme
- Dokumentation des originalen Zustands (Integrität) der sicherheitsbedürftigen Subsysteme
- Definition sicherheitsrelevanter Prozessschritte und sicherheitsrelevanter Lieferketten zwischen den Prozessschritten
- Gewährleistung der Integrität von Ausgangs- und Endzustand im Transportprozess
- Verhinderung von Analyse und Informationsabfluss während des Transportprozesses
- Gewährleistung der eindeutigen Identifikation und Herkunft der Produkte

Da nicht zwangsläufig das gesamte System schützenswert ist – z.B. ist bei der Integration eines Lagebildsystems in ein handelsübliches Fahrzeug i.d.R. nur der Integrationsanteil schützenswert, nicht das gesamte Fahrzeug - müssen die schützenswerten Anteile eines Systems definiert und der originale Zustand fälschungssicher beschrieben und dokumentiert werden. Außerdem ist nicht jeder Übergang zwischen zwei Prozessschritten gleichermaßen kritisch. Die Übergabe zwischen einem externen Entwicklungspartner und dem OEM ist hier anders einzustufen als eine interne Übergabe zwischen zwei Entwicklungsteams. Daher müssen auch die zu schützenden Prozessschritte und die zu schützenden Übergänge definiert und dokumentiert werden. Um zu gewährleisten, dass während eines Übergangs keine Manipulation der zu schützenden Systeme stattgefunden hat, ist nachzuweisen, dass der Ausgangs- und Endzustand des zu schützenden Systems identisch sind. Zum Beispiel können HD-Bildaufnahmen eingesetzt werden, um den Zustand einer Platine vor und nach einem Transport automatisiert zu dokumentieren und auszuwerten. Neben dieser Prüfung einer physischen Manipulation des Systems ist aber auch sicherzustellen, dass während eines Transportprozesses kein Auslesen von Informationen oder kein Reverse Engineering der zu schützenden Systeme erfolgt, was nicht sichtbar ist und somit unerkannt bleiben würde.

Grundsätzliche lassen sich die folgenden Bereiche zur Umsetzung von Sicherheitsmaßnahmen im Hinblick auf die dargestellten Sicherheitsziele identifizieren:

- Informationssicherheit: Realisierung einer gesicherten IT-Infrastruktur für Hersteller, Partner und Zulieferer in Entwicklung, Fertigung und Betrieb, sowie die Absicherung der Kommunikation zwischen allen Beteiligten

- Prozesssicherheit: Gestaltung sicherer Entwicklungs-, Fertigungs- und Wartungsprozesse.

- Technische Sicherheit: Umsetzung technischer Maßnahmen zur Gewährleistung der Sicherheitsziele in den zu schützenden Systemen und Subsystemen; Implementierung von Security by Design innerhalb der Systeme

- Physische Sicherung: Absicherung der Entwicklungs-, Fertigungs- und Logistikflächen vom Hersteller und allen am Gesamtprozess Beteiligten

- Logistische Sicherheit: Absicherung des Transportes von Systemen innerhalb der Organisation und zwischen den Prozessbeteiligten

- Organisatorische Sicherheit: Entwicklung und Implementierung von Sicherheitsprozessen, z.B. Sicherheitsüberprüfung von Mitarbeitern, in der Organisation. Sensibilisierung aller Prozessbeteiligten für Sicherheitsbelange innerhalb und außerhalb der Organisation. Schaffung einer Sicherheitskultur

Im Kontext der Umsetzung und Ausgestaltung eines Sicherheitskonzeptes zur Absicherung der Lieferkette sind hier für die ausgewählten Sicherheitsziele im Folgenden einige exemplarische Maßnahmen mit besonderer Relevanz hervorgehoben. Dabei muss die Umsetzung der Maßnahmen nicht nur für den Hersteller oder Integrator des schützenswerten Systems, sondern auch für alle externen Beteiligten gefordert werden.

Definition und Dokumentation der sicherheitsbedürftigen Subsysteme

- Integration und Dokumentation des Risikomanagements im digitalen Zwilling, bzw. Produktdatenmanagementsystem

Dokumentation des originalen Zustands der sicherheitsbedürftigen Subsysteme

- Nutzung von Entwicklungsumgebungen und Source-Code-Control-Systemen mit fälschungssicherer Dokumentation des Source-Codes und des Entwicklungsprozesses
- Nutzung von Code-Signaturprozessen
- Schaffung eindeutiger Identifikationsmerkmale für Systeme und deren Komponenten

Definition von zu schützenden Prozessschritten und Übergängen zwischen Prozessschritten

- Nutzung eines Prozessmanagementsystems zur Dokumentation des Risikomanagements in den Entwicklungs-, Fertigungs- und Wartungsprozessen

Gewährleistung der Identität von Ausgangs- und Endzustand im Transportprozess

- Nutzung von z.B. Kryptologie und Smart Chips zur Codesignatur und Absicherung des Bootprozesses
- Fälschungssichere Dokumentation und Vergleich von Ausgangs- und Endzustand durch den Einsatz von Video, Photographie und hochgenauer Gewichtsanalyse
- Bereitstellung einer Verifikationsmöglichkeit des Bauzustands gegen den Originalzustand des digitalen Zwillings bzw. Produktdatenmanagementsystems

Verhinderung von Analyse und Informationsabfluss während des Transportprozesses

- Dokumentation von Zugriffen durch fälschungssichere Logging-Verfahren
- Verschlüsselung von Code und Informationen
- Implementierung rollenbasierter Zugangskonzepte im Logistikprozess
- Verwendung manipulationssicherer Verpackungen

Die hier dargestellte Auflistung der Sicherheitsmaßnahmen zur Absicherung der Lieferkette kann aufgrund der generischen Ausprägung nur einen selektiven Überblick über wesentliche Maßnahmen geben. Für die konkrete Ausprägung eines Sicherheitskonzeptes zur Absicherung der Lieferkette ist eine dedizierte Analyse notwendig, die das Systemdesign schützenswerter Systeme in der militärischen Nutzung genauso beinhaltet wie die Gestaltung des kommerziellen Konsortiums und die dort etablierten Abhängigkeiten.

Grundsätzlich ist bei den Betrachtungen zur sicheren Lieferkette ebenfalls die Herausforderung der Aufwuchsfähigkeit im Lebenszyklus vertrauenswürdiger IT zu berücksichtigen. IT-Komponenten unterliegen – naturgemäß – ständiger Weiterentwicklung und Änderungen. Hierbei kann es sich um Änderungen innerhalb von Komponenten bzw. Produkten (z.B. Aktualisierungen hinsichtlich Funktionalität oder Schließen von Sicherheitslücken) aber auch um den Austausch kompletter Komponenten bzw. Produkte handeln.

Neben generellen SW-Produkten betrifft das auch zunehmend HW-Produkte, deren Funktionen werden zunehmend in spezifischer SW realisiert werden. Diese Entwicklung macht auch vor dem Hochsicherheitsumfeld nicht halt. So unterliegen z.B. auch Verschlüsselungsverfahren der Aktualisierung, zukünftig eher mehr als weniger. Daher werden jene in Form spezifischer SW und HW realisiert und müssen innerhalb der Nutzung aktualisiert werden können. Neben Hochsicherheit/Krypto gilt dies auch für andere kritische Elemente (z.B. Steuerungskomponenten in Waffensystemen). Hierbei sind die durchgängige Integrität, die Vertraulichkeit der Produkte und deren Konfiguration, aber insbesondere auch die Vertrauenswürdigkeit von Prozessen und Verfahren zu schützen.

4.1 Konkrete Gefährdungsszenarien hinsichtlich Etablierung und Aufrechterhaltung sicherer Lieferketten für vertrauenswürdige IT der Bundeswehr

Die Bundeswehr muss in die Lage versetzt werden, auch künftig den weiter zunehmenden Risiken des Cyber- und Informationsraumes mit einer effektiven Cyber-Verteidigung zu begegnen. Dazu ist eine Betrachtung aller IT-Systeme von Waffensystemen und Plattformen unabdingbar. Auch sie sind bedroht. „Damit die Bundeswehr ihre Aufgaben im Cyber- und Informationsraum zukünftig wahrnehmen kann, gilt es u. a. (…) von Waffensystemen und Gefechtsständen bis zu Lieferketten in der Rüstung kritische Bereiche auch durch den gezielten Rückgriff auf nationale Schlüsseltechnologien zu härten.“[19]

Geheimdienste sowie militärische Cyberangreifer verfügen mitunter heute über ein fundiertes und breites Spektrum an Fachwissen bzgl. der IT-Sicherheit von Computersystemen aller Art. Zudem haben sie regelmäßig ausreichend Ressourcen, um auch sensitive Informationen zu erlangen (Cyber Spionage) oder Lieferketten zu infiltrieren (Manipulationen im Liefer-, Entwicklungs- und Herstellungsprozess), um technische Schwachstellen eines Zielsystems zu identifizieren oder zu generieren.
Schwachstellen in IT-Elementen sind im militärischen Umfeld in hohem Maße kritisch. Angriffe auf unteren Ebenen, wie die Hardware- oder Betriebssystemebene können die Sicherheitsmaßnahmen der darüber liegenden Ebenen prinzipiell umgangen werden.

In vielen militärischen Ausrüstungselementen sind verschiedene IT-Elemente auf COTS-Basis enthalten, beispielsweise Prozessorchips, Speicherbausteine oder Software (sowohl das Betriebssystem als auch Anwendungen). Es ist davon auszugehen, dass verschiedene Schwachstellen auf den jeweiligen Ebenen eines IT-Systems existieren.
Dadurch können auch Waffensysteme durch einen Angriff auf eingebettete IT (z.B. Computer, Sensoren) erfolgreich kompromittiert und die in der Praxis unabdingbaren IT-Sicherheitsziele wie Vertraulichkeit[20], und Integrität[21] und die Verfügbarkeit[22] verletzt werden. Das kann erhebliche Konsequenzen bzgl. der Einsatzfähigkeit von Waffensystemen nach sich ziehen.

Zumindest bei einigen staatlichen Akteuren ist davon auszugehen, dass sie über folgende Fähigkeiten verfügen:

- Beeinflussung von Standardisierungen, so dass schwächere Vorgaben in den Standard einfließen als möglich, um bessere Angriffsmöglichkeiten zu ermöglichen (z.B. für Zufallszahlengeneratoren[23])
- Durchführung entfernter Angriffe, ohne Netzwerkverbindung zum Ziel (siehe z.B. Operation Olympic Games (Stuxnet))[24]
- Ausspionieren von Lieferanten und / oder deren Lieferketten, um Informationen über Hard- und Softwaresysteme zu erlangen

---

[19] Siehe Konzeption der Bundeswehr, 20. Juli 2018, S. 44; siehe https://www.bmvg.de/de/aktuelles/konzeption-der-bundeswehr-26384

[20] **Vertraulichkeit** ist der Zustand, der unbefugte Informationsgewinnung oder –beschaffung ausschließt.

[21] **Integrität** bezeichnet die Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.

[22] **Verfügbarkeit** ist der Zustand, der die erforderliche und zugesicherte Nutzbarkeit von Informationen sowie der IT sicherstellt.

[23] Bernstein D.J., Lange T., Niederhagen R. (2016) Dual EC: A Standardized Back Door. In: Ryan P., Naccache D., Quisquater JJ. (eds) The New Codebreakers. Lecture Notes in Computer Science, vol 9100. Springer, Berlin, Heidelberg.

[24] https://www.academia.edu/42320191/CONFLICT_ANALYSIS_OPERATION_OLYMPIC_GAMES

- Manipulation von Originalbauteilen oder (Teil-)Komponenten während des Transports, des Wareneingangs oder der Lagerhaltung (z.B. durch Austausch)
- Infiltration von Lieferketten für unterschiedliche Subsysteme (Zulieferer von kommerziellen Hardwarekomponenten oder Werkzeugen), um sicherheitskritischere Software- (z.B. Firmware) sowie Hardwarekomponenten vorab zu manipulieren.

Für einige Angreifer sind auch nicht mit dem Internet verbundene, militärische Systeme potenziell erreichbar. Interne WLANs oder LANs z.B. von Gefechtsständen oder Battle Management Systemen (BMS) haben üblicherweise eine erhebliche Komplexität weisen eine starke Vernetzung mit anderen Komponenten auf. Die Lieferketten sind sehr umfangreich und verschachtelt, so dass nicht davon auszugehen ist, dass alle Punkte jederzeit unter Kontrolle des Nutzers sind.

Dies wird in der Praxis immer noch vielfach unterschätzt bzw. übersehen. Eine nachträgliche „on-top“ Berücksichtigung führt häufig zu einem nur unzureichenden Sicherheitslevel, trotz aller dann implementierten und vermeintlich schützenden Sicherheitsmaßnahmen wie (zertifizierten) Software und Hardwarekomponenten.

Staatliche Angreifer können oft unerwartet früh in der Entwicklung oder Produktion dieser Systeme angreifen, was dazu führen kann, dass spätere Eingriffe im Betrieb oder final bei System-Updates (z.B. Remote Maintenance) unentdeckt bleiben. Dabei spielen dem Angreifer lange Entwicklungs- und Betriebszeiten von Waffensystemen und deren Komponenten in die Hände.
Insbesondere durch Kombination von Infiltration und Eingriff in die Lieferketten können sowohl z.B. Zero-Day-Exploits ausgenutzt als auch spezifische Angriffe entwickelt und angewendet werden.

Im Falle von Kill Switches kann weiterhin durch ein geeignetes externes Signal, wie z.B. eine bestimmte GPS-Position, ein Ausfall der Komponente herbeigeführt werden. Dadurch kann jegliche sonstige Sicherheitsmaßnahme im System wirkungslos gemacht werden. Diese Angriffe sind ohne vorbeugende Maßnahmen, insbesondere bei älteren und häufig nur bedingt austauschbaren Systemen, nur schwer bis gar nicht detektierbar und können somit diverse Sicherheitsprozesse unterwandern.

Entwicklungs- und Lebenszyklus-Konflikte zwischen der klassischen IT-Welt und der der Waffensysteme prägen sich zusätzlich aus. Viele Waffensysteme haben oft sehr lange Entwicklungs- und Nutzungszeiträume, während derer die Wahrscheinlichkeit steigt, dass in der verbauten IT enthaltene Schwachstellen möglichen Angreifern bekannt werden und IT Komponenten im Rahmen des Lebenszyklus ausgetauscht werden müssen. Damit besteht die Möglichkeit, dass neue Waffensysteme bei Marktreife/Einführung mit verwundbarer Technologie (z.B. aufgrund bekannter Schwachstellen) genutzt werden. Bestenfalls sind die Schwachstellen zwar dann auch den Nutzenden bekannt, allerdings besteht trotzdem ein höheres Risiko, weil ggf. nicht schnell genug darauf reagiert werden kann.

Generell ist davon auszugehen, dass auch Systeme auf Basis von Technologien, die bereits einige Jahre im Markt verfügbar sind durch bisher nicht bekannte Schwachstellen angreifbar sein können. Bei solchen Systemen sind Design und Implementierung wohlbekannt und die zur Pflege notwendigen Prozesse und Anforderungen verstanden und grundsätzlich etabliert.

Bei grundsätzlich neuen Systemen bzw. Technologien sind Schwachstellen häufiger technisch unentdeckt bzw. nicht öffentlich publiziert, und das Design bzw. die Implementierung ist nur bedingt in den vielfältigen Szenarien der Nutzer erprobt. Dadurch besteht ein signifikantes Risiko durch „unknown unknowns“ und die fehlende Erfahrung in der Nutzung und Betriebsführung sowie die ggf. (noch) nicht ausreichende SW-Pflege. Bei neuen Systemen bzw. Technologien kann auch die Prüfung

hinsichtlich ggf. enthaltener „ungewollter Zusatzfunktionen“ ungleich aufwändiger sein als z.B. im Rahmen der SW-Pflege bekannter Systeme.

Typischerweise verbleiben militärische Systeme länger in Nutzung als es bei IT-Komponenten im zivilen Markt üblich ist. Bedingt durch die Auflagen für und Einsatzbedingungen von Waffensystemen ist es schwierig, die in der kommerziellen IT stattfindenden Plattform-Evolutionen insbesondere hinsichtlich der IT-Sicherheitseigenschaften zeitnah zu adaptieren. Sowohl die Verfügbarkeit als auch die Anwendbarkeit von Sicherheitsaktualisierungen sind mitunter problematisch. Hierbei sind auch Akkreditierungs- und Zulassungsprozesse zu berücksichtigen.

Neben Angriffen auf die Qualität der eingesetzten Bauteile, die z.B. zu kürzeren Lebenszeiten, bzw. schlechteren Leistungsparametern führen können und nachfolgend zu Austauschmaßnahmen mit entsprechendem Aufwand und Kosten, sind für staatliche Akteure insbesondere Manipulationen attraktiv, die ein gezieltes Ausschalten von Systemen ermöglichen und damit entsprechende gegnerische Operationen planbar machen. Dies gilt sowohl für in Nutzung befindliche militärische und sicherheitsrelevante Systeme als auch für industrielle Produktionsanlagen.

Bei Angriffen wird versucht Schwachstellen der Systeme auszunutzen. Das Vorhandensein solcher Schwachstellen ist bei der Nutzung konventioneller Entwicklungsmethoden auch mit aufwendigen Qualitätsprozessen nicht vollständig zu verhindern.

Darüber hinaus können Gegner zusätzlich gezielt in den Produktentstehungsprozess eingreifen, um in IT-basierten Produkten gezielt Schwachstellen einzufügen. Dadurch soll ein Kompromittieren des Produktes während seines Betriebes ermöglicht, bzw. vereinfacht werden.
Ein Produkt ist dabei auf seinem Entstehungsgang vielen Angriffsmöglichkeiten ausgesetzt. Es ist z.B. vorstellbar, dass Produkte (sowohl Hardware als auch Software) schon beim Hersteller im Designprozess durch „Zusatzfunktionen“ (z.B. Malware) angereichert werden. Damit kann ist es gegebenenfalls möglich alle Software-basierten Sicherheitsmaßnahmen zu umgehen.

Dies erfordert für staatliche Angreifer einen ausreichenden Einfluss auf entsprechende Hersteller, der in einigen Ländern z.B. durch gesetzliche Regelungen gegeben ist. Alternativ können entsprechende Änderungen mit mehr Aufwand und größerem Entdeckungsrisiko verdeckt durch korrumpierte Entwicklungsinfrastrukturen eingebracht werden.

Weiter können durch Nutzung manipulierter Entwicklungswerkzeuge (Electronic Design Automation (EDA) Tools) Schadelemente in deren Design einfließen. Aufgrund des großen Umfangs und der Komplexität von Mikroprozessordesigns ist deren Kontrolle anspruchsvoll, kostenintensiv und entsprechende Manipulationen bleiben mit großer Wahrscheinlichkeit unentdeckt. Voraussetzung ist hier ebenfalls ein ausreichender Einfluss auf die Hersteller entsprechender EDA Tools. Softwareseitig können z.B. entsprechend präparierte Compiler Schadcode in Programm-Binaries einfügen, die nur sehr schwer erkannt werden können[25].

Ein weiterer möglicher Angriffspunkt besteht während der Produktion des fertigen Prozessordesigns. Allgemein besteht hier das Risiko, dass das ein Design vor der eigentlichen Produktion kompromittiert wird.

Viele der genannten Vorgehensweisen erfordern einen Akteur mit weitreichendem Einfluss und Mitteln, um die benötigten kommerziellen Stakeholder zu den entsprechenden Handlungen bewegen

[25] Zum Wirkprinzip korrumpierter Compiler siehe: Reflections on Trusting Trust von Ken Thompson, 1984 in Communications of the ACM

zu können. Dies birgt für diese ein erhebliches Risiko, weil bei einer Entdeckung ein Reputationsverlust mit ggf. existenziellen Konsequenzen für diese Firmen drohen kann.

Staatliche Akteure verfügen in vielen Ländern schon heute über rechtlich abgesicherte Möglichkeiten nationale Firmen dazu zu verpflichten entsprechende Funktionen in ihre Produkte einzubauen.

Durch aktuell kaum vorhandene Fähigkeiten und Kapazitäten solche Manipulationen überprüfen zu können ist die Entdeckungswahrscheinlichkeit nach wie vor gering.

4.1.1 Betrachtung des Produktlebenszyklus

Jedes Produkt unterliegt bei seinem Weg von der Idee bis zum Nutzungsende einem Lebenszyklus (Lifecycle). Dieser beginnt mit der Idee zu einem Produkt und endet mit der Verschrottung oder der Verwertung. Dieser Lebenszyklus wird in verschiedene Phasen unterteilt. Die übliche Phasen werden im Folgenden dargestellt.

Entwicklungsphase
In der Entwicklungsphase werden Kundenanforderungen und technische Lösungen miteinander verbunden und in einem kreativen Prozess zu einer Produktbeschreibung vereint. Das Ergebnis der Entwicklung können 3D-Modelle, Zeichnungen, Softwaremodelle und ähnliches sein. Oft wird die Fertigung der Software, das Coding, bereits in der Entwicklungsphase durchgeführt. Die Entwicklungsphase wird in der „as designed“ Systemstruktur dokumentiert.

Fertigungsvorbereitung
In der Fertigungsvorbereitung werden anhand der Produktbeschreibung die Fertigungsmittel beschrieben. Fertigungsmittel sind Systeme, die zur Fertigung der Produkte benötigt werden. Im mechanischen Bereich sind das z.B. die Anlagen für einen Montage- oder Bestückungsprozess. Im Software-bereich wäre dies die Entwicklung oder Auswahl der für das Coding benutzen Integrated Development Environments (IDEs) oder Frameworks. Ergebnisse der Fertigungsvorbereitung sind die Fertigungsunterlagen und -programme.

Fertigung
In der Fertigung werden mithilfe der Fertigungsmittel die Produkte oder Systeme hergestellt. Im mechanischen Bereich ist das die Fertigung und Montage, im Softwarebereich das Schreiben des Source Codes und ggf. das Integrieren in ein System das Äquivalent. Das Ergebnis der Fertigung ist das fertige System. Die Systeme werden in der „as build“ Systemstruktur dokumentiert.

Prüfung / Qualitätssicherung
In der Prüfung/ Qualitätssicherung werden die in der Entwicklungsphase beschriebenen Eigenschaften eines Systems geprüft und dokumentiert. Das Ergebnis der Prüfung ist die Prüfdokumentation, die das funktionsgerechte Verhalten des Systems dokumentiert.

Transport
In der Transportphase wird das fertige System verpackt und an den Kunden versandt.

Nutzung, Wartung und Instandhaltung
Während der Nutzungsphase wird das System vom Endnutzer bestimmungsgerecht verwendet. Dabei werden regelmäßig Wartungen durchgeführt und abnutzungsrelevante Bestandteile des Systems ausgetauscht, bzw. Softwarekomponenten aktualisiert. Die Systeme werden in der „as maintained“ Systemstruktur dokumentiert.

Aussonderung und Verwertung
Nach Beendigung der Nutzungsphase werden die Systeme aus der Nutzung ausgegliedert und zerstört oder im Recycling einer alternativen Verwendung zugeführt.

Für die Betrachtung der Risiken verschiedener Systemkomponenten ist die Betrachtung des gesamten Lebenszyklus notwendig.

Personal im Kontext der Produktherstellung sind sowohl Mitarbeitende des herstellenden Unternehmens als auch Fremdpersonal, wie z.B. Dienstleister oder Praktikanten, die in den entsprechenden Prozessschritt eingebunden sind. Systeme und Subsysteme beziehen sich sowohl auf Hardware, Software und embedded Software. Systeme können selbst Subsystem in übergeordneten Systemen sein und vice versa.

Manipulation beinhaltet sowohl den kompletten Austausch als auch die Veränderung eines Systems oder eines Subsystems. Eine Manipulation kann sowohl interaktiv als auch durch einen Automatismus erfolgen.

4.1.2 Manipulationen/Fehler im Fertigungsprozess Mikroelektronik inkl. Firmware

Beitrag Industrieverbände (BDSV und Bitkom)

Die Lieferkette für elektronische Bauelemente ist seit je her Angriffen ausgesetzt. Durch die rasant fortschreitende Entwicklung und den damit verbundenen immer kürzer werdenden Innovationszyklen sind elektronische Bauelemente oftmals nur kurze Zeit verfügbar. Werden die Komponenten nach Einstellung der Fertigung noch benötigt, z.B. für Reparatur oder als Ersatzteil, so tritt in vielen Fällen eine Beschaffungsnot ein. Besonders betroffen sind hier Produkte mit langer Nutzungsdauer, wie z.B. militärische Produkte. Aber auch in den Branchen Medizin-, Gebäude-, Luft-& Raumfahrt-, Bahntechnik tritt dieses Phänomen auf. Da i.d.R. die Bereitschaft besteht, für die Teile hohe Geldbeträge zu zahlen, zieht dies die Aufmerksamkeit krimineller Kreise auf sich. Bauelemente werden entweder gefälscht, oder sie werden aus Schrott ausgebaut und als Neuware in den Umlauf gebracht.

Dies kann durch längerfristige qualifizierte Lagerhaltung von Bauteilen und einer langfristigen Release-Planung von Endprodukten oder Komponenten entschärft werden. Die Bauteile selbst sollten über die bekannten und vertrauenswürdigen Lieferanten beschafft werden. In Anwendungsfällen wo dies technisch nicht möglich oder aus wirtschaftlichen Gründen nicht abbildbar ist, werden neben der übergreifenden technischen Kompatibilität der Teile aus unterschiedlichen Fertigungen bzw. Design-Generationen auch möglichst durchgehende Transparenz über Design, Fertigung und Integration sowie entsprechende Validierungsmöglichkeiten benötigt.

Eine ähnliche Situation entsteht in Phasen hoher Nachfrage. So kann eine Beschaffungsnot auch dann entstehen, wenn eine Massenproduktion von Elektronikprodukten anläuft, weil etwa der Produktionsstart mehrerer neuer Modelle von Mobiltelefonen gleichzeitig erfolgt. Hier ist nicht nur die Ersatzeilfertigung betroffen, sondern auch die Neuproduktionen von Elektronikkomponenten.

Für die Nutzenden bedeutet die Kompromittierung der Lieferkette z.B. auch das Risiko eines unvorhersehbaren Ausfalls. „Wegen der Transformationswirkung der Elektronik kann dies zu enormen, ja gewaltigen Schäden für Mensch und Umwelt führen“ [26].

Einige Hersteller lagern die Verpackung und Prüfung von Bauelementen in eigenständige Unternehmen aus. In jüngster Zeit haben Mitarbeiter dieser Unternehmen in einigen Fällen Ausschussware inkl. der Zertifikate in den Verkehr gebracht, um sich zu bereichern.

[26] Poschmann, Hartmut, Gefälschte Bauteile, Teil 1 und 2 in Produktion von Leiterplatten und Systemen (PLUS) 2012

Durch einschlägige Vorkommnisse motiviert hat das U.S. Department of the Navy, Naval Air Systems Command (NAVAIR) im Juni 2007 eine Untersuchung der Situation beauftragt, die folgende Ergebnisse lieferte[27]:

- Bei 39 % der involvierten 387 Firmen und Organisationen im betrachteten Untersuchungszeitraum 2005-2008 konnten Fälschungen ermittelt werden.
- Die Anzahl der im Rahmen der Untersuchungen erkannten Bauteilfälschungen war von 3868 im Jahr 2005 auf 9356 im Jahr 2008 gestiegen.
- Alle Glieder der Zulieferkette sind betroffen
- Das oftmalige Fehlen der Traceability (Rückverfolgbarkeit) in der Zulieferkette war ein offensichtlicher Mangel.
- Strengere Testprotokolle und Qualitätskontrollen für Lagervorräte sind erforderlich.
- Die meisten Unternehmen haben keine Strategien zur Vermeidung des Einsatzes gefälschter Bauteile.

In einschlägiger Fachliteratur[28] und dem Bericht des US Department of Commerce zu gefälschten elektronischen Bauteilen[29] sind Beispiele für gefälschte Bauteile in Waffensystemen aufgeführt:

- Electromagnetic Interference Filter (EIF) im Hubschrauber für U-Boot-Bekämpfung US Navy SH-60B und CH-46 Helicopter:
- Speicherbausteine in Boden-Luft-Raketen US THAAD (Terminal High Altitude Area Defense) Missile
- u.a. Bauteile im Vereisungskontrollmodul, gebrauchte IC von Samsung, Fälschung von Xilinx-FPGA in Transport- und Aufklärungsflugzeuge sowie U-Boot-Jäger US Military Airplanes C-17, C-130J, C-27J, P-8A Poseidon, AH-64, SH-60B

Kriminelle Energie kann dazu führen, dass auch in militärischen Systemen die Lieferkette kompromittiert wird. In den vorher referenzierten Quellen ist anhand von Beispielen dargestellt, dass die Fälschung den Konsumenten oftmals erst über mehrere Stufen (vier-sechs Stufen) einer ansonsten einwandfreien Lieferkette erreicht. Somit wurde bereits erheblicher Aufwand betrieben, um die Fälschung zu verschleiern. Sofern jedoch Akteure hinzukommen, die über einen höheren Professionalitäts- oder Organisationsgrad und ggf. eine andere Motivation verfügen, ist mit einer neuen Qualität zu rechnen. Zudem können diese Akteure auf die bereits im Elektronikmarkt existierenden, gut „ausgearbeiteten“ Strukturen für die Kompromittierung der Lieferkette zurückgreifen.

Exemplarisch wird nachfolgend davon ausgegangen, dass die Lieferkette als Angriffspunkt durch Terroristen „genutzt“ wird, um gezielt Schaden anzurichten. Hier würden also auch Vorgehensweisen Sinn ergeben, die keinen unmittelbaren wirtschaftlichen Nutzen haben.

Solche Akteure können etwa Cyberkriminelle sein, die beispielsweise in die Systeme eines Originallieferanten eindringen und dort direkt auf die Designs (auch die Firmware) zugreifen, um ihr Ziel zu erreichen. So könnten Funktionen eines Produktes gezielt zu bestimmten Zeitpunkten oder wenn sich das Produkt in bestimmten geographischen Regionen aufhält deaktiviert werden. Auch wäre

[27] https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/ADA586414.xhtml#

[28] Poschmann, Hartmut, Gefälschte Bauteile, Teil 1 und 2 in Produktion von Leiterplatten und Systemen (PLUS) 2012

[29] https://www.bis.doc.gov/index.php/documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file

denkbar, dass Kommunikationspfade implementiert werden, die über einen nicht dokumentierten physikalischen Datenpfad interne Speicherinhalte an ein zuvor definiertes Ziel senden. Beim Originallieferant manipulierte Bauelemente sind, sehr schwer zu identifizieren. Eine Möglichkeit zur Erkennung wäre vom Originallieferant eine zertifizierte Prozessreife zu verlangen oder die verdächtigen Bauelemente einer Anomalie-Erkennung zu unterziehen.

Firmware, die ein Anwender selbst in die Elektronikkomponenten integriert, könnte auf dem Weg vom Originallieferant zum Anwender modifiziert oder ausgetauscht werden. Das Geschäft mit Firmware ist lukrativ, und so wird sie oftmals zusätzlich zur Elektronikkomponente als Produkt verkauft, und wird entsprechend erst nach Entrichtung des Kaufpreises geliefert. Sprich, die Firmware durchläuft die Lieferkette ggf. getrennt von der Elektronikkomponente, wodurch dieser Angriffspunkt entsteht. In einer anderen Variante könnten Bausteine, die der Originallieferant mit bereits integrierter Firmware an den Anwender liefert, abgefangen werden und die Firmware auf den Bausteinen ersetzt werden.

Eine weitere Qualität wäre erreicht, wenn ein Angreifer gleich mehrere Elektronikkomponenten oder Firmware unterschiedlichster Firmen manipuliert, so dass sie erst im Zusammenspiel eine Wirkung entfalten. Bei der Einzelkomponente könnte man dann zwar eine Manipulation feststellen, die Gesamtwirkung wäre jedoch nicht erkennbar, wenn nicht auch die Manipulation der weiteren beteiligten Komponenten gefunden wird. Für das oben genannte Beispiel des nicht dokumentierten Kommunikationspfades würde dies bedeuten, dass der Angreifer ggf. auch verfügbare Kommunikationsinfrastruktur (WLAN Router o.ä.) manipuliert, so dass sie die von dem manipulierten Produkt ausgesendeten Daten empfangen und an den Angreifer weiterleiten kann.

Ein möglicher Ansatz wäre die eindeutige Kennzeichnung von Schaltkreisen oder Elektronikkomponenten. Hierzu sind aktuell jedoch keine für den Industrieeinsatz reife Lösungen verfügbar. Sehr wohl gibt es Ansätze, bei denen informationsverarbeitende Bausteine Individualisierungsinformationen bereitstellen[30]. Diese Ansätze sind jedoch zugeschnitten auf Verschlüsselungsaufgaben. Meist ist das Ziel, die auf dem Baustein betriebene Software/Firmware gegen „Raubkopieren“ und somit unlizenzierter Benutzung zu schützen. Eine Optimierung dieser Verfahren zur Absicherung der Lieferkette existiert zurzeit nicht.

Ein weiterer, möglicher Ansatz wäre etwa für die Gesamtstruktur der Chipfläche ein vertrauenswürdiges Referenzbild zu generieren, dieses dann im Rahmen einer Wareneingangsprüfung beim Nutzer mit der real gelieferten Chipstruktur (automatisiert) zu vergleichen. Wegen der zunehmend kleiner werdenden Halbleiterstrukturen würde man hier jedoch sehr teure optische Analysesysteme benötigen, die diese Strukturen auflösen könnten, zudem ist die Methodik invasiv, das heißt der Prüfling wird zerstört.

[30] Stéphane di Vito, Schlüssel aus der DNA eines Chips, Elektronik 18 2020

4.1.3 Manipulationen/Fehler in COTS Hardware-Komponenten

Beitrag Industrieverbände (BDSV und Bitkom)

COTS-HW-Komponenten stellen IT-Massenprodukte wie APC, Server oder Laptops dar, welche von internationalen Konzernen für den globalen Massenmarkt entwickelt und produziert werden. Geprägt ist die Herstellung vom Preisdruck des Marktes und kurzen technologischen Entwicklungssprüngen, sodass eine weltweite Dislozierung vernetzter Produktions- und Entwicklungsstandorten zur Kostenoptimierung erfolgte. Reine Hardwarekomponenten sind in der heuteigen IT kaum noch anzutreffen. In der Regel bestehen auch als HW-Komponenten angesehene Systeme wie z.B. Ethernet-Switches (TCP/IP) als Embedded Systems aus Hardware und Software. Im Folgenden werden deshalb COTS-Systeme betrachtet.

Die Standorte unterliegen den jeweiligen nationalen Gesetzgebungen, woraus sich je nach Staat und anwendbarer lokaler Gesetzgebung in der Bewertung durch andere Staaten bzw. Kunden Risiken ergeben können. Dies trifft auch weitestgehend für in MOTS und GOTS Produkte enthaltene HW-Komponenten zu, Ausnahmen sind (wenige) spezifisch lokal gefertigte HW-Komponenten wie z.B. spezifische Krypto- oder EK-Bauteile.

Im Bereich der Entwicklung bestehen vorrangig organisatorisch geprägte Risiken. Kompromittierte IT-Systeme und Manipulationen durch eigenes bzw. extern beauftragtes Personal bilden die größten Gefahren. Die schnelle Weiterentwicklung der IT führt zu permanenten Anpassungen von Prüfverfahren, deren Evaluierung von Agilität geprägt ist.

Für die Produktion (Planung, Fertigung, Integration, Qualitätssicherung gem. Kap. „Absicherung der Lieferketten“) erfolgt ein Zukauf von Bauteilen und Baugruppen über ausgesuchte Lieferanten, die eine zeit- und qualitätsgerechte Lieferkette garantieren können. Auf diese Weise soll unter anderem die Lieferung sog. Grauware aus dem Drittmarkt bzw. Nachbauten, die Manipulationen oder zusätzliche Schwachstellen aufweisen, ausgeschlossen werden. Die Verantwortung hierfür liegt bei den Lieferanten.

Die Anforderungen an die Lieferanten und deren verlässlichen Versorgung mit Bauteilen/-gruppen beziehen sich auf das Vorhandensein von zugesicherten Eigenschaften (Qualität), weniger auf die Prüfung unerwünschter Eigenschaften (zusätzlicher Code). Organisatorische Maßnahmen sind z.B. die Prüfung von Versiegelungen, Transportsicherungen und Prüfplomben. Die Suche nach gezielten Manipulationen wird im Allgemeinen nur stichprobenartig durchgeführt. Eine Manipulation von kundenspezifischen Endgeräten durch gezielt eingeschleuste Bauteile/-gruppen wird durch die fehlende Zuordnung und der Menge der hergestellten Produkte grundsätzlich erschwert (z.B. Speicher).

Die internen organisatorischen Risiken von Manipulationen und Fehlereinschleusung bei der Produktion unterscheiden sich in den jeweiligen nationalen Rahmenbedingungen. Neben staatlichen Regelungen stellen gesellschaftliche Gegebenheiten niedrigere oder höhere Risikopotentiale dar.

Für die höheren Ansprüche an die Ware zur geschäftlichen Nutzung werden zusätzliche Möglichkeiten der Anpassungen von Eigenschaften der Endgeräte durch Customizing angeboten und adaptiv zusätzliche Maßnahmen für die Bereiche Produktion und Transportwege vorgenommen. Dazu werden diese während oder nach der Produktion kundenindividuell z.B. um spezielle Baugruppen, zusätzliche

SW oder spezielle Verschlüsselungen/Versiegelungen angepasst. Neben höheren Preisen ergeben sich zusätzliche Fehlerquellen und Manipulationsmöglichkeiten, bieten auf der anderen Seite aber auch die Möglichkeit für einen höheren Schutz oder spezielle Tests/Zertifizierungen.

Die Produktion selbst erfolgt grundsätzlich auf einheitlichen Fertigungsstraßen. Für angepasste (customized) HW können adaptiv zusätzliche Maßnahmen für die Bereiche Produktion und Transportwege vorgenommen werden

In Bezug auf ungewünschte Funktionen in COTS-HW-Komponenten ist grundsätzlich festzustellen, dass ein solcher möglicher Angriff erheblichen Streuungsverlusten unterliegt, da sich nur ein Bruchteil der COTS-Komponenten tatsächlich in sicherheitskritischen Nutzungen befindet. Das Szenario ist abstrakt gesehen vergleichbar mit bekannten breitflächigen Angriffen auf Internet-Router[31].

Solche möglichen Angriffe sind organisatorisch aufwändig und unterliegen – sofern breitflächig und nicht verdeckt durchgeführt - einer hohen Entdeckungswahrscheinlichkeit.

Für die Risikobetrachtung der Angriffsmöglichkeiten auf COTS-Systeme sollte die gesamte Wertschöpfungs- und Zuliefererkette von der Entwicklung über die Fertigungsvorbereitung und -Fertigung sowie der Transport innerhalb der Kette und zum Kunden betrachtet werden. Alle diese Phasen bieten verschiedene Angriffsmöglichkeiten.

Entwicklung

- Ungewünschte Funktionen werden durch kompromittiertes Personal in die Entwicklungsunterlagen eingebracht.
- Personal verwendet Komponenten von Zulieferer(n), die dort manipuliert wurden und unerwünschte Funktionen beinhalten.

Fertigungsvorbereitung

- Fertigungsunterlagen werden durch kompromittierte Unterlagen dahingehend manipuliert, dass die gefertigten Systeme unerwünschte, in den Entwicklungsunterlagen nicht beschriebene Funktionen beinhalten.
- Im Rahmen von „Make or Buy“ werden baugleiche Subsystem beschafft, die unerwünschte Systemfunktionen beinhalten.

Fertigung

- Während der Fertigung werden Steuerungsprogramme der Produktionsanlagen ausgetauscht oder verändert.
- Während der Fertigung werden Halbzeuge, Subsysteme oder Hilfsstoffe ausgetauscht oder verändert.

Prüfung

- Prüfvorschriften werden unzureichend definiert.
- Prüfmittel und -prozesse werden manipuliert, um die Erkennung von unerwünschten Funktionen zu erschweren.
- Prüfdokumentationen werden zur Verschleierung manipuliert.

[31] https://www.heise.de/news/WLAN-Router-im-Visier-von-Hackern-4852953.html

Transport

- Während des Transportes werden Systeme oder Subsysteme durch solche mit ungewünschten Eigenschaften ausgetauscht

Wartung, Instandhaltung und Entsorgung

- Im Rahmen von Wartungs- und Instandhaltungsmaßnahmen werden Subsysteme durch solche mit ungewünschten Funktionen ausgetauscht oder manipuliert.
- Im Rahmen von Wartungs-, Instandhaltung und Entsorgungsmaßnahmen werden unautorisiert Informationen aus Systemen oder Subsystemen ausgelesen. Hierbei kann es sich um unbewusst/ungewollt in den Systemen noch enthaltene vertrauliche operationelle Informationen sowie um systemimmanent enthaltene Informationen (z.B. Programmcode, Konfigurationsdaten) handeln, die einem potenziellen Angreifer konkrete Anhaltspunkte liefern.

Es kann davon ausgegangen werden, dass ein Update neue Funktionen (Innovationen) und die Beseitigungen möglicher Angriffsstellen (Verwundbarkeiten), aber auch die Implementierung neuer Verwundbarkeiten beinhaltet.

Gleichzeitig wird die Wahrscheinlichkeit der Nutzung von Verwundbarkeiten durch einen Angreifer über die Zeit immer größer, wenn Verwundbarkeiten bekannt werden. Gleichzeitig können nach Bekanntwerden von Verwundbarkeiten diese oftmals auch geschlossen werden, so dass die vorhandene Funktionalität zunehmend "gehärtet" wird.

Es ist also abzuwägen ob der operative Nutzen von Innovationen und die Beseitigung bekannter Verwundbarkeiten gegenüber der Integration neuer Verwundbarkeiten zu bevorzugen sind.

4.1.4 Manipulationen/Fehler in weiterverwendeten Software-Komponenten Dritter und Software-Lieferketten

Beitrag Industrieverbände (BDSV und Bitkom)

Beim Entwickeln von Software vertraut man implizit oder explizit diversen Zuliefern, die nicht unter der eigenen Kontrolle stehen. Mit zunehmender Komplexität der Aufgaben wird immer mehr externe Expertise eingeholt, sei es in Form von Third-Party Software und Softwarekomponenten (sowohl Open-Source als auch Closed-Source) oder von temporärem Personaleinsatz (Consultants bzw. Entwickler). Dazu kommen Third-Party Entwicklungswerkzeuge, sowie ebenfalls eine zunehmend vielfältigere Infrastruktur - lokale und public Clouds, mobiles Arbeiten etc.

Dadurch gibt es eine Vielfalt von Ansatzpunkten für Angriffe und unterschiedliche Auswirkungen. Aus Perspektive des SW-Herstellers als Element in der Lieferkette geht es hier nicht nur darum, die eigene Infrastruktur gegen Kompromittierung zu schützen, sondern insbesondere auch die Aufrechterhaltung der Position als vertrauenswürdiger Zulieferer. Die erstellte und potenziell kompromittierte Software wird evtl. in kritischen Bereichen oder kritischen Mengen eingesetzt und kann so z.B. für Spionage und Sabotage genutzt werden.

In diesem Kapitel werden sowohl Probleme, die in einer Delivery-Chain-Attacke auf Nutzer münden können, als auch Delivery-Chain Probleme, die Einfluss auf die Softwareentwicklung (und damit auch auf die ausgelieferte Software) haben, betrachtet. Dabei

geht es um Auswirkungen einer hinsichtlich der Nutzung von Third-Party Software und Softwarekomponenten schadhaften, unzuverlässigen oder gar bewusst kompromittierten Delivery-Chain auf die eigene Entwicklung und wie dadurch das Endprodukt gefährdet wird.

Auch wenn Third-Party Komponenten schon länger benutzt werden, haben die aktuellen Software-Ökosysteme, wie insb. JavaScript (NPM), eine neue Qualität: hier wird eine Vielfalt von Bibliotheken aus verschiedenen Quellen zu neuen Bibliotheken zusammengeführt, welche dann wiederum wieder in anderen verwendet werden etc. Dazu kommen evtl. feste Abhängigkeiten von bestimmten Softwareversionen, ohne nachträglich zu prüfen, ob hier evtl. inzwischen bekannte Sicherheitsprobleme aufgetreten sind. Bei Ruby, Python oder Perl gibt es ähnliche Ökosysteme, diese haben jedoch nicht die Filigranität von NPM.

Dazu kommt die Abhängigkeit von klassischen Third-Party Bibliotheken für komplexe und wichtige Aufgaben, z.B. OpenSSL, GnuTLS, NSS, Secure Transport für TLS (gesicherte Kommunikation, z.B. für HTTPS). Auch wenn mit der kritischen Heartbleed-Verwundbarkeit in OpenSSL im Jahr 2014 die Abhängigkeit kritischer Software von einer nur unzureichend gepflegten Softwarebibliothek offensichtlich wurde, wiesen in den Folgejahren sämtliche großen und auch kleineren SSL-Bibliotheken kritische Sicherheitslücken auf, unabhängig davon, ob es sich um einen kommerziellen Anbieter oder Open Source handelt. Gründe dafür sind u.a. das Alter und die zunehmende Komplexität der Software. Auch bezüglich der Software ist dieser Trend sichtbar. Auf der einen Seite ergibt sich eine größere Abhängigkeit von externen Komponenten, auf der anderen Seite eine zunehmende Komplexität des eigenen Codes: „Feature-itis“ statt Minimalismus.

Generell sind aber alle diese Ökosysteme, Third-Party Software und Softwarekomponenten teilweise nicht-offensichtliche, aber kritische Abhängigkeiten von einer Vielzahl von Autoren, das heißt ein

einzelner Autor kann unbemerkt bewusst (Backdoor) oder unbewusst (Bug) gravierende Sicherheitsprobleme produzieren.

Diese Probleme haben in den letzten Jahren zugenommen, weil immer mehr auf vorhandene Open-Source aufgebaut wird, sowohl von Endprodukten als auch die Open-Source-Bibliotheken. Dieses Vorgehen ermöglicht eine höhere Entwicklungsgeschwindigkeit bei gleichzeitig geringeren Kosten. Das heißt allerdings nicht, dass kommerzielle Hersteller zwingend eine bessere Option sind. So sind diese einem zunehmenden Kostendruck ausgesetzt (da die Integration von Open-Source ist aus oben beschriebenen Gründen billiger ist), was negativen Einfluss auf die Qualität der Produkte hat. Das führt auch dazu, dass für diese ebenfalls viel Open-Source eingesetzt wird, auch in kritischen Bereichen.

Eine eigenständige tiefergehende Evaluation der Komponenten und Software vor dem Einsatz ist selbst bei Open Source nicht möglich, da eine beschränkte lokale Expertise und begrenzte zeitliche Ressourcen der hohen Komplexität und Größe gegenüberstehen.

Der erste Schritt zur Sicherung von Software-Lieferkette besteht darin, den Aufbau und die Funktionsweise der eigenen Liefer- und Fertigungskette zu verstehen: Wie gelangen einzelne Bausteine (Softwarequellen, komponenten und pakete) in die Pipeline? Das Prinzip ist für Software und Hardware gleich, wobei im Bereich der Software Manipulationen und Fehler einfacher zu etablieren sind und eine physische Absicherung kaum wirksam möglich ist. Bedrohungen für die Software-Lieferkette nehmen zu, entweder durch die nachlässige Aufnahme angreifbarer bzw. unsicherer SW-Komponenten oder durch gezielte Manipulation. Während Produzenten um die kontinuierliche Bereitstellung und die Durchsetzung von Sicherheitsscans in ihren Pipelines kämpfen, wird die Pipeline selbst zum attraktivsten Angriffsvektor für einen Angreifer.

Wenn die Pipeline kompromittiert werden kann, sind andere Sicherheitsmechanismen weitgehend wirkungslos. Als Beispiel sei hier die SW-basierte potenzielle Kompromittierung des Supermicro-Motherboards genannt: Es war nicht notwendig, verdächtige Komponenten in die Lieferkette zu injizieren, da es deutlich einfacher war, durch Angriffe auf die Pipeline vorhandene Komponenten bzw. deren SW-Stand zu manipulieren.

Eine skizzierte Karte der Pipeline und der Einstiegspunkte, an denen besagte hinzugefügt werden können, genügt. So kann bestimmt werden, wo zusätzliche Kontrollen eingefügt werden sollten. Haben Entwickler beispielsweise vollen Zugriff auf Komponenten-Repositories im Internet, ist es wichtig, dass alle Softwarebuilds mithilfe eines Tools zur Analyse der Softwarezusammensetzung auf anfällige Komponenten gescannt werden.

Ein sichereres Betriebsmodell besteht darin, die bislang uneingeschränkte Verwendung von Komponenten generell zu begrenzen und eine lokale Instanz bekannter, geprüfter und genehmigter Komponenten auf einem Repository-Server bereitzustellen. In jedem Fall sollte eine Richtlinie zur Nutzung von Komponenten und Bibliotheken erstellt und veröffentlicht werden, damit Entwickler sich des Risikos bewusst sind und Software innerhalb akzeptabler Sicherheitsgrenzen entwickeln.

Schließlich ist es unerlässlich, dass sich eine Organisation ständig über Risiken im Hinblick auf Komponenten von Drittanbietern auf dem Laufenden hält und diese bewertet. Viele Tools zur Analyse der Softwarezusammensetzung ermöglichen das Scannen entweder beim Schreiben von Code oder zum Zeitpunkt des Deployments. Zudem ist ein pragmatischer Ansatz zur Bewältigung technischer Schulden nötig, die durch den Einsatz von Komponenten von Drittanbietern „geerbt“ werden.

Der zweite Schritt zur Sicherung der Software-Lieferkette besteht darin, sicherzustellen, dass Sicherheitskontrollen in der Pipeline nicht trivial umgangen werden können. Wenn Entwickler unter Druck stehen, einen Termin einzuhalten, ist das Umgehen von Sicherheitstests in einem Buildprozess verlockend. Buildpipelines können z. B. schlecht konstruiert und gesteuert sein, was zu einer nicht ausreichenden Testabdeckung und Wiederholbarkeit führt.

Das Nutzen unveränderlicher Pipelines, die aus einer „goldenen Quelle“ gebaut wurden, trägt dazu bei, dass Pipelines einheitlich gebaut werden, wodurch die Variabilität verringert wird. Die zusätzliche Verwendung digitaler Signaturen und Software-Manifeste ermöglicht es, die Authentizität eines Pipelineprozesses zu erzwingen und verifizierbar zu machen. Release-Kandidaten kann eine „Authentizitäts-Signatur“ hinzugefügt werden, die belegt, dass alle Sicherheitstests in Übereinstimmung mit den geltenden Richtlinien abgeschlossen wurden.

Der Aufstieg der Cloud-Native-Bewegung bietet eine Gelegenheit, die Absicherung der Lieferkette in die Buildpipeline zu integrieren. Ein wesentlicher Anteil des Lebenszyklus-Entwicklungsprozesses für z. B. Container ermöglicht somit Sicherheit als integralen Teil des Prozesses und nicht als nachträgliches oder „aufgepfropftes“ Zusatzelement.

Beispielsweise ist es möglich, nur genehmigte und geprüfte Basisimages (z.B. aus der Docker Trusted Registry) zum Erstellen von Containern zu verwenden. Außerdem ermöglichen zahlreiche Tools das Scannen von Schwachstellen, wenn Container erstellt werden, und die Buildpipeline selbst kann gehärtet und undurchlässig für externe Manipulationen oder Optimierungen gemacht werden.

Governance kann zum Zeitpunkt der Bereitstellung mit dem Konzept eines "Zulassungscontrollers" durchzusetzen. Dies ist ein robuster Mechanismus innerhalb eines Orchestrators, um die Authentizität der Pipeline zu erzwingen, bevor ein Release-Candidate für die Produktion freigegeben werden kann.

In vielen Fällen haben Unternehmen nicht ohne Weiteres containerzentrierte Werkzeugketten bauen, und müssen daher andere Mechanismen nutzen, um Authentizität zu erzwingen. Das Update Framework (TUF) bietet eine hervorragende Referenz für einen robusten Softwareupdateprozess, durch den Angriffe oder Kompromisse verhindert werden. Tatsächlich wird TUF als Dockers Notary in der Cloud Native Computing Foundation implementiert, um Containersicherheit zu gewährleisten.

Eine weitere ausgezeichnete und allgemein anwendbare Implementierung eines Supply-Chain-Schutzrahmens ist In-Toto. Auf diese Weise kann ein Pipeline-Designer (die Entwurfsautorität) die Schritte innerhalb der Buildpipeline bildlich entwerfen und dann die Befehlszeilentools von In-Toto verwenden, um jede Phase des Prozesses kryptografisch zu signieren.

Auf diese Weise kann ein endgültiger Release-Kandidat formell überprüft werden, um alle Phasen des angegebenen Prozesses erreicht zu haben. In-Totos generisches und modulares Design ermöglicht, es auf ältere Buildpipelines anzuwenden, sodass die Lieferkettensicherheit sichergestellt werden kann. Ein vollständiger Übergang zu einem Containerlebenszyklus ist keine Voraussetzung.

Einfache Hygienemaßnahmen wie das Scannen von Schwachstellen oder die Verwendung von zweifelsfrei funktionierenden Komponenten adressieren bereits Risiken in der Lieferkette. Durch moderne Methoden zur Entwicklung des Containerlebenszyklus kann die Lieferkettensicherheit so gestaltet werden kann, dass Kompromisse unwahrscheinlich sind.

Neben dieser auf die Technologie fokussierten Betrachtung ist auch eine Analyse der verwendeten Drittanbieter erforderlich. Hier gibt es eine Bandbreite angefangen von Kleinstanbietern (die bspw. ein Spezialprodukt anbieten und mit fünf Mitarbeitende beschäftigen) auf der einen Seite bis zu internationalen Großkonzernen mit einem weitgefächerten Produktportfolio auf der anderen Seite.

Entscheidend ist dabei, in wie weit der Anbieter in der Lage ist, Sicherheitsanforderungen, wobei hier explizit nicht nur der Nachweis einschlägiger Zertifizierungen gemeint ist, einzuhalten und auf neue Bedrohungen direkt und angemessen zu reagieren. Wünschenswert wären die proaktive Gestaltung und Weiterentwicklung der Produkte, um gegenüber den jeweiligen Kunden ein Höchstmaß an Sicherheit und Verlässlichkeit zu gewährleisten.

Gerade bei Anbietern mit Entwicklungsstandorten außerhalb Deutschlands und Nutzung dieser Ressourcen für sicherheitsrelevante Komponenten, müssen konkrete Mechanismen zur Risikominimierung existieren. Hier könnte eine ausgeprägte Nutzung von externen Audits durch den Kunden oder eine neutrale Instanz eine Maßnahme zur Risikoreduzierung sein.

Zusätzlich zu diesen anbieterbezogenen Punkten ist die Gestaltung und Ausprägung der eingesetzten Software ein relevanter Aspekt. Bei der Nutzung von Standardsoftware (z.B. ERP-Software) erfolgt im Regelfall eine kundenspezifische Ausprägung bzw. Implementierung. Diese Implementierungsaufgaben werden häufig durch externe Berater vorgenommen und reichen von Systemeinstellungen bis hin zu umfassenden Programmierungen. Hier ergibt sich thematisch eine Verknüpfung mit der im folgenden Abschnitt dargestellten Eigenentwicklung von Software-Komponenten. Die Möglichkeiten / Erfordernisse mit Programmierung oder der Nutzung von Skriptsprachen die vorhandene Software für den jeweiligen Anwendungsfall zu optimieren, verstärken sich derzeit permanent. Gründe hierfür sind beispielsweise die immer umfassender geforderte (Micro-)Service-Orientierung und Interoperabilität über APIs.

Die aktuell immer weiter fortschreitende Integration und Nutzung von Maschine Learning Funktionalitäten erzeugt ebenfalls eine weitere Vermischung von Standard- und individualer Programmierung. Den hierdurch entstehenden Risiken muss mindestens durch ein Vier-Augen-Prinzip begegnet werden und stellt ganz neue Anforderungen an die Beurteilungsfähigkeit.

4.1.5 Manipulationen/Fehler in eigenentwickelten Software-Komponenten

Beitrag Industrieverbände (BDSV und Bitkom)

Grundsätzlich ist eigenentwickelte Software und deren Zusammenstellung ähnlichen Risiken ausgesetzt wie Drittkomponenten und somit auch durch ähnliche Methoden effektiv angreifbar bzw. manipulierbar. Bei der Eigenentwicklung verfügt der Produzent in der Regel aber über eine effektivere Kontrolle über den Prozess der SW-Entwicklung (Plan-Design-Build-Test) sowie der Integration in bzw. der Anpassung an spezifische Laufzeitumgebungen.

Abnehmende Beherrschung des eigenen Software-Stacks

Wenn der eigene Software-Stack nicht ausreichend beherrscht wird, führt dies zu Sicherheitsrisiken, die ein Angreifer bei dem im Einsatz befindlichen Produkt ausnutzen kann. Ein mangelndes Verständnis des eigenen Codes erhöht das Risiko, durch Dritte handwerklich versiert, aber versteckt eingefügte explizite Backdoors nicht zu erkennen.

Einmal geschriebener Code hat oft eine Lebensdauer, die initial nicht geplant war. Der Code wird erweitert, kopiert, an neue Anforderungen angepasst etc. Das Gesamtsystem wird größer, die Komplexität steigt und Zusammenhänge lassen sich schwerer verstehen und schwerer debuggen. Je weiter sich das System in diese Richtung bewegt und je mehr es den Entwicklern entgleitet, desto schwieriger wird es, die Kontrolle zurückzugewinnen, und desto unwilliger werden die Entwickler mit diesem Code arbeiten.

Vorhandener Code wird evtl. auch in Kontexten eingesetzt, für die er nicht gedacht war, wodurch „plötzlich“ wenig offensichtliche Sicherheitsprobleme erzeugt werden. Ähnliche Effekte können bei der Nutzung von Third-Party-Komponenten oder auch Third-Party-Software auftreten. So kann z. B. der Code nicht mehr gepflegt sein, neue Versionen zeigen ein geändertes Verhalten, weisen z. B. ein angepasstes Application-Programming-Interface (API) auf, oder es ist nicht mehr zuverlässig nachvollziehbar, ob bzw. welche kritischen Anteile geändert wurden. Mit zunehmender Lebensdauer steigen also die Chancen für kritische Fehler aus unterschiedlichen Gründen.

Dazu kommt der Druck, mehr Funktionalität in kürzerer Zeit mit weniger Aufwand bereit zu stellen:

- Notwendige Codepflege (Refactoring) wird aus Zeit- und Kostengründen verschoben - und wird letztendlich niemals gemacht, weil der Zeitaufwand dafür inzwischen immer größer geworden ist.

- Um schneller zu sein, wird mehr „Quick and Dirty“ programmiert und mehr Third-Party-Code verwendet. Dies verstärkt die beschriebenen Probleme bzgl. der abnehmenden Beherrschbarkeit des Software Stack.

- Quick (and Dirty) ist ein Feind von Sicherheit. Ausreichende Sicherheit wird oftmals weder beim Design noch beim Testen berücksichtigt, das heißt der Fokus liegt auf der Funktionalität.

Angriffe auf die Integrität des Quellcodes

Hier geht es um die Einbringung bösartiger Änderungen in die Codebasis, in der Hoffnung, dass dies nicht bemerkt wird. Ist der Angreifer in der Entwicklungsumgebung, kann er auch Änderungen am Quellcode vornehmen. Dies ist insbesondere dann kritisch, wenn kein zuverlässiger Review von Änderungen erfolgt oder wenn der Angreifer in der Lage ist, Codeänderungen ohne Review durchzuführen. Diese Problematik besteht vor allem bei öffentlich erreichbaren Repositorys (typischerweise Open Source), wenn ein Angreifer Zugriff auf die Credentials eines vertrauenswürdigen Nutzers hat (z. B. Credential-Phishing) oder aber der Entwickler selbst „rogue“ geworden ist (z. B. wegen finanzieller Anreize). Bei proprietärer Software hingegen ist es wahrscheinlicher, dass Insider solche Backdoors explizit einbauen und dazu evtl. Reviewprozesse aushebeln. Allerdings zeigt das Codebeispiel bei „The Linux Backdoor Attempt of 2003“ auch, dass eine Backdoor nicht zwingend offensichtlich sein muss.

Angriffe auf die Bereitstellung und Verteilung der Software

In Bezug auf die Situation, dass Software fertig ist und als definierte Version ausgeliefert wird, stellt sich die Frage, ob die vom Hersteller zur Auslieferung vorgesehene Version auch in der originalen Form beim Ziel ankommt. Software oder Software-Update werden teilweise zum Download bereitgestellt und mehr oder weniger wirksam gegen Manipulation geschützt (z. B. durch Prüfsummen oder Signaturen vom Hersteller), sodass eine Kompromittierung des Downloadportals ausreichend ist.

Angriffe über die Reputation der Software bzw. des Herstellers

Software wird heute typischerweise signiert, womit eine Vertrauensstellung elektronisch durchgesetzt wird. Oftmals umfasst die Signatur nicht alle relevanten Teile der Software, sodass durch Modifikation nicht signierter Teile Schadcode eingebettet werden kann. Einen besseren Weg stellen somit in das Kundensystem und Update-Programm integrierte Sicherheitsmechanismen dar, die die Überprüfung der korrekten Signatur und der Software hinsichtlich Umfang und Abdeckung durch die Signatur vornehmen. Hier besteht dann „nur“ das Problem des initialen Vertrauens, aus dem alles weitere abgeleitet werden kann. Eine Kompromittierung dieser Vertrauensinfrastruktur, z. B. über das Stehlen der zum Signieren benutzten Zertifikate, ist allerdings kritisch und konnte in der Praxis auch schon beobachtet werden. Sofern ein Angreifer sich in die Lage versetzt, sich über die Signatur der Software als vertrauenswürdiger Hersteller auszugeben, kann die Signatur als verlässlicher Mechanismus ebenfalls „ausgehebelt“ werden. Das kann z. B. relativ einfach möglich sein, wenn die Signaturüberprüfung nicht ausreichend stark und gesichert ist oder der Angreifer sich Zugriff zu dem Code-Signing-Zertifikat und dem privaten Schlüssel des Herstellers verschafft.

4.1.6 Manipulationen/Fehler in Consumer-IT

In der Betrachtung der Consumer-IT sollen in erster Linie Kommunikationsgeräte oder solche mit Kommunikationsmöglichkeiten aus den Gruppen Tablets, Smartphones, Mobiltelefone und die dazugehörige Kommunikationsinfrastruktur betrachtet werden. Die Vorteile dieser Consumer-IT liegen in der innovativen Handhabung, Erweiterbarkeit und vielfältigen Nutzungsmöglichkeiten. Dem stehen vielfältige Sicherheitsrisiken in der Basisinfrastruktur, der Hardware, dem Baseband, der Betriebssysteme und den Anwendungen gegenüber.

Den größten Marktanteil[32] bilden z.Zt. die Produkte der Unternehmen Apple und Samsung. Aus Eigeninteresse und insbesondere aufgrund der Erwartungshaltung der Geschäftskunden haben diese Firmen viel in Sicherheit investiert, insbesondere Kryptographie. So ist beispielsweise die Dateienverschlüsselung auf den Geräten oder in den Clouddiensten so umgesetzt, dass sie auch für strafverfolgende Behörden eine große Hürde darstellen. Basierend auf den herstellerspezifischen Sicherheitsmaßnahmen können grundsätzlich mit zusätzlichem Aufwand weitere gesicherte Einsatzszenarien im begrenzten Umfang umgesetzt. werden Im Folgenden werden zunächst die grundsätzlichen Schwachpunkte in den o.g. Technikbestandteilen und eine mögliche Kompensierung beschrieben.

Telekommunikationsinfrastruktur

Im Wesentlichen soll hier die Mobilfunkinfrastruktur betrachtet werden. Sicherheitsmaßnahmen wurden von einer Mobilfunkgenerationen zur nächsten beständig ausgebaut (2G, 3G, 4G, 5G) und mögliche Schwachstellen und Angriffsszenarien werden in den internationalen Standardisierungsgremien diskutiert. Es ist jedoch Sache des einzelnen Providers und/oder Staates, die empfohlenen oder möglichen Sicherheitsmaßnahmen entsprechend zu implementieren oder umzusetzen. Dies wird mitunter sehr unterschiedlich gehandhabt. Es bestehen die beiden Grundsatzprobleme der Interoperabilität zwischen den Providern, als auch die Abwärtskompatibilität in den Standards oder Netzgenerationen. Letzteres lässt sich beispielsweise eindämmen, in dem man den Endgeräten die Nutzung älterer Standards wie 2G oder 3G untersagt.

Grundsätzlich lässt sich über die zu verwendende öffentliche Infrastruktur eine eigene Ende-zu-Ende-Verschlüsselung nutzen, die bei einer eventuellen Kompromittierung der Infrastruktur das Erlangen von Gesprächsinhalten verhindert. Zudem lassen sich auch Metadaten (wer kommuniziert mit wem) verschleiern. Eine weitere Gegenmaßnahme ist die Errichtung von eigenen Netzen, zumindest lokalen Campusnetzen. Diese gilt es jedoch nicht nur zur betreiben, sondern auch aktiv zu schützen gegen Ausspionieren über Messgeräte und/oder gefälschten Funkzellen.

Neben dem Schutz vor Spionage ist insbesondere für eine militärische Nutzung auch die resiliente Verfügbarkeit, insbesondere der Schutz vor Sabotage, unabdingbar.

Hardware

Bei der Hardware ist es sehr aufwändig Chip-Design und -Produktion durchgängig und kontinuierlich zu bewerten. Zudem wirken sich der schnelle Entwicklungszyklus und die zeitlich nur vorübergehende Verfügbarkeit der HW-Elemente negativ aus. Dies ist nicht per se negativ, da sich viele

[32] Siehe https://www.idc.com/getdoc.jsp?containerId=prUS47410621

Entwicklungsschritte auch positiv auf Sicherheitsfunktionen auswirken, eine permanente Evaluierung wäre jedoch enorm aufwändig.

Ein erwähnenswertes negatives Beispiel ist die Verwundbarkeit des Snapdragon Chipsatzes, der in Millionen Android-Geräten verbaut ist und der die komplette Übernahme des Smartphones und Manipulation der Daten erlaubt, beispielsweise durch Installation einer kompromittierten App.

Zudem sind Schwachstellen bekannt, die die Kompromittierung des Endgerätes über sogenannte Basebandattacks ermöglichen. Diese erfolgen unterhalb des Betriebssystems und den Anwendungen. Schutzmaßnahmen auf deren Ebene sind daher gegen solche Angriffe nicht wirksam.

Betriebssysteme

Die beiden prominenten Mobilbetriebssystemhersteller Apple und Google investieren umfassend Ressourcen, um die Betriebssysteme und SW-Komponenten sicher zu programmieren und immer wieder neue Schutzmechanismen zu integrieren. Es stehen jedoch die Nutzbarkeit und neue Funktionen (Beispiel: mobile Payment) im Vordergrund. Der Komplexitätsgrad und die beständigen Erweiterungen um Funktionen führen zu Sicherheitslücken, was ein regelmäßiges Aktualisieren obligatorisch macht. Die Betriebssysteme haben zwar einen hohen Sicherheitsgrad erreicht, sie gelten jedoch bestenfalls als temporär sicher und es werden immer wieder auch hochwertige Exploits (insb. der Klassen Remote Code Execution/RCE, Full Chain with Persistence/FCP und Zero Click) bekannt, die die Kompromittierung eines Gerätes erlauben.

Anwendungen

Bei den in den offiziellen Appstores von z.B. Google und Apple verfügbaren Apps ist durch eine stringente Qualitätskontrolle dieser Unternehmen mittlerweile ein hoher Sicherheitsstandard erreicht, so dass mit Schadsoftware versehene Programme relativ selten sind. Malware findet sich im Wesentlichen in alternativen Appstores wieder. Trotzdem ist es für das Erfüllen hoher Sicherheitsanforderungen unabdingbar, allgemein verfügbare Apps zu untersuchen und zu bewerten oder gegebenenfalls ausschließlich auf selbst entwickelte Apps zu setzen, die jedoch ebenso überprüft werden müssen.

4.2 Internationale und nationale Standards

Es konnten keine nationalen oder internationalen Standards identifiziert werden, welche die Herausforderungen der sicheren Lieferkette in Bezug auf vertrauenswürdige IT und die militärischen Belange (oder z.B. die der kritischen Infrastrukturen) abdecken.

In anderen Branchen sind die Standardisierung der Lieferkette (inkl. der Nachverfolgbarkeit von Produkten bis hin zur Herstellung) und entsprechende Regulierung national und international üblich, beispielsweise in der Luftfahrt, der Lebensmittel- und Pharmaindustrie sowie der Automobilbranche und auch in Hinsichtlich auf Gefahrenstoffe. Neben der initialen Herstellung, Distribution und Nutzung ist hier teilw. auch die Entsorgung abgedeckt (siehe z.B. REACH)[33]

Im Bereich der NATO wurde die Herausforderung ebenfalls erkannt. Verfügbare Vorgaben wie z.B. “Technical and Implementation Directive on Supply Chain Security for COTS CIS Security Enforcing Products“ AC/322-D(2017)0016 (INV) adressieren die Aufgabenstellung grundsätzlich, haben aber nicht den Anspruch der Operationalisierung von Detailvorgaben oder der übergreifenden Lösungsherbeiführung.

[33] https://www.umweltbundesamt.de/themen/chemikalien/reach-chemikalien-reach

5 Handlungsempfehlung

Gemeinsames Kapitel BMVg (BMVg CIT) /Industrieverbände (BDSV und Bitkom)

Basierend auf der vorhergehenden Analyse wurde Handlungsbedarf identifiziert, qualifiziert und Handlungsempfehlungen zur weitergehenden Etablierung und Aufrechterhaltung der sicheren Lieferkette abgeleitet.

- Die Fähigkeit zur Etablierung und Aufrechterhaltung der sicheren Lieferkette als Schlüsselfähigkeit sollte im Rahmen der nationalen Anstrengungen angemessen Berücksichtigung finden. Dies sollte einhergehen mit der Umsetzung der Empfehlungen aus dem Ideenpapier „Nationale Schlüsseltechnologien und –fähigkeiten für Entwicklung, Realisierung und Lebenszyklusunterstützung vertrauenswürdiger IT der Bundeswehr“ (vIT), das in den Jahren 20182019 vom EK2 erarbeitet und 2020 veröffentlicht wurde.

- Bei der Absicherung der Lieferkette ist grundsätzlich der gesamte Produktlebenszyklus inklusive der Entwicklung, Produktion, Nutzung und Weiterentwicklung zu betrachten. Hierfür sind realistische Zyklen und der Einbezug spezifischer Rahmenbedingungen sowie gemeinsame Standards und Methoden unerlässlich. Hierzu sollte ein konsistentes Management System über den gesamten Prozess hinweg (inkl. Risikomanagement, Metrik, Verifikation/Validierung) etabliert werden, welches sowohl durch die Anbieter (z.B. Hersteller, Systemintegratoren) der jeweiligen Produkte wie auch durch die anwenderseitigen Integratoren dieser Produkte anzuwenden ist.

- Die unterschiedlichen Anwendungsfälle für sichere Lieferketten und die jeweils benötigte spezifische Ausprägung sind derzeit noch nicht hinreichend konzeptionell erschlossen und entsprechend noch nicht umfänglich regulatorisch abgebildet. Zur Ermöglichung der nachhaltigen Handlungsfähigkeit und -sicherheit sollten die Anforderungen zur Etablierung und Aufrechterhaltung für sichere Lieferkette(n) hinsichtlich der Technisch-Logistischen Betreuung (TLB)[34] durch das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) als Grundlage f. Rüstungsprojekte präzisierend beschrieben werden.

- Die in den Detailbetrachtungen identifizierten spezifischen Handlungsfelder (z.B. Operationalisierung und Regulierung, Ableitung einer Metrik, Etablierung spezifisches Risikomanagement) 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 ist wünschenswert, aber für bereits vorhandene Systeme „nachträglich“ bis z.B. zu den einzelnen elektronischen Bausteinen unrealistisch oder unwirtschaftlich. Deshalb sind stattdessen im Rahmen des Lebenszyklus

[34] Siehe hierzu Beschreibung CPM – Customer Product Management, Verfahrensvorschrift zur Bedarfsermittlung und Bedarfsdeckung in der Bundeswehr (A-1500/3); https://www.bundeswehr.de/de/organisation/ausruestung-baainbw/ruestungsprojekte/customer-product-management

Maßnahmen einzuführen, mit denen Risiken jeweils erkannt, bewertet und mitigiert werden können. Hierzu ist anbieter- und anwenderseitig ein Risikomanagement zu etablieren.

- Als Grundlage zur praktischen Etablierung, Aufrechterhaltung und Bewertung sowie Weiterentwicklung der sicheren Lieferkette und damit zusammenhängender Management Systeme (Prozesse, Kennzahlen) sollten sowohl industrie- als auch amtsseitig die hierfür relevanten technischen Informationen (z.B. digitale Stücklisten mit notwendiger Granularität, Konfigurationsinformationen, Risikobewertung) durchgängig und digital erfasst, zwischen den beteiligten Stellen (einschließlich den Anwendern) ausgetauscht und über den Lebenszyklus hinweg verwendet werden. Hierfür sollten nach Möglichkeit offene Standards und gemeinsamer Wortschatz zur Anwendung kommen, um von Anfang an interoperabel zu sein und den Aufwand zur Realisierung und Weiterentwicklung dieser Grundlagen für alle Beteiligten so gering wie möglich halten zu können.

- Etablierung und Nutzung akkreditierter Prüfstellen und Prüfverfahren, die Tests und Prüfung im Rahmen von Zertifizierungen, Akkreditierungen und Zulassungen durchführen. Diese Verfahren sind grundsätzlich aus dem Kontext vertrauenswürdiger IT-Komponenten aber auch der Eignungs- und Einsatzprüfungen komplexer Systeme bekannt. Generell ist nicht nur zu prüfen, ob die gewünschten Funktionen erfüllt werden, sondern auch darauf, ob weitere, gegebenenfalls unerwünschte oder sogar schädliche Funktionen erfüllt werden (können). Eine Durchführung solcher Prüfungen setzt allerdings gegebenenfalls voraus, dass die Prüfstelle über hinreichende Produktinformationen bis hin zum Quellcode verfügt, was in der Regel nur bei nationalen Herstellern gefordert und durchgesetzt werden kann. Zu beachten ist hier auch das gesamte Konfigurationsmanagement solcher Produkte und die Notwendigkeit erneuter Prüfungen nach Updates oder Konfigurationsänderungen. In der Praxis werden derartige Prüfungen derzeit nur für wenige Produkte ermöglicht, die in sicherheitskritischen Bereichen verwendet werden. Zu berücksichtigen ist auch, dass solche Prüfungen aufwändig und sind und nachgehalten werden müssen. Für komplexe im GB BMVg bereits genutzte Systeme wird es als unwahrscheinlich erachtet, dass derartige Prüfungen effektiv und effizient nachträglich vorgenommen werden können.

- Die Informationen zur sicheren Lieferkette, deren Überwachung und Risikomanagement sollten durch GB BMVg und Industrie in eine gemeinsame Lage InfoSichh eingebracht und so die gemeinsame Sicht aller beteiligten Stellen und deren Handlungsfähigkeit gestärkt werden.

5.1 Analyse/Einordnung in internationalen Kontext

Einige der im Rahmen der Arbeit des Expertenkreises 2 identifizierten Handlungsfelder bzw. –themen werden bereits im Rahmen internationaler Forschungs- und Gremien-Aktivitäten mit unterschiedlicher Ausprägung DEU Teilhabe betrachtet.

EU: Es existiert eine Initiative der EU zur Förderung der europäischen Fähigkeiten hinsichtlich Entwicklung und Fertigung sowie Integration von Prozessoren und Halbleitern.[35] [36]

EDA: Im Rahmen des Vorhabens EXCEED (trustEd and fleXible system-on-Chip for EuropEan Defence application) wird die Etablierung und Nutzung vertrauenswürdiger "System-On-Chip" Technologie und Ökosystem für militärische Anwendungen untersucht.[37]

NATO: Im Rahmen der Entwicklung des Federated Mission Networking (FMN [38] [39]) unter Schirmherrschaft des NATO Allied Command Transformation (ACT) werden auch die Sicherheit der Lieferkette(n) als wichtiger Faktor erkannt und betrachtet. Spezifische operationelle Standards sind hierzu bisher noch nicht verfügbar. [40] [41]

Bi-laterale und multi-laterale Kooperationen: Der GB BMVg hat mehrere Kooperationen mit Partnernationen hinsichtlich Cyber/Informationstechnik (z.B. Cyber/IT Engagement Framework/CITEF[42][43]) oder Rüstung (z.B. Organisation for Joint Armament Co-operation/OCCAR[44]) vereinbart.

Im Rahmen der weiteren Aktivitäten auf der Basis der im vorhergehenden Abschnitt und den in den folgenden Abschnitten empfohlenen Maßnahmen sollten die bereits laufenden und geplanten internationalen Aktivitäten im Detail hinsichtlich der Nutzbarkeit zur Stärkung der Fähigkeit zur Etablierung und Aufrechterhaltung sicherer Lieferketten für vertrauenswürdige IT analysiert und dort Themen bei Bedarf eingebracht werden.

[35] https://digital-strategy.ec.europa.eu/en/library/joint-declaration-processors-and-semiconductor-technologies

[36] https://www.heise.de/news/IPCEI-Mikroelektronik-EU-Halbleiterfertigung-fuer-mehr-als-100-Milliarden-Euro-4983443.html

[37] https://www.eda.europa.eu/info-hub/press-centre/latest-news/2020/11/05/exceed-defence-research-project-kicks-off

[38] https://www.act.nato.int/activities/fmn

[39] https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx

[40] http://www.cjoscoe.org/infosite/wp-content/uploads/2020/03/2020-Allied-Interoperability-and-Integration-Guide_Version-2.0.pdf

[41] https://usacac.army.mil/sites/default/files/publications/20-12web.pdf

[42] https://www.bundeswehr.de/resource/blob/1467690/728e2f22986b85a2feb69792f805d840/nv-31-2020-abt-iv-data.pdf

[43] https://www.afcea.org/content/nations-intensify-cooperation-cyberspace

[44] http://www.occar.int/

5.2 Nutzung offener Standards und Initiativen

Aufgrund der Komplexität und Interdependenz der einzelnen Elemente der sicheren Lieferkette ist eine Betrachtung auf Ebene der Elemente bzw. Organisationen und Wertschöpfungsschritten unerlässlich. Nur so kann eine durchgängig sichere und nachvollziehbare Lieferkette erreicht werden.

Hierzu bietet sich die Etablierung und Umsetzung von Mindeststandards und Maßnahmen gemeinsamer interoperabler Standards an. Solche Standards und deren Umsetzung bilden die Basis für vertrauenswürdige Zertifizierung und transparenten Auditierung entsprechender Anteile der Lieferkette. Fernerhin können durch die Anwendung von Standards die notwendige Orchestrierung und Operationalisierung des übergreifenden Managementsystems zur sicheren Lieferkette ermöglicht und der für einzelne Organisationen notwendige Aufwand optimiert werden. Außerdem können Umsetzungsrisiken minimiert werden.

Sowohl im Bereich der Informationstechnologie und Informationssicherheit als auch generell bei Managementsystemen (z.B. Qualitätsmanagement) haben sich die breite Verfügbarkeit, also die Vermeidung proprietärer bzw. nationaler Ansätze, und die übergreifende Akzeptanz und die Eigenschaft „Interoperability by Design“ als entscheidend für die Wirksamkeit und Zukunftsfähigkeit erwiesen.

Weitere Erfolgsfaktoren sind der effiziente Einsatz verfügbarer Mittel und Ressourcen, die „betriebsbegleitende“ Umsetzbarkeit und die kontinuierliche Weiterentwicklung aller Elemente der sicheren Lieferkette im Kanon mit anderen relevanten Methoden und Standards, wie z.B. Architekturmethoden und Qualitätsstandards. Ein weiterer Faktor ist die technische Unterstützung z.B. durch Werkzeuge wie z.B. Threat & Risk Intelligence Exchange, Prozessautomation, Einbindung in Systeme wie Product Lifecycle Management, IT-Service Management & Control, Information Security Management.

In den beiden folgenden Abschnitten wird als Ergebnis der Arbeit des EK2 jeweils ein Beispiel für relevante Standards erläutert. Eine Nutz- und Adaptierbarkeit für die sichere Lieferkette im Kontext der vertrauenswürdigen IT für die Bundeswehr sollte analog zu den weiteren empfohlenen Maßnahmen geprüft werden.

5.2.1 Zertifizierung von Organisationen

Eine entscheidende Rolle bei der Etablierung und Aufrechterhaltung der sicheren Lieferkette haben neben dem Bedarfsträger, in dessen Verantwortung unter anderem die Planung und Anforderungsdefinition liegen, auch die Hersteller und Systemintegratoren als wertschöpfende und ausführende Elemente im Rahmen der Bedarfsdeckung. Dazu gehört auch die Lebenszyklusunterstützung. Daher ist es erforderlich, dass diese beiden Rollenträger unter Anwendung zueinander interoperabler Methoden, Standards und Verfahren zusammenarbeiten.

Im Bereich der IT-Architektur haben sich das „The Open Group Architectural Framework“ (TOGAF[45]) und das NATO Architecture Framework (NAF[46]) als interoperable Methoden-Standards für IT- und Prozessarchitektur im militärischen und industriellen Umfeld bewährt.

Für den Bereich der Zertifizierung sicherer Lieferketten existiert das „The Open Trusted Technology Provider Standard (O-TTPS) Certification Program“[47]. Um dem steigenden Bedarf nach prüfbarer Vorgabenkonformität von IT-Produkten und Sicherheit über die unterschiedlichen Elemente und Wertschöpfungsschritte der Lieferkette und des Produktlebenszyklus hinweg gerecht zu werden, wurde dieses Programm von betroffenen Organisationen entwickelt. Der zu Grunde liegende offene Standard umfasst Best Practices hinsichtlich aller Phasen des Produktlebenszyklus für IT-Produkte und deren (globaler) Lieferkette.

5.2.2 Transparenz zu Produktbestandteilen

Zur Etablierung und Aufrechterhaltung von Informationssicherheit und Nachprüfbarkeit von Produkteigenschaften, Lieferketten und der Lebenszyklusunterstützung sind verlässliche und detaillierte Informationen zu den Bestandteilen von IT-Komponenten und deren Konfiguration etc. essenziell. Sinnvollerweise werden diese Informationen standardisiert elektronisch gesichert zwischen den beteiligten Organisationen ausgetauscht, damit die Weiterverarbeitung und die Aktualisierung möglichst frei von Medienbrüchen und Verzögerungen erfolgen können.

Hierzu sind auch die vertrauenswürdige, ggf. partielle, Attestierung der Korrektheit der Informationen auf Ebene der Komponenten und die Bereitstellung der Information über die Lieferkette hinweg erforderlich. Das „The Digital Bill of Materials (DBOM[48]) Consortium“, bestehend aus Industrie, Forschungs- und Regierungsorganisationen, hat dazu einen Methoden-Standard sowie technische Schnittstellen entwickelt. Das Projekt wurde der Linux Foundation zur Pflege übergeben und Ergebnisse werden u.a. via GitHub[49] veröffentlicht. Ausgerichtet auf z.B. Hersteller von IT-Komponenten und Betreiber kritischer Infrastrukturen hat sich international bereits ein Ökosystem entwickelt, in dem dieser Standard von den Beteiligten angewendet und weiterentwickelt wird.

Eine spezifische Adaption der DBOM ist die sog. Software Bill of Materials (SBOM[50]). SBOM ist ein Konzept für ein verschachteltes effektives Inventarverzeichnis von SW-Komponenten bzw. Bausteinen.

[45] https://www.opengroup.org/togaf

[46] https://www.nato.int/cps/en/natohq/topics_157575.htm?

[47] https://www.opengroup.org/certifications/o-ttps

[48] https://dbom-project.readthedocs.io/en/latest/what-dbom.html

[49] https://github.com/DBOMproject

[50] https://www.ntia.gov/sbom

Das Ziel ist, schon im Laufe der Entwicklung die Informationen auf möglichst niedriger Ebene für alle SW-Komponenten, auch von Dritten, bereitzustellen. Dazu gehören neben den typischen Inventarinformationen auch Konfigurations- und Schwachstelleninformationen. Dieser Ansatz wurde von der US-amerikanischen National Telecommunications and Information Administration initiiert und dann wie DBOM durch eine Community of Interest konzeptionell weiterentwickelt und adaptiert. SBOM findet im Bereich der kritischen Infrastrukturen und missionskritischer IT insbesondere in den USA bzw. bei der US-Regulierung unterliegenden Produkten und Märkten zunehmend Verwendung.

5.3 Vorschlag für eine Metrik „schutzbedarfsabhängige Anforderungen an Lieferkette und deren Absicherung“

Für die Etablierung und Aufrechterhaltung der sicheren Lieferkette ist die Gewährleistung der eindeutigen Identifikation und Herkunft der einzelnen Produkte unerlässlich.

Die Anforderungen an die Produkteigenschaften sowie die sichere Lieferkette sind abhängig von dem Schutzbedarf eines Einzelproduktes (z.B. Komponente) bzw. des übergreifenden Systems festzulegen. Organisatorische Anforderungen an Produkteigenschaften können z.B. die anzuwendende Regulierung sein und Anforderungen hinsichtlich der zur Herstellung qualifizierten Unternehmen bzw. Herkunftsländer. Technische Produkteigenschaften sind z.B. die Beschaffenheit von spezifischen Funktionen und Mechanismen.

Im Laufe des Produktlebenszyklus kann sich Änderungsbedarf an den initialen Anforderungen bzw. deren Umsetzung ergeben, dabei können Faktoren wie veränderte politische Rahmenbedingungen oder neue technische Entwicklungen dazu führen, dass Risikobewertung und der Schutzbedarf angepasst werden müssen.

Ausgehend vom "Ist-Zustand" wird hier nie eine vollständige Sicherheit erreicht werden können. So werden selbst für sehr hohen Schutzbedarf, also z.B. für VS-Kryptoprodukte, teilweise handelsübliche Field Programmable Gate Arrays (FPGAs) verwendet. Entsprechend ist für die Etablierung und Aufrechterhaltung sicherer Lieferketten ein Risikomanagement unabdingbar. Dieses Risikomanagement muss den gesamten Lebenszyklus eines Systems bzw. der Komponente(n) abdecken und bezüglich der Anforderungen und Vorgaben umso spezifischer ausgeprägt werden, je höher der Schutzbedarf festgelegt wurde.

Da die Bereitstellung uneingeschränkt vertrauenswürdigen (Teil-)Komponenten nicht machbar ist, sind hier entsprechende Lösungsansätze vorzusehen. Z.B. muss abhängig vom Schutzbedarf das Lieferkettenkonzept ggf. eine "Kapselung" von Teilkomponenten (z.B. Mikroelektronik-Komponenten nicht vertrauenswürdiger Herkunft, die aber unbedingt benötigt werden) vorsehen und die Anforderungen daran beschreiben.

Im Rahmen der Arbeit des Expertenkreis 2 wurde ein erster Vorschlag zur Metrik hinsichtlich Ausprägung der Anforderungen an sicherere Lieferkette(n) und deren Absicherung in Abhängigkeit vom Schutzbedarf des Systems und dessen Komponenten erarbeitet:

- Kategorie 1 - sehr geringer Schutzbedarf: Verwendung handelsüblicher IT-Produkte. Nur Berücksichtigung funktionaler und wirtschaftlicher Kriterien

- Kategorie 2 - geringer Schutzbedarf: Es sollte ein "Lieferkettenkonzept" erarbeitet werden, in dem eine Differenzierung zwischen Teilen eines Systems hinsichtlich deren Sicherheitskritikalität erfolgt. Auf dieser Grundlage werden dann Maßnahmen mit Blick auf Lieferketten festgelegt. Es werden aber weiterhin handelsübliche IT-Produkte verwendet.

- Kategorie 3 - mittlerer Schutzbedarf: Wie bei "geringer Schutzbedarf", jedoch werden für sicherheitskritische Teile des Systems Festlegungen hinsichtlich der Produktherkunft (z.B. aus Europa, aus Deutschland, aus einem NATO-Land etc.) getroffen. Die Festlegung, welcher Teil des Systems wie sicherheitskritisch ist, erfolgt dabei nach einem noch festzulegenden standardisierten Verfahren. Es werden noch keine Forderungen auf der Ebene der Teilkomponenten (z.B. Speicherelement aus Deutschland) getroffen, aber grundlegende Anforderungen an Standards der einzelnen Phasen der Lieferkette bzw. des Produktlebenszyklus gestellt. Diese müssen von den Herstellern und ggf. anderen Beteiligten im Rahmen des Lebenszyklus eingehalten und diese Einhaltung durch entsprechende Zertifizierung nachgewiesen werden.

- Kategorie 4 - hoher Schutzbedarf: Wie bei "mittlerer Schutzbedarf, jedoch mit stärkerer Einschränkung hinsichtlich der Produktherkunft, -eigenschaften und -handhabung (z.B. wie aus dem Umfeld der VS-IT oder auch anderen sensitiven Gütern bekannt). Es muss die Einhaltung von Standards durch den gesamten Lebenszyklus hinweg durch entsprechende Zertifizierungen nachgewiesen und kontinuierlich überwacht werden. Teilweise werden hier auch Forderungen auf der Ebene von Teilkomponenten (z.B. Herkunft Mikroelektronik) gestellt.

- Kategorie 5 - sehr hoher Schutzbedarf: Wie hoher Schutzbedarf jedoch noch stringentere Forderungen auf der Ebene der Teilkomponenten.

Die Überprüfung der Umsetzbarkeit hinsichtlich Anforderungskonformität und Wirksamkeit sowie die kontinuierliche Überwachung zur Aufrechterhaltung und bedarfsorientierten Weiterentwicklung des initial etablierten Absicherungsniveaus sind im Lebenszyklus zu berücksichtigen.

5.4 Regulierungs- und Operationalisierungsbedarf

Die IT der Bundeswehr unterliegt hohen Ansprüchen an die Vertrauenswürdigkeit. Diese sind in verschiedenen gesetzlichen und untergesetzlichen Vorgaben erfasst. Grundsätzlich ist für die Beschaffung von Rüstungsgütern durch die Bundeswehrverwaltung (Art. 87b GG) das öffentliche Vergaberecht einschlägig.

Besondere Anforderungen an die Vertrauenswürdigkeit, insbesondere die Sicherstellung der Informationssicherheit, wird an VS-IT gestellt, also Informationstechnik zur Handhabung von Verschlusssachen (VS). Dies ergibt sich aus dem Sicherheitsüberprüfungsgesetz (SÜG[51]), in dem festgelegt ist, dass das BMVg im Einvernehmen mit dem Bundeministerium des Innern, für Bau und Heimat (BMI) allgemeine Verwaltungsvorschriften zur Ausführung des Gesetzes erlässt. Dies erfolgt in einer eigenen Verschlusssachenanordnung (VSA-BMVg), die nach der Änderung der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA[52]) des BMI im Jahr 2018 zurzeit durch das BMVg erstellt wird. In der VSA-BMVg sollen, soweit möglich, die Besonderheiten von VS-IT im Gegensatz zum Umgang mit „Papier-Verschlusssachen“ berücksichtigt werden. Für die Nutzung von VS-IT ist gem. § 50 VSA eine Freigabe durch die jeweilige Dienststellenleitung erforderlich. Produkte, die innerhalb von VS-IT Sicherheitsfunktionen übernehmen, sind gem. § 52 VSA vor ihrem Einsatz vom Bundesamt für Sicherheit in der Informationstechnologie (BSI) zuzulassen.

Auch außerhalb des Umgangs mit VS spielen nationale Vorgaben der zuständigen Behörde eine Rolle. So prüft und zertifiziert das BSI informationstechnische Produkte oder Komponenten sowie informationstechnische Systeme nach Common Criteria (CC) oder Technischen Richtlinien.[53] In Schutzprofilen werden generische Anforderungen an eine Produktkategorie festgeschrieben, dies sind sowohl Anforderungen an die Funktionalität als auch an die Vertrauenswürdigkeit. Durch die Schutzprofile kann das BSI also Mindeststandards für bestimmte Produktgruppen setzen.

Im GB BMVg gelten für den Umgang mit IT besondere Regeln. Eine zentrale Rolle spielt dabei die Allgemeine Regelung „Informationssicherheit“ (A-960/1). Die darin enthaltenen Vorgaben berücksichtigen den IT-Grundschutz des BSI, allerdings gibt es – den besonderen Aufgaben und somit Anforderungen der Streitkräfte entsprechend – bundeswehrspezifische Ergänzungen.

Ergänzend zu den bereits erwähnten Kompetenzen des BSI nimmt das Prüfzentrum für IT-Sicherheit in der Bundeswehr (PZITSichhBw) Prüf- und Beratungsaufgaben im GB des BMVg wahr. Das PZITSichhBw ist bisher die einzige nach ISO/IEC 17025:2018 vom BSI anerkannte Prüfstelle im Zuständigkeitsbereich des BMVg. Das PZITSichhBw wurde am 1. Oktober 1992 mittels Erlasses durch das BMVg an der Wehrtechnischen Dienststelle 81 (WTD 81) im Geschäftsfeld 210 „IT-Sicherheit“ eingerichtet und war damit eine der Grundlagen für die fachliche Zusammenarbeit mit dem BSI. Im Rahmen dieser Tätigkeit werden IT-Sicherheitsprodukte nach Common Criteria im ständigen Dialog mit dem Auftraggeber, dem Hersteller und dem BSI geprüft. Das Ziel ist, diese für VS-Verarbeitung durch das BSI zuzulassen und in der Bundeswehr und Behörden einzusetzen. Dazu verfügt das PZITSichhBw über eigene Labor- und Testeinrichtungen. Des Weiteren übernimmt das PZITSichhBw eine Beratungsfunktion für Vorhaben

[51] http://www.gesetze-im-internet.de/s_g/
[52] https://www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/staatlicher-geheimschutz/staatlicher-geheimschutz-node.html
[53] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/VB-Produkte.pdf?__blob=publicationFile&v=1

und Projekte in allen Phasen des CPM hinsichtlich des Projektelements „Informationssicherheit, IT-Architektur/-Standardisierung und Datenschutz“.

Im GB BMVg ist für IT grundsätzlich eine Akkreditierung und Freigabe zur Nutzung erforderlich. Für die Prüfung und Akkreditierung ist die Deutsche militärische Security Accreditation Authority (DEUmilSAA) zuständig, diese Aufgabe ist ihr vom BMI für alle Akkreditierungsbelange des GB BMVg übertragen worden. Die DEUmilSAA gehört zum Zentrum für Cybersicherheit der Bundeswehr (ZCSBw) und fungiert als Schnittstelle zwischen den Projekten im GB BMVG auf der einen Seite und den für die Regulierung und Zulassung von IT zuständigen nationalen und internationalen Stellen (z.B. national dem BSI, international der NATO MILITARY COMMITTEE COMMUNICATIONS AND INFORMATION SYSTEM SECURITY AND EVALUATION AGENCY/SECAN) auf der anderen Seite.

Das ZCSBw hält neben der Akkreditierung auch Fähigkeiten zur Schwachstellenanalyse und für Penetration Testing vor. Mit diesen Fähigkeiten ist die Bundeswehr in der Lage, priorisiert vorhandene und in Einführung befindliche Systeme zu untersuchen. Die Ergebnisse sind Grundlage für Akkreditierungen, Freigaben oder Vorgaben zur Mitigation.
Für wehrtechnisch genutzte Produkte erstellt das BAAINBw regelmäßig „Technische Lieferbedingungen“ (TLB)[54], die technische und technisch-organisatorische Forderungen aufstellen. Sie orientieren sich an den zivilen DIN-Normen (DIN 820-Reihe). Für die Überprüfung der Einhaltung dieser TLB verfügt das BAAINBw über Organisationselemente zur Qualitätssicherung und Güteprüfung. Die Anpassung bzw. Erstellung entsprechender TLB wären eine Möglichkeit, Aspekte der sicheren Lieferkette im Beschaffungsvorgang stärker zu berücksichtigen und Mindeststandards einzuführen.

Sollen Aspekte der Lieferkettensicherheit stärker berücksichtigt werden und als Anforderungen in die Beschaffung von IT einfließen sind voraussichtlich erhebliche Aufwände im Bereich Prüfung, Zulassung und Zertifizierung erforderlich. Grundsätzlich ist daher zu prüfen, ob und wie externe Prüf- und Zertifizierungsstellen (analog zur Zertifizierung gem. ISO-Standards) eingebunden werden können.

Um dem Ziel sicherer Lieferketten für vertrauenswürdige IT im GB BMVg möglichst nahe zu kommen wäre ein Managementsystem wünschenswert, in das Industrie und Amtsseite durchgehend über den gesamten Prozess hinweg eingebunden sind. Dies beinhaltet das Risikomanagement, eine Metrik, Lage und Validierung/Verifikation. Dafür sind neben gemeinsamen Standards und deren Operationalisierung entsprechende Strukturen und Ressourcen bei allen beteiligten Organisationen erforderlich.

Im IT-Sicherheitsgesetz 2.0[55], das in Federführung des BMI erarbeitet und im Bundestag verabschiedet wurde, werden Vorgaben mit Relevanz für die Lieferketten von bestimmten Organisationen gemacht (z.B. KRITIS[56], sowie Unternehmen im besonderen öffentlichen Interesse). Im Rahmen des Gesetzgebungsverfahrens war das BMVg beteiligt, die Industrieverbände BDSV[57] und Bitkom[58] wurden angehört. Aus den Regelungen des neuen Gesetztes und den zu erschaffenden Rechtverordnungen können Auswirkungen auf bzw. Wechselwirkungen mit den zukünftigen sicheren Lieferketten für die vertrauenswürdige IT des GB BMVg entstehen. Diese sollten im weiteren Vorgehen zwischen dem GB BMVg und der Industrie betrachtet und berücksichtigt werden.

[54] https://www.bundeswehr.de/de/organisation/ausruestung-baainbw/vergabe/technische-lieferbedingungen
[55] https://www.bundestag.de/dokumente/textarchiv/2021/kw16-de-sicherheit-informationstechnischer-systeme-834878
[56] https://www.kritis.bund.de/SubSites/Kritis/DE/Rechtsrahmen/IT-SiG_node.html
[57] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/it-sicherheitsgesetz/bdsv-stellungnahme.pdf?__blob=publicationFile&v=3
[58] https://www.bitkom.org/sites/default/files/2020-12/201211_sn_bitkom_it-sicherheitsgesetz_2.0.pdf

5.5 Umgang mit den Handlungsempfehlungen

Die in diesem Ideenpapier beschriebenen Erkenntnisse und Empfehlungen zur weiterführenden Etablierung und Aufrechterhaltung sicherer Lieferketten werden durch die am strategischen Industriedialog teilnehmenden Organisation im Rahmen ihrer jeweiligen Zuständigkeit weiter verfolgt.

Im Rahmen dessen werden im Expertenkreis 2 gemäß der Mandatierung durch den Gesprächskreis 4 folgende Themen weiter behandelt werden:

- Nähere Betrachtung der Erstellung von TLB für sichere Lieferketten als Grundlage für Rüstungsprojekte und deren Lebenszyklusmanagement
- Austauschen der Teilnehmenden, wie relevante Informationen zur Lieferkette in ein gemeinsames Cyberlagebild eingebracht werden können
- Identifikation und Berücksichtigung von Erkenntnissen („Lessons Learned“) zu sicheren Lieferketten und vertrauenswürdiger IT aus der COVID-19 Pandemie

6 Urheberschaftsnachweis

An diesem Dokument als Ergebnis der Arbeiten des Expertenkreises 2 haben Vertreter der Mitgliedsunternehmen der Verbände BDSV e.V. und Bitkom e.V. sowie das Bundesministerium der Verteidigung und der Geschäftsbereich des BMVg aktiv mitgewirkt. Es wird nochmals ausdrücklich auf die Ausführungen auf Seite 4 und die ausgewiesene Urheberschaft und Verantwortlichkeit hingewiesen. Diese wird hier gesammelt zusammengefasst dargestellt:

Gemeinsame Kapitel/Abschnitte von BMVg und den Industrieverbänden sind:

- 1 Vorwort
- 2 Zielsetzung des Expertenkreises
- 3 Ergebnisse im Überblick
- 4 Detailbetrachtungen (mit Ausnahme 4.1.2 – 4.1.5)
- 5 Handlungsempfehlung

Die Industrieverbände BDSV und Bitkom verantworten folgende Kapitel/Abschnitte:

- 4.1.2 Manipulation/Fehler im Fertigungsprozess Mikroelektronik inkl. Firmware
- 4.1.3 Manipulation/Fehler in COTS Hardware-Komponenten
- 4.1.4 Manipulation/Fehler in weiterverwendeten Software-Komponenten Dritter und Software-Lieferketten
- 4.1.5 Manipulation/Fehler in eigenentwickelten Software-Komponenten

Seitens der Verbände BDSV e.V. und Bitkom e.V. haben folgende Mitgliedsunternehmen im EK2 und bei der Erstellung dieses Dokumentes mitgewirkt:

- Airbus Defence and Space GmbH
- Atos Information Technology GmbH
- Cisco Systems GmbH
- Fujitsu Technology Solutions GmbH
- genua GmbH
- Hensoldt Sensors GmbH
- INFODAS GmbH
- Rheinmetall Electronics GmbH
- Rohde & Schwarz GmbH & Co. KG
- SAP Deutschland SE & Co. KG
- Software AG Deutschland GmbH
- T-Systems International GmbH

- Utimaco GmbH