Ideenpapier

„Nationale Schlüsseltechnologien und -fähigkeiten für Entwicklung, Realisierung und Lebenszyklusunterstützung vertrauenswürdiger IT der Bundeswehr“

Ergebnisse des Expertenkreises 2 (EK2)
im Rahmen des Gesprächskreises Innovationen Cyber/IT (GK 4 ICIT)

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

im Rahmen des strategischen Industriedialoges

zwischen
dem Bundesministerium der Verteidigung
und dem Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V.

Version: Mitgeprüfte und mitgezeichnete Vordruckversion nach Vorlage Leitung BMVg
Stand 07. August 2019

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

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 ... **4**

2 Zielsetzung des Expertenkreises ... **5**

3 Ergebnisse im Überblick ... **8**

4 Detailbetrachtungen ... **11**
4.1 Gefährdungen für vertrauenswürdige IT ... 11
4.1.1 Hardware am Beispiel von MELTDOWN und SPECTRE ... 11
4.1.2 Software am Beispiel des Heartbleed-Bug ... 12
4.1.3 Hardwarenahe Software/Firmware am Beispiel Exploit BadUSB ... 13
4.2 Randbedingungen der im GB BMVg und im kommerziellen Massenmarkt eingesetzten IT Produkte ... 14
4.3 Detailbetrachtung pro Handlungsfeld ... 16
4.3.1 Embedded IT ... *16*
4.3.2 IT-Komponenten Land-, Luft- und Seefahrzeuge ... *18*
4.3.3 IT-Bausteine und -funktionen in IT-Sicherheitsprodukten inkl. HW für das mil. Umfeld – Fokus sichere Netzwerkschnittstelle ... *20*
4.3.4 IT-Bausteine und -funktionen in IT-Sicherheitsprodukten inkl. HW für das mil. Umfeld – Fokus Verschlüsselung ... *22*
4.3.5 IT-Bausteine und -funktionen in IT-Sicherheitsprodukten inkl. HW für das mil. Umfeld – Fokus Security Gateways ... *23*
4.3.6 Absicherung pot. unsicherer Betriebssysteme und Laufzeitumgebungen ... *25*
4.3.7 Absicherung Middleware ... *27*
4.3.8 Realisierung sicherer Führungsinformationssysteme (C4ISR) ... *30*
4.3.9 Sicherer Betrieb komplexer IT-Umgebungen ... *32*
4.3.10 Absicherung der Lieferketten ... *35*
4.3.11 Schnittstelle Projekt/Rüstung ... *40*
4.3.12 IT-Sicherheitsüberprüfung von IT-Systemen und Zulassung für den VS-Betrieb ... *43*
4.3.13 Akkreditierung von IT-Systemen ... *46*
4.3.14 Zukünftige Anwendungsgebiete ... *48*
4.2.14.1 Moving Target Defence (MTD) ... *51*
4.4 Einordnung in IT-Architektur und Wertschöpfungskette ... 52
4.5 Bewertung Beitrags- und Zukunftsfähigkeit ... 53

5 Handlungsempfehlung ... **55**
5.1 Entwicklung „Vision“ ... 56
5.1.1 Schnittstelle Projekt/Rüstung ... 56
5.1.2 IT-Sicherheitsüberprüfung von IT-Systemen und Zulassung für den VS-Betrieb ... 57
5.1.3 Akkreditierung ... 57
5.1.4 Moving Target Defence (MTD) ... 58
5.2 Zuordnung Handlungsbedarf ... 59
5.2.1 Schnittstelle Projekt/Rüstung ... *59*
5.2.2 IT-Sicherheitsüberprüfung von IT-Systemen und Zulassung für den VS-Betrieb ... *60*
5.2.3 Akkreditierung ... *60*
5.2.4 Moving Target Defence (MTD) ... 61
5.3 Empfohlene Maßnahmen ... 63
5.3.1 Schnittstelle Projekt/Rüstung ... 64
5.3.2 IT-*Sicherheitsüberprüfung von IT-Systemen und Zulassung für den VS-Betrieb* ... 65

5.3.3 Akkreditierung 65
5.3.4 Moving Target Defense (MTD) 65
5.4 Analyse/Einordnung in internationalen Kontext 66
5.5 Ausblick 68

6 Anhang 69
6.1 Urheberschaft 69
6.2 Referenzen und Quellen 71
6.3 Abkürzungsverzeichnis 73

Abbildungsverzeichnis Seite

Abbildung 1: Zuordnung zum Entstehunggang von IT-Systemen 6
Abbildung 2: Betrachtung Funktionale Cluster 7
Abbildung 3: Randbedingungen von IT-Produkten 15
Abbildung 4: Fähigkeitsbezoene Schwerpunkte für die Ausrichtung wehrtechnischer F&T im Bereich Cyber/IT 2019/2020 69

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 04. September 2017 wurde der bereits identifizierte Handlungsbedarf für den Themenbereich vertrauenswürdige IT priorisiert und seitdem auf Fachebene im Expertenkreis „Nationale Schlüsseltechnologien und -fähigkeiten für Entwicklung, Realisierung und Lebenszyklusunterstützung vertrauenswürdiger IT der Bundeswehr“ (EK 2) diskutiert. Hierbei liegt der Fokus auf mittel bis langfristig wirkende Maßnahmen mit nachhaltigem Nutzen.

Sowohl seitens BMVg, des Geschäftsbereich BMVg als auch der Verbände von Seiten der Industrie/Wirtschaft wurden hierfür ständige Vertreter benannt. Die Leitung des EK2 erfolgt gemeinsam durch einen Vertreter BMVg und einen Vertreter Verbände, die Leitung für die Verbände wird durch den Bitkom gestellt. Die Verbände BDSV und Bitkom von Seiten der Industrie/Wirtschaft haben eine gemeinsame Position und Ideen in das vorliegende Dokument eingebracht.

Das vorliegende Dokument enthält die Ergebnisse des EK2 aus der Periode Dezember 2017 bis Juni 2019 und basiert auf den Beiträgen der beteiligten Vertreter. Dieses Dokument stellt den Gesamtbeitrag GK ICIT/EK 2 zur Fortführung und Detaillierung des Diskussionsprozesseses dar und bildet eine unverbindliche Grundlage zur Anregung weiterer Schritte.

Berlin, im August 2019

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)

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). Die Qualität und Quantität von Cyberangriffen nimmt in allen Bereichen zu. Um diesem Trend entgegenzuwirken und zugleich digitale Souveränität zu erreichen, kommt dem Einsatz ausreichend vertrauenswürdiger IT besondere Bedeutung zu.

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[1] 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 zur digitalen Souveränität sowie Informations- und Cybersicherheit alleine lösen kann, sondern es hier der arbeitsteiligen Kooperation bedarf. Analog dazu werden Technologien und Fähigkeiten mit Abhängigkeit zu internationalen Standards und dem IT-Massenmarkt nur bedingt national sinnvoll besetzt werden können, so dass hier interdisziplinäre und internationale Zusammenarbeit notwendig sein wird.

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

[1] 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 6.2 1)

Diese Technologien und Fähigkeiten können im Rahmen des nachfolgend dargestellten Ablaufes zum Entstehungsgang von IT-Systemen entsprechend verortet werden.

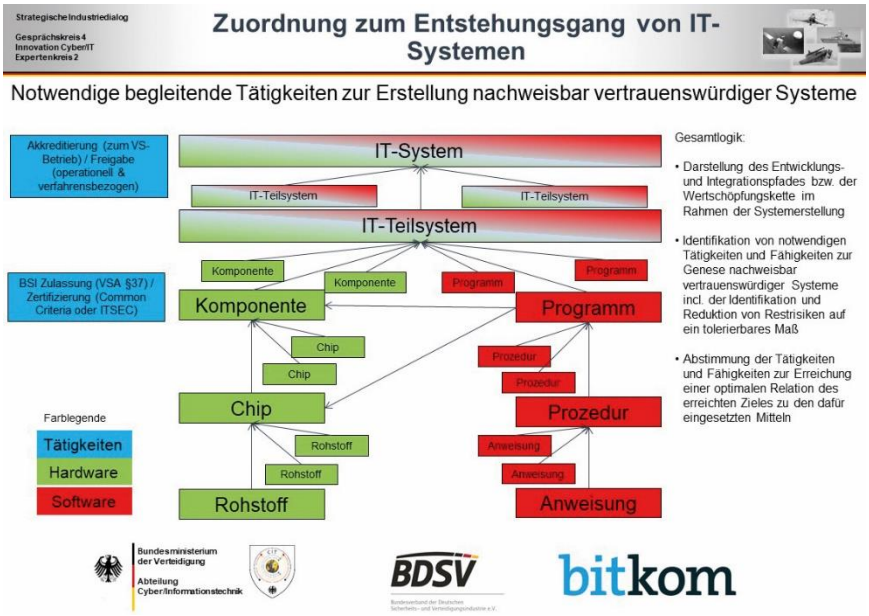


Abbildung 1: Zuordnung zum Entstehungsgang von IT-Systemen

Eine Betrachtungsweise kann auch hinsichtlich funktionaler Cluster erfolgen, wie in der nachfolgenden Darstellung verdeutlicht.

Der Expertenkreis 2 beleuchtet beide einander ergänzende Sichtweisen, um eine vollständige Gesamtschau zu erhalten und durch dessen Bewertung eine Ableitung von Maßnahmen bzw. Handlungsempfehlungen zu ermöglichen.

Abbildung 2: Betrachtung Funktionale Cluster

3 Ergebnisse im Überblick

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

Gemäß der ersten Sitzung des Gesprächskreises 4 Innovation Cyber/IT vom 4. September 2017 besteht im Rahmen der Diskussion um die digitale Souveränität das Selbstverständnis, dass hinsichtlich Software national grundsätzlich ausreichende Fähigkeiten vorhanden sind und dieser Teilbereich entsprechend beherrschbar erscheint. Im Bereich der Hardware besteht die Wahrnehmung, dass nationale Kapazitäten zwar zurückgefahren sind, jedoch nationales Know-how grundsätzlich vorhanden ist.

Das Vorhandensein sowie der Auf- und Abbau von Kompetenzen und Know-how und den notwendigen konzeptionellen und praktischen Fähigkeiten im Bereich der IT folgt wesentlich der Beschaffenheit des Marktes. Dies gilt ebenso für die Kompetenzen bzgl. IT-Sicherheit und IT-Sicherheitstechnologien. Da sich die Anforderungen für IT des Massenmarktes und des Bereiches staatlich zu schützender Verschlusssachen sowie kritischer Infrastrukturen und missionskritischer Anwendungen erheblich hinsichtlich der regulatorischen Vorgaben, dem z.Zt. adressierbaren Volumen der nationalen wie europäischen regulierten Märkte wie auch der Einsatzumgebung, dem Lebenszyklus und den Auswirkungen im Fall von Fehlfunktion unterscheiden, reagiert der Markt entsprechend darauf.

In der Folge werden die IT-Produkte regelmäßig aufgrund wirtschaftlicher Erwägungen, der Nutzerfreundlichkeit oder Praktikabilität entsprechend für Marktsegmente geeigneten Zuschnittes (Massenmarkt, behördliche Kunden, ...) optimiert, wobei in einem gegebenen IT-Produkt genau die je Marktsegment benötigen Anforderungen abgebildet werden. Regularien und Standards, und damit die Sicherheit, werden zwar als Anforderung verstanden aber i.d.R. abhängig von der Ausrichtung auf Marktsegmente nur im aus Sicht Haftung und Regulierung in einem notwenigen Mindestmaß berücksichtigt.

Daraus entsteht ein entsprechendes Spannungsfeld, wobei die Spannung mit dem Schutzbedarf der Informationen und der Kritikalität und Besonderheit des Einsatzzweckes steigt. Vor diesem Hintergrund müssen vorhandene Kompetenzen bestmöglich zur Schaffung und Aufrechterhaltung hinreichend verlässlicher Kommunikations- und Informationssysteme genutzt werden.

Ferner gilt es, die zukünftig benötigten Kompetenzen zur Entwicklung, Herstellung und Anwendung verlässlicher Kommunikations- und Informationssysteme ausgehend von z.Zt. vorhandenen Kompetenzen nachhaltig zu entwickeln. Vor dem Hintergrund auch längerfristig begrenzter Verfügbarkeit von Ressourcen (national sowie international), den zunehmenden Auswirkungen digitaler Konvergenz und Abhängigkeiten von globalen Marktmechanismen müssen hier hinsichtlich der Fähigkeit zur Bereitstellung von Schlüsselfunktionalität inkl. der dazu notwendigen Liefer- und Wertschöpfungsketten die Schwerpunkte mit Bedacht gewählt und im Vorgehen Prioritäten gesetzt werden. Sowohl die Fokussierung auf Schwerpunkte als auch die Priorisierung soll grundsätzliche und regelmäßig zu aktualisierende Risikobetrachtungen berücksichtigen, um aktuelle und zukünftige Risiken angemessen adressieren zu können. Hierzu bedarf es gemeinsamer Methoden und Sichtweisen.

Auch deutsche Hersteller müssen ihre Lösungen und Produkte auf dem internationalen Markt verkaufen, um die notwendigen Investitionen zu finanzieren. D.h. eine Konzentration nur auf den nationalen Markt, insbesondere den regulierten nationalen behördlichen Bedarf alleine ist aus Sicht der Anbieter nicht zielführend, da dies nicht genug Marktvolumen für entsprechende Investitionen bietet und die Zukunftsfähigkeit und Sicherheit von Produkten und Lösungen als auch die Innovationskraft sowohl in kommerzieller als auch technologischer Hinsicht gefährdet.

Die Ergebnisse der Arbeiten des Expertenkreises 2 spiegeln die teils komplementären Fähigkeiten und Schwerpunkte wieder, die sich durch die Rolle als Auftraggeber/Forderer bzw. Auftragnehmer/Bereitsteller techn. Lösungen zwangsläufig herausbilden. Diesbezüglich ist besonders das Kapitel 4.2 entsprechend zu würdigen. Vor diesem Hintergrund kommt der EK2 zu folgenden Ergebnissen:

- Die zu Beginn des neugestarteten Industriedialoges formulierte Selbsteinschätzung wird bestätigt, dass hinsichtlich SW grundsätzlich ausreichende Fähigkeiten national vorhanden sind und in HW zwar nationales Know-How vorhanden ist, die Kapazitäten aber zurückgefahren sind.

- Die die wesentlichen nationalen Sicherheitsinteressen betreffenden Anteile von Cyber/IT sollten im Rahmen der nationalen Schlüsseltechnologien angemessen Berücksichtigung finden.

- Der Begriff der Schlüsselfähigkeiten[2] sollte zusätzlich eingeführt, übergreifend abgestimmt und definiert sowie detailliert werden.

[2] Definition Schlüsselfähigkeiten: 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. (Arbeitshypothese bis zur Bereitstellung einer umfänglichen und formal abgestimmten Definition (siehe5.3 (2))

- Die Anwendungsfälle vertrauenswürdiger IT, die derzeit noch nicht hinreichend verlässlich regulatorisch abgebildet sind, sollten zur Handlungssicherheit diesbezüglich präzisiert werden.

- Die in den Detailbetrachtungen identifizierten spezifischen Handlungsfelder (z.B. sichere Lieferketten) sollten weiter betrachtet werden. Hierzu sind geplante sowie bereits laufende Forschungs- und Entwicklungsvorhaben im nationalen und internationalen Bereich mit einzubeziehen.

Die Darlegung der gesamten Lieferkette ist wünschenswert, aber „nachträglich“ bis zu den einzelnen elektronischen Bausteinen ggf. unrealistisch bzw. ggf. auch unwirtschaftlich. Hier helfen Prüfungen akkreditierter Prüfstellen, die Tests und Prüfung im Rahmen von Zertifizierungen und Zulassungen durchführen. Bei Liefereinheiten ist generell nicht nur darauf zu prüfen, ob sie die gewünschten Funktionen erfüllen, sondern auch darauf, ob sie weitere ggf. unerwünschte oder sogar schädliche Funktionen erfüllen (können). Eine ernsthafte Durchführung solcher Prüfungen setzt allerdings voraus, dass der Prüfer über hinreichende Produktinformationen bis hin zum Quellcode verfügt, was in der Regel nur bei nationalen Herstellern gefordert und durchgesetzt werden kann. In der Praxis werden derartige Prüfungen derzeit nur für sehr spezifische Produkte ermöglicht, die in sicherheitskritischen Bereichen verwendet werden. Zu beachten ist hier auch das gesamte Konfigurationsmanagement solcher Produkte und die Notwendigkeit erneuter Prüfungen nach Updates oder Konfigurationsänderungen.

Bei der Absicherung der Lieferkette wäre 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.

4 Detailbetrachtungen

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.

4.1 Gefährdungen für vertrauenswürdige IT

Zur Einführung in den Themenkomplex ist im Rahmen dieses Ideenpapieres als gemeinsame Basis eine Betrachtung der Gefährdungen zweckmäßig. Relevante Beispiele für Gefährdungen der Vertrauenswürdigkeit von IT in Hardware und Software sowie im Zwischenbereich haben erhebliche Auswirkungen im Bereich der Informationssicherheit und in der Vergangenheit nach Bekanntwerden auch stets entsprechende mediale Außenwirkung.

4.1.1 Hardware am Beispiel von MELTDOWN und SPECTRE

Beitrag Industrieverbände (BDSV und Bitkom)

Wie durch die Sicherheitslücken MELTDOWN und SPECTRE aufgedeckt, stellt kommerzielle, hoch komplexe Hardware eine generelle Herausforderung dar. Diese Funktionalität greift schon im architekturellen Design von Prozessoren inkl. systemnaher Software auf Komponenten zurück, deren Design weder transparent validiert noch einsehbar ist. Im Fall von Schwachstellen auf tiefen Systemebenen der Prozessoren ist die Erkennung komplex und aufwendig, das „Auffüllen“ derartiger Lücken mit Hilfe von Softwareaktualisierungen nur bedingt möglich. Das Beheben von Lücken oder Fehlern in Hardware durch Software ist zwar grundsätzlich möglich, aber sehr aufwändig und komplex.

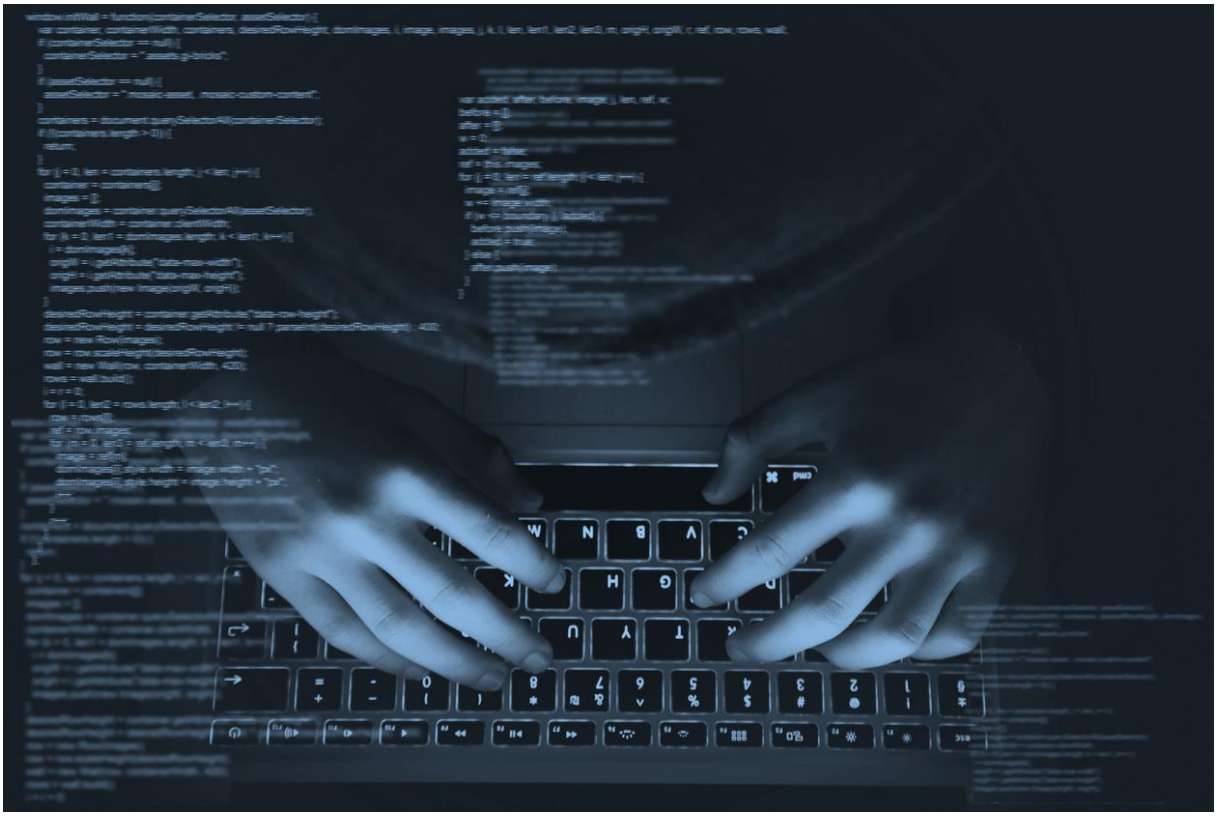
Eine weitere Herausforderung stellen Hardware-Trojaner für Chipbausteine dar, welche primär während der Design oder Produktionsphase „eingespielt“ werden. Untersuchungen der letzten Jahre haben gezeigt, dass es hierfür zahlreiche Angriffsvarianten gibt, von Hardware-Backdoors über Störregister bis hin zu Spezialdotierungen zur Manipulation beispielsweise von Zufallsgeneratoren. Eine zentrale Herausforderung hierbei stellt die extrem schwierige Detektierbarkeit derartiger Angriffsmöglichkeiten oder gar operativer Angriffe dar. Dies führt - neben anderen Schwachstellen - in der Praxis u.a. zur erhöhten Verwundbarkeit und immer mehr konkreten Angriffsvektoren bei komplexen vernetzten Systemen in der phys. Welt wie z.B. von Automobilen und Schiffen.

Die Anforderungen und der Bedarf an sicheren Vertrauensankern als Teil des Hardware- und Systemdesign wird kontinuierlich steigen (Security by design), analog dazu auch die Risiken für die Sicherheit der Systeme sofern keine grundsätzlichen Verbesserungen im Design herbeigeführt werden. Entsprechend ist zukünftig von Wachstum des Bedarfs an vertrauenswürdigen Elementen (z.B. Vertrauensanker) als elementarer Bestandteil der Architektur auszugehen (siehe 6.2.2).

4.1.2 Software am Beispiel des Heartbleed-Bug

Beitrag BMVg (BMVg CIT II 2)

Die Herausforderungen bei der Software werden nachfolgend am Beispiel des Heartbleed-Bug verdeutlicht. Der „Heartbleed-Bug“ ist eine Sicherheitslücke in dem „Heartbeat“-Programmodul von OpenSSL. Bei OpenSSL handelt es sich um eine freie Software-Bibliothek für Transport Layer Security (TLS), welche Implementierungen verschiedener Verschlüsselungen umfasst. Web- und Mail-Server und auch andere Dienste wie Virtual Private Networks (VPN) oder Router nutzen häufig diese Bibliothek für TLS/SSL-Verbindungen. OpenSSL enthält in den Versionen 1.0.1 bis 1.0.1f eine Schwachstelle, den „Heartbleed-Bug“. Bei Ausnutzung der Schwachstelle ist ein Angreifer in der Lage, Speicherinhalte des OpenSSL Servers auszulesen, sofern diese die „Heartbeat“-Erweiterung aktiviert haben. Unter Umständen können dabei die geheimen Schlüssel von OpenSSL-Servern ausgelesen werden (siehe 6.2 3). Mit OpenSSL Version 1.0.1g steht ein entsprechendes Update zur Verfügung.



Falls jedoch vorher eine verwundbare OpenSSL-Version mit aktivierter Heartbeat-Erweiterung eingesetzt worden ist, kann eine in der Vergangenheit liegende Kompromittierung von kryptografischen Schlüsseln nicht ausgeschlossen werden. Daher wurde neben dem notwendigen SW-Upgrade empfohlen, die verwendeten Server- und Client-Zertifikate auszutauschen, die alten Zertifikate zu sperren und sämtliche Passwörter der betroffenen Systeme zu ändern (siehe 6.2 4).

4.1.3 Hardwarenahe Software/Firmware am Beispiel Exploit BadUSB

Beitrag Industrieverbände (BDSV und Bitkom)

Am Beispiel des Exploit BadUSB wird die Problematik der Angriffe über Hard- und Firmware dargestellt und auf das besondere Problem der präventiv nicht prüfbaren Qualität eingegangen. Wie in vielen Gebieten der ITK wurde auch im Umfeld der USB Peripheriegeräte zuerst die Funktionalität implementiert und auf Funktionen der IT-Sicherheit weitgehend verzichtet.

Viele der Sicherheitsprobleme lagen (und liegen noch) an der Einbettung in die Betriebssysteme. Der hier behandelte Exploit nutzt aber die zunehmende „Intelligenz“ auch einfacher USB-Geräte wie etwa Memory Sticks. USB Geräte werden bei der Nutzung nicht authentisiert, sondern im besten Fall identifiziert, obwohl die Möglichkeiten einer starken Authentisierung im Prinzip gegeben wären. Noch nicht einmal beim Verändern des Controllers (Patchen) auf dem USB-Stick benötigt man eine Authentisierung.

Hauptgründe für diesen Sachverhalt sind Kosten und „Commodity“. Wenn der Hersteller weitere Hürden für ein Update einbauen würde, dann würde das Update zum einen technisch kompliziert werden und zum anderen müssten neue Sicherheitsfunktionen implementiert werden. Beides sind Kostentreiber.

Zweifelsohne ist es eine gute Abhilfe, wenn – wie das heute bereits der Fall ist – Securitydevices samt deren Controller gegenseitig stark authentisiert werden. Das geht aktuell aber nur mit einigen extra dafür ausgelegten Devices unter Nutzung von guten Device Control Produkten.

Am wichtigsten wäre es, eine Infrastruktur zur Authentisierung der Devices auch vor einer Re-Programmierung aufzubauen, die in der Hardware der Devices verankert ist. Standardisierung, Aufbau und Verbreitung der Infrastruktur benötigen aber viel Zeit, so dass das keine zeitnahe Hilfe bietet.

Wesentliche Teile des Exploits können durch eine professionelle Device (Schnittstellen)-Kontrolle in Zusammenarbeit mit einer Applikationskontrolle verhindert werden, wenn diese auch Contents für Applikationen einschränkt. Eine professionelle Applikationskontrolle prüft jeden gestarteten Prozess (und nicht nur jede gestartete Anwendung) und verfolgt zurück, wo der Ausgangspunkt für den Prozessstart ist.

Werden keine Prozesse akzeptiert, deren Ursprung auf einem Peripheriegerät liegt oder deren Ursprung nicht systemtechnisch sicher zu einer positiv freigegebenen Quelle nachvollzogen werden kann, können die Auswirkungen des Schadcodes im Wesentlichen verhindert werden (siehe 6.2.5).

4.2 Randbedingungen der im GB BMVg und im kommerziellen Massenmarkt eingesetzten IT-Produkte

Beitrag BMVg (BMVg CIT II 2)

Zur Einführung in den Themenkomplex im Rahmen dieses Whitepapers ist es ebenfalls notwendig, die Rahmenbedingungen der im GB BMVg und dem kommerziellen Massenmarkt eingesetzten IT-Produkte beispielhaft dazulegen.

Umweltanforderungen:
Die Anforderungen an thermische und mechanische Belastungsfähigkeit, sowie Verträglichkeit gegenüber Feuchtigkeit sind bei IT-Produkten des Massenmarktes und der Endanwender in der Regel sehr begrenzt. In Einzelfällen werden Produkte angeboten, die nach den Normen IEC 60529 bzw. DIN EN 60529 definierte Schutzgrade (siehe 6.2.26)) erfüllen und über die vorgenannten Anforderungen bereits im Sinne einer erweiterten Alltagstauglichkeit hinaus gehen (z.B. wasserdichte und stoßfeste Smartphones Schutzart IP67, siehe 6.2.7 und 8).

Im militärischen Bereich richten sich die Anforderungen entsprechend nach dem Military Standard 810 „DEPARTMENT OF DEFENSE – TEST METHOD STANDARD – ENVIRONMENTAL ENGINEERING CONSIDERATIONS AND LABORATORY TESTS“, der aktuell in der Version MIL-STD-810G vom 31. Oktober 2008 öffentlich verfügbar ist (siehe 6.2.9). Hier werden alle relevanten Umweltanforderungen systematisch dokumentiert und abgebildet.

Elektromagnetische Abstrahlung:
IT-Produkte des Massenmarktes und für Endanwender erfüllen hinsichtlich der elektromagnetischen Verträglichkeit regelmäßig die Anforderung in einem gegebenen elektromagnetischen Umfeld funktionieren zu können und dieses Umfeld, zu der auch andere Geräte gehören, im Sinne einer umfassenden Funktionsfähigkeit nicht unzulässig nachteilig zu beeinflussen.

Bei IT-Produkten zur Verwendung für die Verarbeitung von staatlich zu schützenden Verschlusssachen müssen hingegen viel weitergehende Anforderungen berücksichtigt werden. So z.B. auch, dass die elektromagnetische Abstrahlung in Qualität und Quantität auf ein solches Maß reduziert wird, dass abgesehen von einer Störung der Umwelt auch eine unbefugte Kenntnisnahme von Informationen (Abstrahlsicherheit/TEMPEST) durch ungewollte elektromagnetische Abstrahlung hinreichend sicher ausgeschlossen werden kann.

Zulassungspflichtigkeit von Produkten mit IT-Sicherheitsfunktionen:
Produkte mit IT-Sicherheitsfunktionen (z.B. Erzeugung kryptografischer Schlüssel, kryptografische Verfahren, Trennung unterschiedlich schutzwürdiger Netzwerke) für den Massenmarkt folgen i.d.R. Best-Practice Lösungen bzw. solchen die sich schlicht als de-facto-Standard etabliert haben.

Produkte mit IT-Sicherheitsfunktionen zur Verwendung für staatlich zu schützende Verschlusssachen müssen sich zwingend nach den Bestimmungen des §4 des Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz – SÜG) bzw. der gem. §35 SÜG im jeweiligen Geltungsbereich erlassenen allgemeinen Verwaltungsvorschriften richten. Für das BMVg war und ist dabei insbesondere der §37 der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) vom 31. März

2006 in der Fassung vom 26. April 2010 (GMBl 2010, S. 846, siehe 6.2.11) maßgeblich, die vorgibt, welche Produkte mit IT-Sicherheitsfunktionen zur Verwendung für VS zugelassen sein müssen.

Dieses - mit dem Schutzbedarf der Informationen und der Kritikalität des Einsatzzweckes steigende – beispielhaft motivierte Spannungsfeld zwischen dem im GB BMVg benötigten und dem im kommerziellen Massenmarkt nachgefragten IT-Produkten ist in beigefügter Abbildung dargestellt. Dies ist unter dem Aspekt des bestmöglichen Einsatzes vorhandener Kompetenzen und Ressourcen zur Schaffung und Aufrechterhaltung hinreichend verlässlicher Kommunikations- und Informationssysteme nachfolgend pro Handlungsfeld im Detail zu betrachten.

Abbildung 3: Randbedingungen von IT-Produkten

4.3 Detailbetrachtung pro Handlungsfeld

4.3.1 Embedded IT

Beitrag Industrieverbände (BDSV und Bitkom)

Da insbesondere Embedded-IT oft in starker Verbindung mit sicherheitskritischer Funktionalität eingesetzt wird (z.B. Produktionsprozesse, Logik bei Steuerungsanlagen, Kontrollfunktionen), existiert bei einem erfolgreichen Angriff ein sehr hohes Schadenspotenzial.

Staatliche als auch nicht-staatliche Akteure im Cyberumfeld verfügen über ein breites Spektrum an Optionen, um Embedded IT-Systeme (z.B. Sensoren oder Steuerungssysteme) anzugreifen. Betrachtet man die Angriffsvektoren für Embedded IT im Allgemeinen, lässt sich erkennen, dass neben den Angriffen auf die Applikationssoftware auch die Betriebssysteme, Firmware, Hardware auch zur Nutzung essentielle Kommunikationsnetzwerke und die Lieferketten ein lohnendes Ziel darstellen. Bei Verfügbarkeit nahezu unbegrenzter Ressourcen kann hierbei zur Vorbereitung eines Angriffes eine Komponente analysiert und re-engineered werden, was zu ausgeklügelten Angriffen führen kann (siehe 6.2.6).

Insbesondere durch den Eingriff in die Lieferketten können feindliche Angreifer „exotische“ Zero-Day Angriffe aufbauen, die jahrelang unentdeckt bleiben. Sie können dabei selbst Security Software gezielt angreifen und über Angriffe auf Hardware und Betriebssysteme tiefere Systemschichten angehen, in denen Angriffe nicht mehr detektierbar sind und von wo aus alle folgenden Sicherheitsprozesse unterwandert werden können.

Als mögliche „Auslöser“ für die „Aktivierung“ sind beispielsweise externe Signale (z.B. spezifische IFF Daten, eingespeiste Informationen via Datenlinks, GPS Daten) denkbar. Wenn diese Signaleinspeisung während eines Einsatzes erfolgt, kann dies katastrophale Folgen für die Operation nach sich ziehen.

Die Herausforderung bei der Absicherung eines Waffensystems besteht darin, dass unter diesen Voraussetzungen als hochsicher betrachtete IT-Netzwerke und OT-Netzwerke bzw. –Komponenten, die in der Vergangenheit überwiegend als nicht vernetzt betrachtet wurden, nun immer mehr vernetzt sind bzw. werden. Unter OT (=Operational Technology) werden hier spezifische IT-Komponenten subsummiert die primär dem Zweck der Steuerung von technischen Verfahren (z.B. Produktionsanlagen) sowie Mess- und Regeltechnik dienen. OT-Komponenten umfassen ebenfalls industrielle Kontroll-Systeme (Industrial Control Systems, ICS). Diese bestehen primär aus gehärteten Commercial-Off-The-Shelf-Systemen und OT-Komponenten unterliegen i.d.R. einem anderen Lebenszyklus (z.B. geringere Frequenz an Aktualisierung). Es ist davon auszugehen, dass hier trotz Härtung und Absicherung nach Stand der Technik zum Zeitpunkt der Realisierung ohne regelmäßige Aktualisierung und weitergehende Optimierung der Absicherung auf Komponentenebene (z.B. in schon in frühere Phase des Entwicklungszyklus) keine nachhaltige Sicherheit gegen die Ausnutzung z.B. z.Zt. noch nicht bekannter Sicherheitslücken in COTS Produkten durch mehrstufige Angriffe erreicht werden kann. Insbesondere sind Commercial-Off-The-Shelf-Systeme in der Breite zugänglich und erlauben dem Angreifer somit, sich schon in der Frühphase der langjährigen Entwicklungszyklen der Waffensysteme darauf vorzubereiten. Die Kombination möglicher Infiltrationen in die Lieferkette mit dem Wissen über verwendete Commercial-Off-The-Shelf-Systeme kann die Basis für erfolgreiche Angriffe darstellen, die für die betroffenen Systeme fatal sein können. Angreifer können dabei multiple Instanzen und Zugänge in verschiedenen Bereichen des Systems anlegen, sowie die volle Kontrolle übernehmen und aufrechterhalten.

Die Angreifer sind so in der Lage, Steuer- und Ergebnisdaten „mitzulesen“ und nach Belieben zu verändern. Dabei können Waffenplattformen, Command & Control-Strukturen und Aufklärungstechnologien angegriffen, gestört, sabotiert und – besonders gravierend – hochgranular auf eine Art und Weise manipuliert werden, die erst erkannt werden kann, wenn es zu spät für Gegenmaßnahmen ist.

Angreifer können dabei

- hochautomatisierte „Fire-And-Forget“ Angriffe platzieren und unter bestimmten Trigger-Bedingungen auslösen, oder
- konstant Erosionen in Technologien herstellen, oder
- flexible Zugänge etablieren und bei Verfügbarkeit eines Rückfluss-Kanals, etwa über ein erfolgreich angegriffenes taktisches Ziel, weiter agieren.

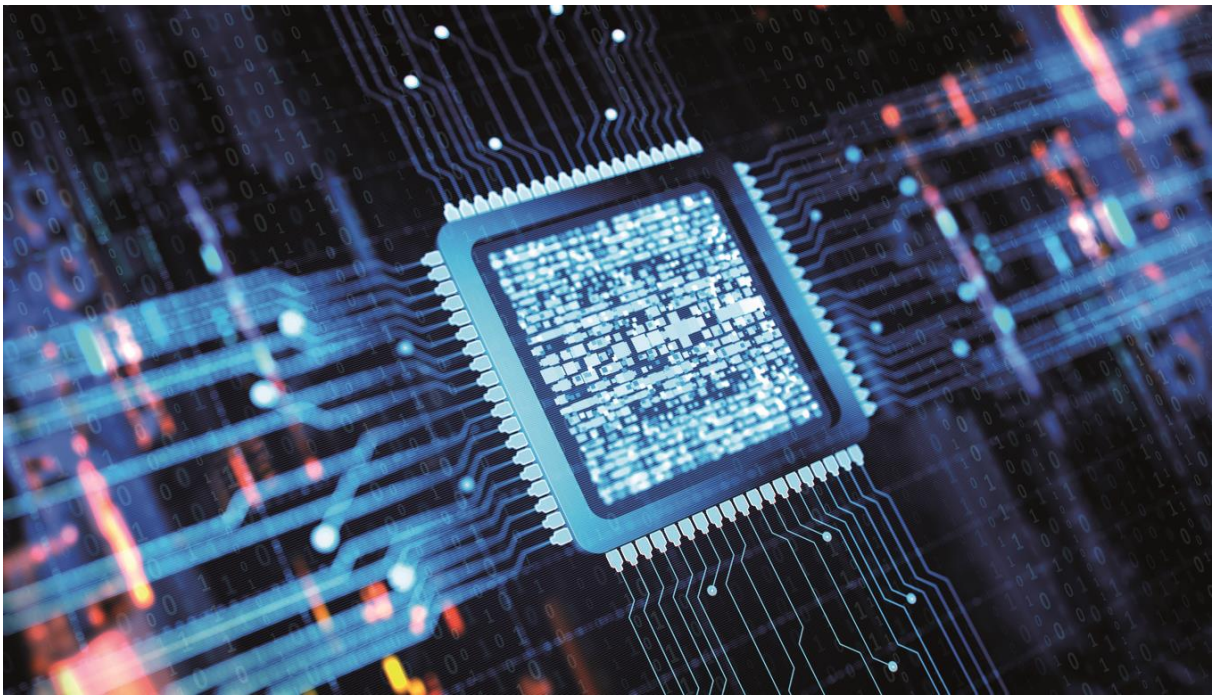
Gute Angreifer werden in der Regel mehrfache Optionen verschiedener Varianten in Kombinationen anbringen. Zahlreiche bekannt gewordene IT-basierte Angriffe mit hochentwickelter Malware unter Ausnutzung von Schwachstellen zeigen die faktische Existenz solcher Fähigkeiten, deren praktische Anwendung und die Konsequenzen.

Bei Nachrichtendiensten und Militärs sind üblicherweise hinreichende Interessen und Fähigkeiten vorhanden, respektive werden aufgebaut, um mehrfach in hohem Maße effektive, nicht detektierbare „elegante“ Angriffe zu platzieren. Auch kleinere, hochgesicherte Systeme bieten in diesem Umfeld bislang nach aktuellem Stand der Erkenntnisse vorauss. keine ausreichend bzw. dauerhaft widerstandsfähige Sicherheit. Führende Konzepte wie z.B. TrustZones oder marktgängige Realisierungen von Security Chips weisen immer noch regelmäßig Sicherheitslücken auf (siehe 6.2.12).

4.3.2 *IT-Komponenten Land-, Luft- und Seefahrzeuge*

Beitrag Industrieverbände (BDSV und Bitkom)

Mikroelektronische Komponenten stellen die wesentliche physikalische Ebene dar, auf der Angriffe aus Sicht der Informationssicherheit ausgetragen werden können. Dies sind Elektronikkomponenten wie integrierte Schaltkreise („Chips“) und die daraus erstellten elektronischen Baugruppen (Printed Circuit Board Assembly PCBA). Dabei stellen die o.g. (Halbleiter-)Schaltkreise die größte Schwachstelle dar; insbesondere, wenn Schaltkreise manipuliert werden, was u. a. auf dem Beschaffungsweg möglich ist und somit zur Thematik der gefälschten Komponenten führt.



Die bereits weit reichende Verbreitung von gefälschten Schaltkreisen ist allerdings primär durch wirtschaftliche Interessen motiviert (siehe 6.2.24). So wird das Ziel verfolgt, für ein Produkt geringer Qualität den Preis eines hochwertigen Produktes zu erlangen. Im weiteren Sinne mindert allerdings auch das Auftreten eines solchen Plagiates die Vertrauenswürdigkeit eines IT-Produktes und adressiert (ggf. unbewusst) die gleichen Angriffsziele wie ein Teil der Cyberangriffe. Dies gilt beispielsweise für eine beabsichtigte Performance-Minderung. Die Anwenderseite hat zwar eine hohe Kompetenz zur Vermeidung der Plagiate entwickelt, es lässt sich jedoch nicht mit Sicherheit behaupten, dass diese Kompetenz auch für Angriffe auf die Lieferkette aus dem Blickwinkel der IT Kriminalität wirksam ist. Hier könnte eine andere Angriffsenergie zu Grunde liegen, die nicht durch die erzielbaren wirtschaftlichen Erträge aus dem unmittelbaren Fälschungsgeschäft limitiert ist.

Militärische Technik fordert oft eine sehr lange Verfügbarkeit und Nutzbarkeit der elektronischen Komponenten. Wegen der demgegenüber immer kürzeren Verfügbarkeit von elektronischen Schaltkreisen kommt es hier nicht selten zu einer Beschaffungsnot, die wiederum die Attraktivität für Plagiarismus steigert. Ohne entsprechende Regenerationsstrategien und Wartungskonzepte hat die im Einsatz befindliche Technologie häufig ein hohes Alter und entspricht weiterhin nicht mehr dem Stand der Technik bzgl. IT-Sicherheit.

Schaltkreise werden immer komplexer, im Wesentlichen getrieben von steigenden Performanz-Anforderungen. Dies erhöht zum einen die Wahrscheinlichkeit von Schwachstellen. Die Hersteller begegnen dieser Schwierigkeit beispielsweise durch immer weiter intensivierten Testaufwand, damit

lässt sich jedoch keine absolute Sicherheit erreichen. Wegen der Komplexität der Schaltkreise werden zum anderen oftmals PCBA Designs (Referenzdesign) von den Herstellern der Schaltkreise vorgeschlagen. Die Industrie gelangt so zu einer signifikanten Zeitersparnis in der Entwicklung, indem diese Designs lediglich kopiert oder nur geringfügig angepasst werden müssen. Dies führt jedoch auf sehr weit verbreitete, gleichartige Designs über Branchengrenzen hinweg: „Monokultur des Entwurfes“. Wenn man vorgegebene Entwicklungszeiten und Kosten einhalten will, wird man zweckmäßigerweise auch für militärische Anwendungen von diesen Referenzdesigns Gebrauch machen. Somit nutzt man für kommerzielle und militärische Lösungen identische Designs. Angreifer, die mit hoher Energie einen Angriff auf ein weit verbreitetes, kommerzielles System vornehmen, entwickeln im gleichen Atemzug ein identisches Risikopotenzial für das analog gestaltete militärische System.

System on a Chip Lösungen vereinen möglichst alle für ein Elektronikprodukt benötigte Funktionen auf einem Chip. Sie haben sich wegen ihrer Vorteile etwa bei Energieverbrauch, Baugröße und Preis weit verbreitet und werden in sehr hoher Stückzahl verwendet. Wie auch schon im Falle der Referenzdesigns führt dies ebenso auf eine Gleichartigkeit der Designs (Monokultur), mit den gleichen, voranstehend genannten Implikationen. Die Problematik setzt sich auch in die Softwareebene fort.

Es stellt sich die Frage, ob bzgl. der Anwendungen für Land, Luft und See, und Raumfahrttechnik unterschiedliche Betrachtungen erforderlich sind. In der Tat gibt es einige aus den Anwendungsgebieten abgeleitete Anforderungen, die auf die IT-Sicherheit der jeweiligen Systeme mittelbar Einfluss haben können. Ergänzend zu den in Kapitel 4.2, sind dazu folgende zu nennen:

- Baugröße: Land und Luft- und Raumfahrtanwendungen fordern oftmals einen sehr geringen Bauraum (Miniaturisierung). In der Folge muss ggf. von den Referenzdesigns abgewichen werden. Durch Individualisierung des Entwurfs auf PCBA Ebene können die voranstehend beschriebenen Phänomene der Monokultur im Entwurf abgemildert werden.
- Die normativen Vorgaben für Entwicklungen im Luftfahrtbereich beinhalten sehr oft hohe Forderungen bzgl. der Nachverfolgbarkeit/Zertifizierung innerhalb der Lieferkette. Was die Wahrscheinlichkeit für Plagiate reduziert.

4.3.3 IT-Bausteine und -Funktionen in IT-Sicherheitsprodukten inkl. HW für das mil. Umfeld – Fokus sichere Netzwerkschnittstelle

Beitrag Industrieverbände (BDSV und Bitkom)

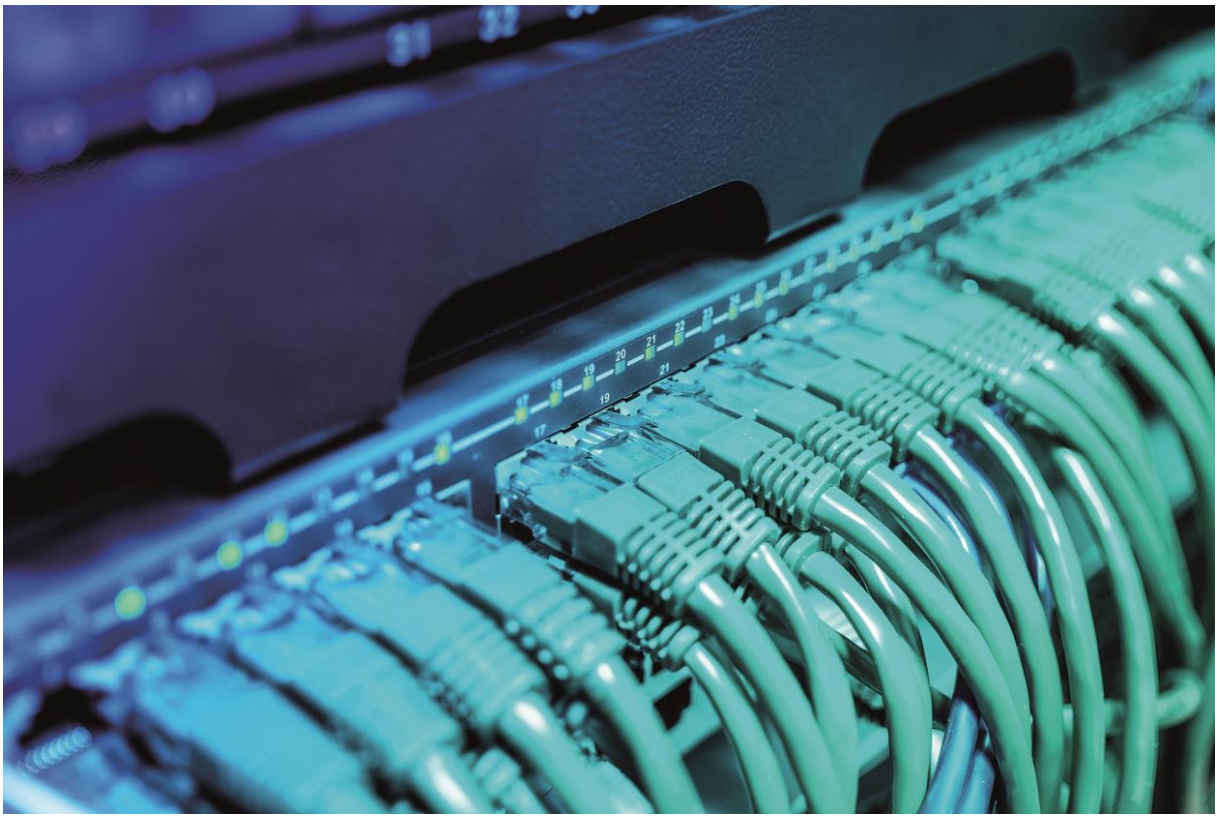
Netzwerkschnittstellen sind eine von mehreren wichtigen Kategorien kommunikations- bzw. I/O-relevanter – sowohl drahtgebundener als auch funkbasierter – Schnittstellen in Hardwareplattformen. Die Netzwerkadapter bilden in nahezu allen IT-Systemen die elementare, physische Schnittstelle zu anderen IT-Systemen. Sie ermöglichen es Computern und Systemen, sich dauerhaft mit einem Netzwerk zu verbinden, um einen Datenaustausch mit anderen Systemen herzustellen. Das Problem: Moderne kommerziell erhältliche Netzwerkkarten sind auf hohen Datendurchsatz optimiert und nicht auf Informationssicherheit. Die Firmware eines Netzwerkadapters kann z.B. so verändert werden, dass sie den Hauptspeicher eines Servers ausliest und z.B. an erreichbare Empfänger verschickt. Auch das vom Endanwender oder Administrator unbemerkte Einschalten eines heruntergefahrenen IT-Systems, die Annahme von interaktiven Kommandos sowie das Injizieren von Schadcode ist – ggf. unter Umgehung der Schutzmechanismen eines Betriebssystems – möglich. Netzwerkadapter stellen somit ein potentiell ungesichertes Einfallstor in das eigentliche IT-System dar. Hierdurch entsteht ein Risiko der Kompromittierung des Gesamtsystems.

Lösen lässt sich auch diese Herausforderung mit „Security by Design“. Ein sicherer Netzwerkadapter muss sich in seiner Funktionalität auf die Kernaufgaben der Netzwerkanbindung konzentrieren. Gegebenenfalls vorhandene Firmware darf nicht manipulierbar sein. Änderungen der Konfiguration dürfen nur von autorisierter Stelle erfolgen und müssen nachvollziehbar bzw. auditierbar sein. Die Funktionalität wird in manipulationsgeschützter Hardware umgesetzt. Dadurch werden externe und interne Angriffsvektoren drastisch reduziert. Um das notwendige Sicherheitsniveau zu erreichen, wird ein solcher sicherer Netzwerkadapter konsequent auf den nötigsten Funktionsumfang in Hardware, Software (inkl. Treiber im Betriebssystem etc.) und Configware beschränkt.

Sichere Netzwerkadapter sind seit 2010 _ zunächst fokussiert auf die Absicherung schwarzer Netzwerkschnittstellen _ Bestandteil FPGA-basierter SINA CORE-Kryptomodule in DEU GEHEIM, NATO SECRET und teilweise auch SECRET UE/EU SECRET zugelassenen SINA H Produkten. Seit 2016 werden in aktuellen Varianten dieser Kryptomodule darüber hinaus auch rote Netzwerkschnittstellen abgesichert. Im gleichen Jahr veröffentlichte das BSI die Version 1.0 eines „VS-Anforderungsprofils für eine Sichere Netzwerkkarte“ (siehe 6.2.13). Vom Lösungsdesign her ist die Umsetzung der Anforderungen gem. VS-Anforderungsprofil des BSI in Form dedizierter HW-Netzwerkadapter möglich. Eine solche, die Anforderungen des BSI an DEU GEHEIM erfüllende, sichere Netzwerkkarte ist als Einzelprodukt zum Einsatz in z.B. Server-Systemen, Arbeitsplatz-PC und anderen PC-basierten Endgeräten seit 2018 ebenfalls verfügbar.

Darüber hinaus bestehen für die besondere Ausnutzung der Spezifik von Hardwareplattformen erfahrungsgemäß alternative verteilte systemintegrative Ansätze. D.h. neben der Nutzung spezieller gesicherter Hardwaremodule als Netzwerkadapter sind auch Ansätze mittels tiefgehender Virtualisierung und Kapselung durch vertrauenswürdige Software und mehrstufige Absicherung erfolgsversprechend.

Eine breitere Verfügbarmachung und Einsatz sicherer HW-Netzwerkadapter erfordert die Bewältigung anspruchsvoller Herausforderungen in einem hochgradig Performance- und Stabilitäts- und Interoperabilitäts-relevantem technischen Umfeld.



Exemplarisch werden dazu im Folgenden einige gerätetechnische systemintegrative Aspekte aufgeführt. Diese betreffen insbesondere die Unterstützung unterschiedlicher:

- stationärer und mobiler Gerätetypen (bspw. Clients, Gateways, Server, IT Sicherheitsprodukte),
- Bauformen (u.a. Desktops, Notebooks, Tablets, möglicherweise auch Smartphones, Blades),
- interner Interfaces zu Bussystemen,
- Medien (LWL in mannigfaltigen Ausprägungen, Kupfer; außerdem Funk, bspw. WLAN),
- Performance-Leistungsklassen,
- Robustheitsprofile und Temperaturbereiche,
- Dimensionierung beim Abstrahlschutz,
- Systemumgebungen (im Kontext von Treibersoftware).

Hinzu kommt, dass dedizierte Hochsicherheitsprodukte (HW, SW z.B. für Absicherungsniveau GEHEIM) hinsichtlich Entwicklung, Nutzung und Lebenszyklus ob der hohen Sicherheitsanforderungen deutlich anspruchsvoller sind als Standard-COTS.

Angesichts der bekannten Risiken und Verwundbarkeiten vorhandener COTS-Implementierungen (marktverfügbarer) Netzwerkadapter ist vor dem Hintergrund der zunehmenden dezentralen Vernetzung von COTS-Einzelkomponenten (z.B. IoT-Geräten) über unterschiedliche Medien wie WLAN, LAN und mobile Funknetze eine Steigerung der Widerstandsfähigkeit bzw. Resilienz der Netzwerkanbindung inkl. Manipulationsschutz insbesondere im Massenmarkt (COTS) für die Aufrechterhaltung von Betriebsstabilität und Funktionsfähigkeit anzustreben.

4.3.4 *IT-Bausteine und -Funktionen in IT-Sicherheitsprodukten inkl. HW für das mil. Umfeld* – Fokus Verschlüsselung

Beitrag Industrieverbände (BDSV und Bitkom)

Hoheitliche Verschlüsselung erfordert die Einhaltung strenger Anforderungen für Hardware, Software und die Gesamtarchitektur. Zugelassene Verschlüsselungslösungen verlangen in der Regel den Einbau von Hardware Security Module (HSM) oder Kryptomodule integriert in einer entsprechenden Architektur mit modularem Aufbau in Hardware und Software. Streitkräfte sowie Behörden und Organisationen aus dem Verteidigungs- und Sicherheitssektor sind heutzutage mehr denn je auf leistungsfähige moderne IT-Strukturen angewiesen, um ihre Verteidigungsfähigkeit auf den Cyber- und Informationsraum auszuweiten. Hinzu kommen steigende Anforderungen im Hinblick auf Mobilität, Flexibilität und Agilität, die an heutige und künftige Einsatzgruppen und deren multinationale Einsatznetze sowie darin integrierten Kryptoprodukten gestellt werden.

Aus den teils langen Nutzungszeiträumen von Kryptosystemen bzw. -komponenten im sicherheitssensitiven Umfeld leitet sich eine weitere Motivation für Agilität ab, insbesondere um im Lebenszyklus Algorithmen zu parametrisieren, optimieren und modernisieren zu können. Im Systemdesign moderner, national verfügbarer Produkte wird diesen Anforderungen in zunehmendem Maße entsprochen.

Die Sicherheit der Kryptoprodukte selbst wird dabei nicht wie in der Vergangenheit durch fest „verdrahtete“ Hardware (z.B. ASICs) realisiert, sondern weitestgehend in Form von Software und Firmware auf programmierbaren Prozessoren bzw. Schaltkreisen (FPGAs) implementiert. Es wird hier auch von Software definierter Krypto gesprochen. Insbesondere zulassungsrelevante Kryptosysteme bedingen zudem hochwertige, auf physikalischen Prinzipien aufsetzende Zufallszahlengeneratoren. In dieser Ausprägung sind die Verschlüsselungsprodukte erweiterbar und können sich unter Berücksichtigung neuer und künftiger Anforderungen (= Kryptoagilität) fortentwickeln, z.B.:

- Einbringung anderer und modifizierter Algorithmen (z.B. elliptische Kurven, Post Quantum Krypto und zusätzliche Schnittstellen)
- Performance-Optimierung.

Außerdem sollten zukünftig mehrere Kryptofunktionalitäten ladbar und abhängig vom jeweiligen aktuellen Anwendungskontext betreibbar sein (=Multi Kryptolösungen). Obiger Aufbau und Funktionalität sind Stand der Technik und von nationalen Anbietern verfügbar.

4.3.5 IT-Bausteine und -funktionen in IT-Sicherheitsprodukten inkl. HW für das mil. Umfeld – Fokus Security Gateways

Beitrag Industrieverbände (BDSV und Bitkom)

Security Gateways ermöglichen den sicheren bzw. kontrollierten Austausch zw. Sicherheitsdomänen mit gleichen oder unterschiedlichen maximal verarbeiteten Geheimhaltungsgraden. Ordnungsgemäß funktionierende Security Gateways ermöglichen einen Datenaustausch der erlaubten Informationen zwischen unterschiedlichen Sicherheitsdomänen. Sicherheits-Gateways ermöglichen somit die exakte Kontrolle und Steuerung des Datenflusses zwischen den unterschiedlichen Netzen. Je nach Einstufungsgrad der zu verbindenden Netze werden verschiedene Security Gateways eingesetzt. Bei der Kopplung von gleich eingestuften Netzen ist eine Netztrennung mit einer Firewall ausreichend. Liegt ein Sicherheitsgefälle zwischen den Netzwerken vor, so ist zwischen uni- oder bidirektionalem Datenaustausch zu unterscheiden. Hier kommen entweder Datendioden oder bidirektionale Sicherheitsgateways zum Einsatz:

- Wird lediglich eine unidirektionale Kommunikation von Daten aus einem niedrig klassifizierten Netz („LOW“, z. B. VS-NfD) in ein höher klassifiziertes Netz („HIGH“, z.B. GEHEIM) benötigt, so kommen Datendioden zum Einsatz. Aus Geheimschutzsicht ist die Übertragung von Daten LOW nach HIGH problemfrei, da alle in LOW existierenden Daten auch in HIGH verarbeitet werden dürfen. Es muss allerdings unbedingt mit der Datendiode sichergestellt werden, dass in der Gegenrichtung absolut keine Informationen übertragen werden.
- Bei bidirektionaler Kommunikation zwischen den verschieden eingestuften Netzen kann die Inhaltskontrolle sowohl manuell mit einem Viewer als auch automatisiert erfolgen. Beim automatisierten Verfahren erfolgt die Prüfung durch Verwendung/Nutzung sogenannter (NATO konformer) XML Security Label oder alternativ prüft ein Parser die Dateien, deren Inhalt in ein genau definiertes Format eingebettet ist. Dagegen sind Dateien mit beliebigen Texten oder Grafiken vom Anwender manuell mit einem Viewer zu prüfen.

Damit Security Gateways einerseits eine Release-Entscheidung sicher treffen können und sich andererseits vor Angriffen schützen können, sind neben einem Sicheren Betriebssystem (siehe Kapitel 4.3.6) weitere spezielle IT-Bausteine und -Funktionen notwendig. So sind zur Absicherung der Kommunikation (sowohl Administration als auch Nutzlast) sichere Signatureinheiten notwendig (siehe Kapitel 4.3.4). Diese kapseln kryptografische Funktionen in dedizierten Hardware-Einheiten, z.B. HSMs (Hardware Security Module) oder Smartcards. Mit Signatureinheiten werden Signaturen erzeugt und Verschlüsselung ermöglicht. Diese sind auch für die Erzeugung und Auswertung von durch digitale Signaturen integritätsgeschützten Sicherheitslabel notwendig.

Zur Verhinderung des ungewollten Abfließens von Daten über die Netzwerkschnittstellen sind des Weiteren vertrauenswürdige Netzwerkkarten notwendig, deren sicherheitstechnische Funktionsweise nachgewiesen wurde. Insbesondere sollen solche vertrauenswürdigen Netzwerkkarten keine Backdoors enthalten und auch keinen Zugriff auf eventuell vorhandene und (z.B. aus wirtschaftlichen Gründen) nicht deaktivierbaren Managementfunktionen des Hostsystems gewähren.

Ein sicheres Booten ist schließlich notwendig, um sicher zu gehen, dass auch tatsächlich die Software des Security Gateways gestartet wurde, die gestartet werden sollte. Zum Aufbau einer geeigneten Kette von Vertrauen sind weitere Hardwarekomponenten, z.B. TPMs (Trusted Platform Module), und Softwarekomponenten, z.B. Microkernel, notwendig. Diese Komponenten müssen sicher und nachweislich in die Bootkette integriert werden, bis die Anwendungsebene mit ihren ebenfalls notwendigen Selbsttests gestartet wurde. Dabei ist die Nutzung von vertrauenswürdiger und

zumindest in wesentlichen Teilen für eine Evaluation offener Firmware ebenfalls notwendig. Über die Evaluierung der Komponenten und des gesamten Systems sowie deren sicherer Erstkonfiguration hinaus ist es notwendig die Aufrechterhaltung und Wirksamkeit der Absicherungsmaßnahmen bzw. Systemeigenschaften im Betrieb kontinuierlich zu überwachen. Bedingt durch die gegebene Beschränkung der für die Entwicklung und Evaluierung einerseits sowie die Pflege und Betriebsführung andererseits verfügbaren nationalen Ressourcen wäre z.B. zu prüfen ob hier die Konsolidierung und Standardisierung von Schlüsselkomponenten wie z.B. Netzwerkadapter, TPMs und Microkernel zielführend ist.

4.3.6 Absicherung potenziell unsicherer Betriebssysteme und Laufzeitumgebungen

Beitrag Industrieverbände (BDSV und Bitkom)

Betriebssysteme und Laufzeitumgebungen bestehen in COTS-Softwareprodukten üblicherweise aus vielen Millionen Lines of Code (LoC). Eine IT-sicherheitstechnische Evaluierung dieser Systeme ist weder unter wirtschaftlichen noch unter praktischen Gesichtspunkten realistisch. Zum Betrieb von Fachanwendungen werden aber genau solche und damit faktisch unsichere Betriebssysteme und Laufzeitumgebungen benötigt (bspw. Office-Umgebungen Webbrowser etc.). Eine Anwendung kann jedoch nur so sicher sein, wie ihre Ausführungsumgebung. Das Konzept von datenbasierter Sicherheit funktioniert nur, wenn diese auf einer sicheren Plattform zur Verarbeitung, insbesondere im Hinblick auf ihre äußeren Schnittstellen (Speicher, Netzwerk) abläuft.

Wie lässt sich aber die Diskrepanz zwischen Hochsicherheitsanwendung und unsicherem Betriebssystem lösen? Dazu gibt es Lösungen, die die Kontrolle der Zugriffsrechte dieser potenziell unsicheren Betriebssysteme durch Sandboxing- und Virtualisierungstechniken erzwingen. Der Virtualisierungshost limitiert dabei den Zugriff der Betriebssysteme auf Hardware und die Kommunikation auf dem Host. Somit lassen sich sicherheitskritische von nicht-sicherheitskritischen Funktionen sicher voneinander trennen. Idealerweise ist der Virtualisierungshost selber evaluiert.

Hierzu gibt es bereits einige Lösungen am Markt, die auf gehärteten Standard-Opensource-Systemen aufsetzen, oder Mikrokern-Betriebssysteme nutzen. Letztere stellen durch die kleine Code-Basis, die im privilegierten Modus der CPU arbeiten, ein besser evaluierbares Betriebssystem zur Verfügung, das die Kontrollfunktionen beim Zugriff auf Schnittstellen und Ressourcen unumgehbar durchsetzen kann.

Alle nicht zwingend mit umfangreichen Rechten ausgestattete Module des Betriebssystems sowie die Anwendungen selber laufen in einem kontrollierten Umfeld mit eingeschränkten Rechten. Gleichzeitig stellt ein solcher Mikrokern auch Separierungsfunktionen zur Verfügung, um verschiedene Anwendungen unabhängig voneinander betreiben zu können. In Verbindung mit Virtualisierung, die dann selbst eine nicht-privilegierte Anwendung auf dem Mikrokern ist, können dann die nicht evaluierbaren Laufzeitumgebungen und die Applikationen, die auf diese angewiesen sind, abgesichert ablaufen. Ein wichtiges Element dieser Absicherung besteht in der Ver- und Entschlüsselung der verarbeiteten Daten, einer Anwendung. Diese muss außerhalb der Anwendung als Funktion auf dem Mikrokern-System implementiert werden. Der Mikrokern an sich ist also nur ein (wichtiger) Teil einer ganzheitlichen Sicherheitsarchitektur, die Kryptografie und Schlüsselmanagement integrieren muss.

Evaluierbare und letztlich evaluierte Mikrokerne und insbesondere darauf aufbauenden Systeme sind zwar auch in Deutschland in Teilbereichen vorhanden bzw. werden entwickelt. Es ist jedoch eine Herausforderung, auf Grund der Marktmacht der COTS-Plattformen, der Hardwareabhängigkeit und der dort vorherrschenden Dynamik von Lebenszyklen und Diversität eine signifikante Verbreitung zu gewinnen. Im Bereich der Hochsicherheitsanwendungen lassen sich jedoch Rahmenbedingungen schaffen, die Entwicklung, Evaluierung und Einsatz solcher Systeme ermöglichen.

Zur Absicherung unsicherer Betriebssysteme eignen sich zum Beispiel Mikrokernel. Ein sicheres Betriebssystem verfügt über einen Mikrokern, in dem nur die unbedingt notwendigen Funktionen im sogenannten privilegierten Modus laufen. Diese Funktionen erhalten damit Vollzugriff auf alle Hardware-Komponenten. Alle weiteren Funktionen, die für ein Betriebssystem notwendig sind, erhalten nur eingeschränkte Rechte. Damit lässt sich die problematische monolithische Struktur aufheben.

Ein weiterer Vorteil des Mikrokernels: Eine lückenlose und intensive Kontrolle aller Funktionen des Betriebssystems ist möglich. Das ist die Vorrausetzung für eine Evaluierung, wie sie für einen Zertifizierungsprozess beispielsweise nach Common Criteria notwendig ist. Damit kann ein hohes Maß an Sicherheit erreicht werden.

Eine mögliche Lösungsvariante können Open Source Microkernel mit einer Zugriffskontrolle basierend auf Object Capabilities wie z.B. Fiasco.OC darstellen. Dieser folgt dem Referenzmonitor-Konzept und auch den Entwurfsprinzipien von Saltzer & Schroeder (siehe 6.2 22) für sichere Systeme besonders gut: Da der grundlegende Mechanismus für die Zugriffskontrolle im Betriebssystemkernel implementiert ist und im privilegierten CPU-Mode läuft, kann er nicht durch Programme im Userspace manipuliert werden (er ist daher tamper proof). Außerdem kann somit sichergestellt werden, dass die Zugriffskontrolle immer und für alle Benutzerprogramme und Ressourcen angesprochen wird (always invoked, complete mediation).

L4-basierte Microkernel wie Fiasco.OC implementieren gemäß den Design-Vorgaben des L4 Entwicklers Jochen Liedtke (siehe 6.2.23) nur die absolut notwendigen Funktionen, basierend auf einer Menge von wenigen Primitiven.

4.3.7 Absicherung Middleware

Beitrag Industrieverbände (BDSV und Bitkom)

Der Begriff der Middleware bezeichnet in der Informationstechnologie eine Vermittlungsschicht zwischen verschiedenen softwaretechnischen Anwendungen und IT-Diensten und sorgt in heterogenen IT-Landschaften für eine ganzheitliche Integration und Abbildung von digitalen Geschäftsprozessen. Sobald verschiedene proprietäre IT-Dienste und Fachapplikationen zur Abbildung von digitalen Geschäftsprozessen miteinander kommunizieren müssen, unterstützt eine Middleware bei deren Orchestrierung, Vermittlung und der Interoperabilität zwischen den IT-Diensten und Fachapplikationen. Die Middleware versteht sich dabei stets als neutrale, vermittelnde Softwareschicht zwischen verteilten Anwendungen und Diensten und ermöglicht durch standardisierte Schnittstellen und Kommunikationsprotokolle eine Harmonisierung und Interoperabilität als Grundvoraussetzung für die Integration proprietärere Applikationen und IT-Dienste. Sie ist architektural meist zwischen der Betriebssystem- und der Applikationsebene angeordnet und ermöglicht einen reibungslosen Ablauf synchroner als auch asynchroner digitaler Geschäftsprozesse.
Heutige Middleware Lösungen stellen die Plattform für Dienste-orientierte Systemlösungen dar und ermöglichen den Aufbau von komplexen, zu meist lose gekoppelten Applikationsnetzen unter der Voraussetzung einer hohen Anwendungsneutralität. Die Anwendungsneutralität bzw. die Integrationsfähigkeit proprietärer Fachanwendungen und IT-Diente wird durch softwaretechnische Adapter und Proxydienste erreicht, die eine Übersetzung zwischen proprietären und standardisierten Schnittstellen der Middleware ermöglichen. Softwaretechnische Bussysteme und Nachrichtenwarteschlangen, sogenannte Message Queue ermöglichen dann den synchronen sowie asynchronen Austausch von Informationen und Nachrichten zwischen den vernetzten Applikationen. Allerdings basieren heutige Middleware Systeme auf einer aufwendigen statischen Vernetzung von Fachapplikationen auf Grundlage des TCP/IP Protokolls, die auf Basis von Adresskonfigurationen zumeist in Form einer IP-Adresse und einer Port Konfiguration ermöglicht werden. Dies hat zur Folge, dass diese Middleware-Systeme zumeist in Rechenzentren zum Einsatz kommen, wo hohe Verfügbarkeit und Bandbreite sowie langfristige gültige Adressenräume zur Verfügung stehen. Da im zunehmenden Maße die Grenzen der Domänenperimeter durch mobile Endgeräte sowie vernetzte on-premise/Edge-basierte IT-Infrastrukturen aufgeweicht werden, sind die Verfügbarkeiten von eingebundenen Fachapplikationen und IT-Diensten sowie die nutzbaren Netzwerkbandbreiten zwischen Ihnen stärker limitiert und zudem oftmals schwankend. Zudem werden die Konfigurationen der Adressenräume zunehmend variabler, wenn die Grenzen des stationären Rechenzentrums verlassen werden. Aus diesem Grund müssen moderne Middleware-Lösungen als verteilte selbst organisierte Systeme ausgelegt werden, die auf diese Dynamik durch automatisierte Prozesse Rechte- und Regelkonform reagieren können. Hierbei spielen Abstraktionen der Applikationsebene eine wesentliche Rolle. Durch sogenannte Proxydienste werden die Schnittstellen von proprietärer Fachanwendungen in standardisierte Schnittstellen überführt, so dass ein Datenfluss zwischen zwei nicht-kompatiblen proprietärer Fachanwendungen über einen Proxydient ermöglicht wird. Somit abstrahieren diese Proxydienste die angebundenen Fachanwendungen, wobei sie durchaus mehreren Fachapplikationen einbinden und vermitteln kann. Die Proxydienste abstrahieren somit die Schnittstellen- und Protokollebene der proprietären Fachapplikation, in dem sie zwischen diesen und eine standardisierte Schnittstelle der Kategorie übersetzen und diese dann über eine Bandbreite optimiertes Protokoll (zumeist binäres Protokoll) anbieten.

Anstelle der aufwendigen Konfiguration und Vernetzung von proprietären Fachapplikation werden diese Applikationskategorien (z.B. Kollaborationsdienst, Kartendienst, etc.) verwendet, die wiederum über ihre Proxydienste dynamisch in die verteilte Middleware-Lösung eingebunden und von dieser

automatisiert verwaltet werden können. Fragt dann ein IT-Dienst bzw. eine Fachanwendung eine digitale Fähigkeit an, liefert die Middleware die IP-Adresse eines Proxy Services der entsprechenden Kategorie zurück, die eine oder mehrere verfügbare Fachapplikation eingebunden hat. Der anfragende Dienst oder die Anwendung kann dann über den Proxydienst die Funktionalität der vermittelten Fachapplikation nutzen.
Wichtigste Aufgaben einer modernen Middleware sind neben der intelligenten Vernetzung von verteilten IT-Diensten und Fachapplikationen, der Bandbreiten optimierten Datenverteilung zwischen Ihnen oder der semantischen und organisatorischen Interoperabilität, die Schaffung einer ganzheitlichen IT-Sicherheit, die sowohl einen Datenschutz vor unberechtigten Zugriff sowie den Schutz vor Datenverlust sicherstellt. Datenmengen sind nicht nur zu managen, sondern vor allem zu schützen. Daten dürfen nur dort verarbeitet werden und für den Personenkreis einsehbar sein, für den sie gedacht sind. Jegliche Öffnung in einem IT-System stellt eine mögliche Gefahr für die Sicherheit dar. Deshalb muss eine Middleware höchsten Sicherheitsanforderungen entsprechen und die Integrität von Daten und Nachrichten stets erfüllen. Dies stellt moderne verteilte Middleware-Lösungen vor drei wesentliche Herausforderungen. Zunächst muss der berechtigte Datenzugriff in einem dynamischen Umfeld entsprechend eines Rollen- und Rechtekonzeptes sichergestellt werden, zum anderen müssen die Daten bei der Vermittlung und dem Transport vor unberechtigten Zugriff geschützt werden. Darüber hinaus muss bei Ausfall von Servern, Maschinen oder Geräten und die damit einhergehende Gefahr des Datenverlustes verhindert werden. Diese drei Forderungen müssen im erschwerten Umfeld einer verteilten IT-Infrastruktur (zentrales Rechenzentrum – dezentrale Rechenzentren – mobile Rechner und Endgeräte) mit hunderten von Rechenknoten gewährleistet werden. Manuell ist dies nicht mehr zu gewährleisten, so dass die Sicherheitsmechanismen automatisiert als intrinsische Fähigkeit der Middleware realisiert werden müssen.

Der berechtigte Zugriff auf Daten erfolgt in Dienst-orientierten IT-Systemen (SOA) stets durch einen IT-Dienst bzw. seiner Dienstschnittstelle, so dass nicht der Zugriff auf die Daten sondern vielmehr der Zugriff auf die Dienstschnittstelle entsprechend vorliegender Berechtigung des Nutzers sichergestellt werden muss. In oben beschriebenen verteilten Middleware-Systemen wird dies durch die Sichtbarkeit von Proxydiensten gewährleistet, die ein anfragender Nutzer bzw. eine Fachanwendung entsprechend seiner/ihrer Berechtigung sehen darf und konsumieren kann. Dazu müssen zuvor Rollen- und Rechtekonzepte spezifiziert sein, die jedem Hub des verteilten Middleware-Systems bekannt sein müssen. Dies wird durch systemische Proxydienste der Middleware erreicht, die ein synchronisiertes Identity and Access Management in jedem Hub der Middlware abbilden und mit proprietären Verzeichnisdiensten verknüpft sind. Dabei muss das Rollen- und Rechtekonzepte nicht nur auf Nutzerebene, sondern auch auf der Ebene der IT-Dienste Anwendung finden, da oftmals ein digitaler Geschäftsprozess durch eine Aneinanderreihung von Fachanwendungen abgebildet wird.

Der sichere Datentransport von einer Fachanwendung zur nächste oder aber zu einem Nutzer über die entsprechenden Proxydienste wird durch Verschlüsselungstechnologie (IPSec, VPN, etc.) gewährleistet. Zudem werden die Daten bandbreitenoptimiert stets durch ein binäres Übertragungsprotokoll übertragen, das die Lesbarkeit zusätzlich einschränkt.

Der Ausfall von Servern, Maschinen oder Geräten ist im Fall einer verteilten IT-Infrastruktur mit verlegefähigen und mobilen Rechenknoten weitaus wahrscheinlicher als für die eines stationären hochverfügbaren Rechenzentrums. Hier muss also ein besonderes Augenmerk auf die Gefahr des Datenverlustes bei Ausfall eines Rechenknoten gegeben werden. Verteilte Middlware-Lösungen müssen somit eine hohe Resilienz bei Ausfall von Rechenkonten aufweisen. Dies wir zum einen durch den hohen Vernetzungsgrad der verteilten Service Hubs der Middleware erreicht, der bei Ausfall eines Service Hubs dafür sorgt, dass ein andere übernimmt. Zudem melden sich Proxydienste dynamisch an den Service Hubs an und werden von diesen orchestriert und in ihrer Verfügbarkeit überwacht. Damit wird sichergestellt, dass bei Ausfall eines Service Hubs oder aber eines angefragten Proxydienstes bei entsprechender Redundanz stets eine Alternative dynamisch zugewiesen werden kann. Zum anderen weisen die Proxy Dienste einen Datenpuffer auf, der die Übertragung der Daten sowie deren Datenintegrität auch bei Ausfall von Datenverbindungen sicherstellt. Dies ermöglicht neben asynchroner Datenübermittlung auch die Prüfung, ob die Daten den Empfänger vollständig erreicht haben.

Mit dem steigenden Grad der Digitalisierung und Vernetzung von IT-Komponenten sowie Anwendungsdiensten nimmt die Bedeutung des Middleware als verbindendes Lösungselement zu. Im deutschen Markt sind sowohl Lösungen auf Basis Open Source als auch kommerzielle Eigenentwicklungen verfügbar. Jene werden nach Bedarf adaptiert und unterstützt von deutschen wie auch internationalen Unternehmen für unterschiedliche Einsatzzwecke, z.B. Büro-IT, missionskritische Anwendungsfelder.

4.3.8 Realisierung sicherer Führungsinformationssysteme (C4ISR)

Beitrag Industrieverbände (BDSV und Bitkom)

Führungsinformationssysteme (FüInfoSys) und C4ISR Systeme (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) bilden das technische Fundament für die militärische Führungsfähigkeit und der vernetzten Operationsführung (NetOpFü). Die durchgängige Vernetzung der Führungsebenen sorgt für beschleunigte Befehls- und Meldeketten und bietet den Entscheidern eine reichhaltige Informationsgrundlage, welche kontinuierlich durch Beobachtung, Überwachung und Aufklärung aktualisiert und bewertet wird. Die Digitalisierung umfasst sowohl die höheren Führungsebenen und deren Arbeit in Stäben oder Führungszellen auf Gefechtsständen als auch die unteren taktischen Führungsebenen. Vor allem die zuletzt genannten stehen im Fokus des Modernisierungsprogramms D-LBO (Digitalisierung Landbasierte Operationen) der Bundeswehr. Hierbei geht es insbesondere um die Ausrüstung der Truppe mit Kommunikationsmitteln und IT Ausstattung für den mobilen Einsatz. Hierzu steht der nächste Innovationsschritt bereits bevor. Der Einzug der Digitalisierung in die Waffeneinsatzsysteme minimiert die Notwendigkeit menschlicher Eingriffe bei der Bedienung von Beobachtungs-, Aufklärungs- und Feuerleitsystemen, so dass insbesondere im Gefecht der funktionale Prozess von der Zielaufklärung bis zur Zielbekämpfung weitgehend automatisiert ablaufen wird. Dabei werden sich dieser und ähnliche Prozesse nicht nur auf Einzelplattformen beschränken, sondern auf vernetzte Plattform-Cluster oder Schwärme.

© 2019 Bundeswehr/Markus Dittrich

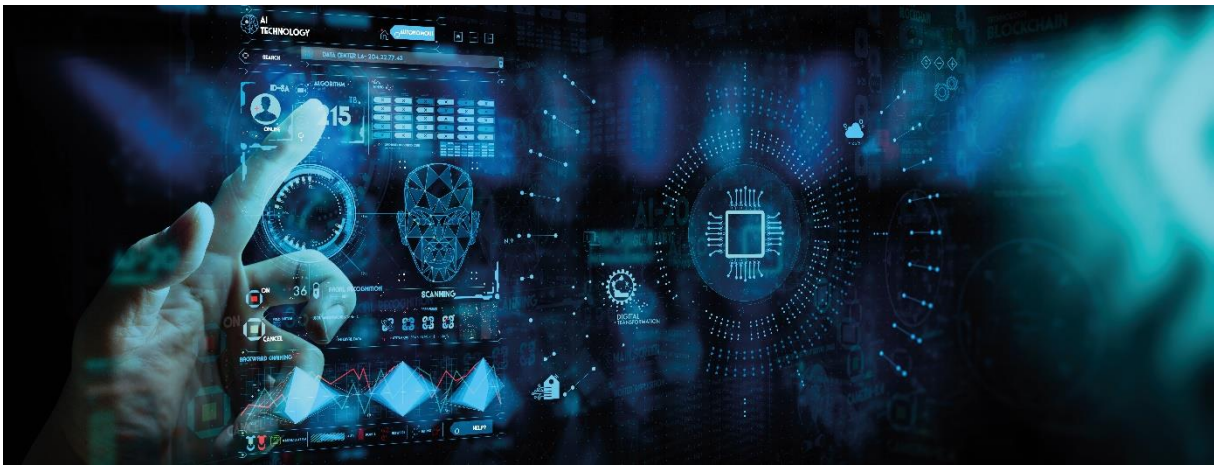
Es geht also um nicht weniger, als die bruchfreie, sichere Integration aller Systeme der Fähigkeitsdomänen Aufklärung, Führung, Wirkung und Unterstützung, wenn man effiziente End2End Prozesse vom Reachback bis hin zum Infanteristen der Zukunft aufbauen will. Grundsätzlich sollten dazu Wege gefunden werden, die heute noch in der Systemlandschaft des IT-SysBw existierenden Grenzen zwischen den administrativen Systemen der Fähigkeitsdomäne Unterstützung und den Fach- und Führungssystemen schrittweise und sicher abzubauen.

Solche militärischen Fähigkeiten beruhen sowohl auf Zukunftstechnologien wie Künstlicher Intelligenz, Maschinellem Sehen, 5G Mobilfunk, Autonomen Systemen usw., aber durchaus auch auf Gegenwartstechnologien wie herkömmlichen Rechnersystemen, Betriebssystemen oder Datenbanken – um nur einige zu nennen. Konsequenterweise sind aus IT-Sicherheitsperspektive beide Technologiestränge relevant, zumal die aufgeführten Gegenwartstechnologien sehr wohl in die Zukunft

fortgeschrieben werden und bereits heute durchgehend eingesetzt werden. Die Herausforderung besteht also darin, eine sichere Integration auf einer gemeinsamen Plattform zu schaffen und Innovationen selbst zu gestalten oder zu treiben, um Abhängigkeiten in puncto Technologieverfügbarkeit zu vermeiden. Gleichzeitig ist es geboten, bei den Gegenwartstechnologien ein gewisses Maß an Eigenständigkeit zu erreichen. Dafür wäre es nicht einmal notwendig, ganze neue Entwicklungen bei null zu starten, wie es etwa Google mit dem Betriebssystem Android vorgemacht hat. Der Sicherheitsgewinn läge in einer besseren Transparenz und Kontrolle der IT Systeme sowohl in kritischen Infrastrukturen als auch in militärischen Informations- und Waffeneinsatzsystemen.

4.3.9 Sicherer Betrieb komplexer IT-Umgebungen

Beitrag Industrieverbände (BDSV und Bitkom)



Ein sicherer Betrieb ist das Fundament jeder ITK-Umgebung. Nur wenn ein solcher gewährleistet ist, kann eine sichere Betriebsumgebung für System aller Art geschaffen und aufrechterhalten werden. Klare Strukturen und Abläufe im Betrieb bilden die Grundlage, um Angriffe und Anomalitäten zeitnah zu erkennen und abwehren zu können. Die Spielregeln hierfür werden in einem Sicherheitsrahmenwerk definiert, das abstrakte Sicherheitskontrollen und Sicherheitsziele regelt. Exemplarisch hierfür ist die Enterprise Security Architecture for Reliable ICT Services (ESARIS) als Industriestandard zu erwähnen. Die dort beschriebenen Sicherheitsziele sind allgemein gültig und für unterschiedlichste IKT-Systeme (soweit sinnvoll) anwendbar und beziehen sich nicht nur auf technische, sondern auch auf organisatorische und prozessuale Maßnahmen. Auch die vorhandenen BSI-Standards und IT-Grundschutzkataloge decken Anteile der Betriebsführung ab.

Die Komplexität der Absicherung ergibt sich weiterhin aus der Homogenität bzw. Heterogenität der jeweiligen IKT-Umgebung. In komplexen, inhomogenen IT Umgebungen ist der notwendige Aufwand für einen sicheren Betrieb in der Regel höher, schon allein durch die Notwendigkeit einer größeren Anzahl an Administrations- und Wartungsprogrammen, aber auch wegen zusätzlich notwendiger Pflege und Anpassungen an zentralen Systemen (z.B. Change Management Database) für die einheitliche Datenerfassung. Eine solche Datenbasis zur Bereitstellung detaillierter Informationen über die verwendete Hard- und Software, sowie deren Konfiguration, ist die Grundlage für einen gut funktionierenden IKT-Betrieb. Zeitnahe Erkennung und Reaktion auf Schwachstellen oder Sicherheitsprobleme aller Art bedingt eine aktuelle Datenbasis. Komplexe Probleme wie die Verwundbarkeiten SPECTRE und MELTDOWN, aber auch vermeintlich banale Schwächen wie Sicherheitslücken in Fernwartungslösungen, zeigen sehr deutlich das die Suche nach Methoden zur Identifikation von betroffenen Systemen und Komponenten nicht erst mit der Veröffentlichung solcher Schwächen beginnen sollte. Der daraus resultierende Verzug ist im Ernstfall nicht hinnehmbar. Grundlage eines sicheren IT Betriebs sind zudem klar definierte, funktionierende und eingespielte Prozesse im Operations Management (ITIL) und dem Security Management. Nur so kann im Ernstfall eine schnelle, koordinierte Reaktion erfolgen. Hier schaffen klare Strukturen und Prozess Handlungssicherheit.

Das mit der Administration und Betriebsführung betraute Personal ist eine weitere wichtige Komponente im Sinne der Etablierung und Aufrechterhaltung des Sicherheitsniveaus. Neben der Gewährleistung der Vertrauenswürdigkeit des Personals (z.B. Sicherheitsüberprüfungen) ist die kontinuierliche Sensibilisierung und Schulung hinsichtlich möglicher aktueller Angriffsvektoren

notwendig. Dies ist insbesondere relevant, da Schwachstellen in den eigentlichen Betriebsprozessen oder beim Betriebspersonal einfache und effektive Angriffe ermöglichen. Vielfach kann dabei mit geringem (technischen) Aufwand ein hoher Penetrationsgrad der angegriffenen IT-Umgebung erreicht werden. Eine angriffsverstärkende Wirkung ergibt sicher hierbei insbesondere daraus, dass die angegriffenen Personen (Administratoren) oft über erweiterte Rechte verfügen oder diese einfach erlangen können.

Neben den eingesetzten IT Werkzeugen, sind insbesondere die Absicherung der Kommunikationswege und die Authentifizierung der handelnden Personen und Systeme wesentliche Elemente für einen sicheren Betrieb. Durch den Einsatz geeigneter Verfahren kann der Weg der Angreifer im IT Verbund („Lateral movement“) deutlich erschwert werden, da Zugangsdaten nicht einfach kopiert oder übertragen werden können und einzelne Angriffstypen nicht mehr sinnvoll umsetzbar sind (z.B. Brute Force Angriffe).

Neben den auf der Konfiguration von Berechtigungen basierenden Verfahren sollten auch Möglichkeiten zur „inhaltlichen Absicherung“ betrachtet werden. So sollte die Möglichkeit bestehen, zu erkennen, ob ein Nutzer ggf. durch Kombination verschiedener berechtigter Anfragen an unterschiedliche Systeme versucht, Informationen zu erschließen, für welche er keine Berechtigung, Ermächtigung oder ein Verarbeitungserfordernis besitzt. Hierzu ist eine Integration der Sicherheits-mechanismen der IT-Plattform mit Sicherheitsmechanismen der Middleware und Fachanwendungen notwendig, um einen umfassenden Schutz in komplexen IT Umgebungen zu ermöglichen.

Neben klassischen Ansätzen zur IT Sicherheit sollten vermehrt auch neue Lösungen und Ansätze geprüft und ggf. übernommen werden. So bieten zahlreiche Startups neue Ansätze zur Abwehr und Detektion von Angriffen an. Ein Beispiel ist hierbei das aktive Auslegen von „Brotkrumen“ (oder auch Fallstricken) für Angreifer. Werden diese “Brotkrumen“ (z.B. spezielle Zugangsdaten) genutzt, so kann unmittelbar ein Angriff erkannt und beobachtet oder eingedämmt werden. Vielfach handelt es sich hierbei jedoch nicht um nationale Lösungsanbieter. Investitionen in die Forschung oder öffentliche Förderung nationaler Lösungsanbieter können hier Abhilfe schaffen.

Ein sicherer IT-Betrieb besteht aus vielen individuell wirksamen Einzelmaßnahmen. So sind neben der klassischen Absicherung von Systemen, Kommunikationsstrecken und Systemzugängen auch zahlreiche weitere führende Maßnahmen für die Detektion und Abwehr von aktiven Angriffen notwendig. Um hochmotivierte und gut ausgestatte Angreifer dauerhaft abwehren zu können, bedarf es ferner neben bewährten (klassischen) Sicher-heitslösungen und Ansätzen auch neue dem Angreifer unbekannten Elemente die als „Stolpersteine“ fungieren.

(c) 2015 Bundeswehr / Pfeil

Die Orchestrierung aller Einzelmaßnahmen zu einem gesamthaft wirksamen Schutz für den IKT-Betrieb wird im Sicherheitsrahmenwerk abgebildet. Hierbei gilt es auch, die menschliche Komponente zu berücksichtigen. Nur entsprechend geschultes und sensibilisiertes Personal kann das Rahmenwerk umsetzen und weiterentwickeln. Das Personal ist weithin auf ein aktuelles und korrektes Lagebild angewiesen. Aktuelle Informationen über die eingesetzten Systeme und Softwarekomponenten

(„Inventar“), sowie die aktuellen Vorgänge zwischen Systemen und Komponenten (z. B. überwacht durch ein „Security Operation Center“) ermöglichen es Angriffe zu erkennen, einzudämmen und abzuwehren.

Durch den Einsatz komplexer Soft- und Hardwaresysteme und bedingt durch die immer kürzeren Entwicklungszyklen für die COTS-Komponenten besteht ein ständiger Bedarf an Patch- und Update-Services. Zur Gewährleistung des sicheren Betriebes, insbesondere der IT-Sicherheit in IT-Systemen, sind daher Patch-Management und der Schutz vor Schadsoftwareessentielle Standardmaßnahmen essenziel. Aus diesem Grund muss eine Möglichkeit für das zeitnahe Aktualisieren geschaffen und wirksam genutzt werden.

Ein effizientes Patch-Management sorgt dafür, dass bekannte Schwachstellen der auf dem System vorhandenen Software möglichst rasch durch Sicherheitsaktualisierungen beseitigt werden.

Grundsätzlich ist der klassische IT-Betrieb im militärischen und zivilen Umfeld ähnlich, es gibt jedoch gerade in Bezug auf missionskritische Umfelder Besonderheiten, die zu berücksichtigen sind.
Operationelle militärische IKT-Systeme haben oftmals einen erhöhten Schutzbedarf und werden als separierte Systeme ohne direkte Anbindung an allgemeine bzw. öffentliche Strukturen wie z.B. das öffentliche Internet betrieben. Die in diesen „geschlossenen“ Systemen enthaltenen Komponenten bedürfen – ebenso wie in offenen Systemen – einer kontrollierten und permanenten Aktualisierung und Überwachung. Aufgrund der spezifischen Anforderungen z.B. hinsichtlich der Evaluierung bzw. Zulassung oder Akkreditierung sicherheitskritischer Komponenten sind hier Laufzeiten und Komplexität deutlich höher als im rein kommerziellen Umfeld. Fernerhin sind dezentrale oder auch in Teilen autark operierende operationelle militärische IT-Systeme – oftmals auch als Bestandteil eines komplexen Systems oder einer Plattform wie z.B. einem Fahrzeug oder einer Infrastruktur - nicht immer durchgängig für zentrale Überwachungs- und Betriebsführungsfunktionen sichtbar bzw. für die Durchführung notwendiger Aktualisierungen oder Konfigurationen verfügbar.
Im Hinblick auf einen qualitativ hochwertigen sicheren Betrieb und vor dem Hintergrund begrenzter personeller und materieller Ressourcen sind Aspekte wie

- Prozessautomation bei und Vereinheitlichung von Verfahren und Technologien, zur Entlastung des IT-Betriebspersonal von Standardaufgaben
- Priorisierung anhand von Risikofaktoren und Wirksamkeit (Selektion welche Komponenten zeitnah aktualisiert werden müssen und welche ggf. weniger prior zu betrachten sind)
- Einsatz von Simulations- und Messverfahren hinsichtlich der Auswirkung von Maßnahmen und Bewertung derer Wirksamkeit

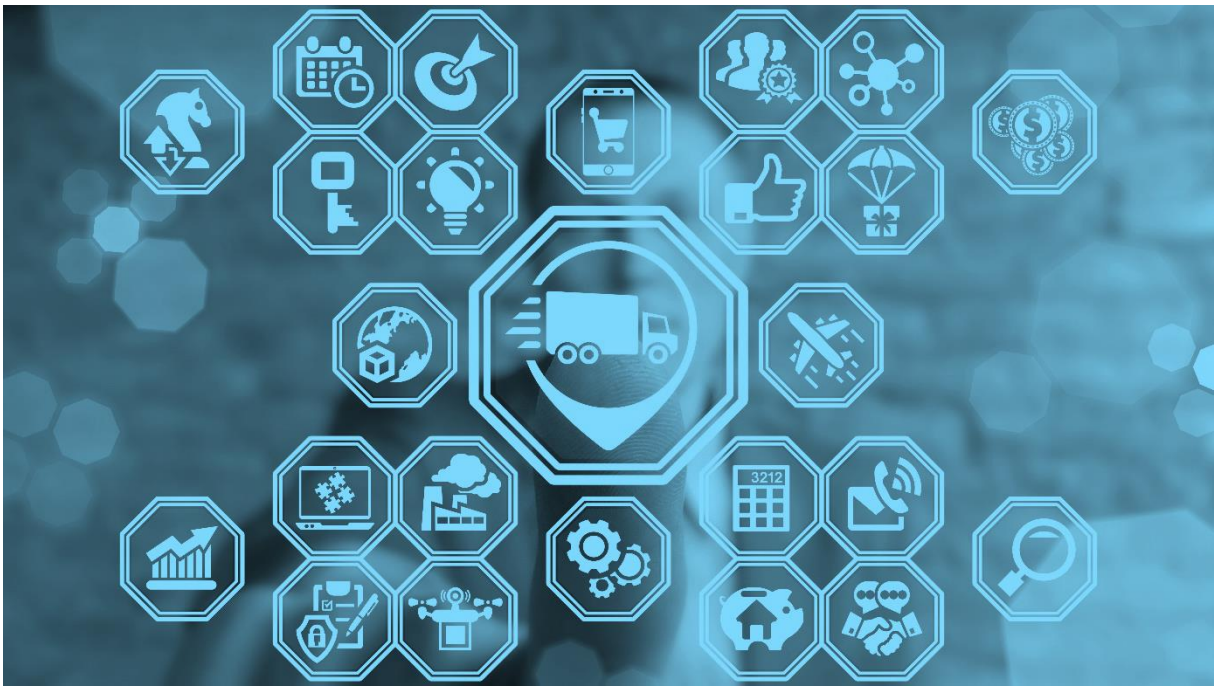
zu berücksichtigen.

In Bezug auf operationelle militärische IT-Verfahren ist ferner zu berücksichtigen, dass eine sicherer IT-Betrieb im Einsatz auch durch die dort verfügbaren personellen Kapazitäten, im Verbund mit den IT-Betriebsressourcen der zentralen Strukturen, ermöglicht werden muss.

Hierzu ist es wichtig die Betriebsverfahren möglichst über Domänengrenzen hinweg konsistent zu etablieren und auch bereits bei der Konzeption von IT-Systemen bzw. den dafür notwendigen Produkten und Komponenten die zur Ermöglichung einer sicheren Betriebsführung notwendigen Belange zu berücksichtigen.

4.3.10 Absicherung der Lieferketten

Beitrag Industrieverbände (BDSV und Bitkom)



Lieferketten können nicht nur national abgesichert sein, sondern benötigen analog zu globalisierten Wertschöpfungs- und Fertigungsprozessen (z.B. im Bereich Mikroelektronik) übergreifende Lösungsansätze (siehe 6.2.14.

Im Zuge der Betrachtung der inhärenten Sicherheit eines IT-Systems wird deutlich, dass die Sicherheit als Eigenschaft des Systems 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 wird. Erschwerend kommt zum Tragen, das der bestehende Kosten- und Wirtschaftlichkeitsdruck in der Vergangenheit zu einer Spezialisierung der einzelnen Unternehmen, und damit zu einer Fragmentierung und Internationalisierung der Fertigungs- und Lieferkette geführt hat. Diese Kette besteht aus den Schritten vor und nach der Lieferung und Inbetriebnahme eines Systems.

Die wesentlichen Elemente der Lieferkette vor der Lieferung bestehen aus folgenden Schritten:

- Entwicklung: Systementwicklung, Produktentwicklung (HW & 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 Lieferung sind weitere Schritte der Lieferkette 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

Die Verknüpfung erfolgt im Wesentlichen an zwei Punkten: der Integration und dem Betrieb bzw. der Wartung.

In jeden Übergang zwischen Schritten in der Lieferkette werden Informationen und gegebenenfalls Systeme zwischen Verantwortlichen 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 aus sicherheitstechnischer Sicht die Gefahr von Manipulation, Informationsabfluss oder Störung des Ablaufs. Ein besonderes Risiko liegt dabei auf den Übergaben vom Zulieferer an den Integrator und den Integrator oder Ersatzteilhersteller zum Nutzer da hier in der Regel längere Transportwege und verschiedene Dienstleister zum Einsatz kommen und somit die Angriffsfläche zur Manipulation vergrößert und die Nachvollziehbarkeit erschwert wird.
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: Information als in HW eingebrachte (embedded) Software oder als Software auf Datenträger
- Informationen: Basisdaten zur Verwendung durch Software oder Informationen zur Bedienung und Wartung des IT-Systems

Ein einfaches Lagebildsystem würde sich in dieser Klassifizierung wie folgt darstellen:

- 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, Unterstützungs-software auf Datenträger(n)
- Informationen: z.B. logistische und geographische Informationen für Lagebild und Betriebs-führung, Konfigurationsparameter, Benutzer- & Betriebsdokumentation auf Datenträger(n)

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

- Manipulation: HW-Systeme können manipuliert werden, um die Verfügbarkeit in kritischen Situationen zu manipulieren – z.B. Ausfall nach 24h non-stop Nutzung. SW-Systeme können manipuliert werden um unberechtigten Zugriff zu realisieren oder um Informationen zu manipulieren – z.B. Schaffung von Blind Spots im Lagebild. Informationen können verfälscht werden – z.B. Entfernung oder Verfremdung von Geodaten.

- Fälschung: Komplette Systeme oder deren Komponenten können ausgetauscht werden – z.B. Austausch von Festplatten auf Versionen mit kleiner MTBF, oder SW-Systeme durch manipulierte, mit Backdoors versehene Versionen.

- IP Misuse: Durch Analyse der Entwicklungsunterlagen oder durch Reverse Engineering von Systemen und Informationen können dritte Kenntnis über Fähigkeiten und Einschränkungen der einzusetzenden Systeme erhalten, sowie gegebenenfalls einen eigenen Fähigkeitsaufwuchs einleiten.

- Informationsabfluss: 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.
Exemplarisch wird sich im Folgenden auf die Absicherung des Übergangs und des Transportes zwischen zwei Arbeitsschritten sowie den Arbeitsschritt „Lieferung“ fokussiert um die Herausforderungen und Handlungsoptionen grundlegend zu erläutern.

Im Rahmen einer Sicherheitsbetrachtung ist grundsätzlich davon auszugehen, dass die Beschaffung von Systemen durch autorisierte Vertriebswege erfolgt, da nur diese unter der Kontrolle des Herstellers liegen. Insbesondere die Nutzung von sogenannten Grau- oder Reimporten verhindert die Umsetzung von durchgängigen 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 von sicherheitsrelevanten Prozessschritten und den sicherheitsrelevanten Lieferketten zwischen den Prozessschritten
- Gewährleistung der Identität von Ausgangs- und Endzustand im Transportprozess
- Verhinderung von Analyse und Informationsabfluss während des Transportprozesses
- Gewährleistung von eindeutiger 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. Ebenfalls ist nicht jeder Übergang zwischen zwei Prozessschritten gleich 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, das Ausgangs- und Endzustand des zu schützenden Systems identisch ist. Zum Beispiel können HD-Bildaufnahmen eingesetzt werden um den Zustand einer Platine vor und nach einem Transport automatisiert zu dokumentieren und auszuwerten. Neben dieser physischen Manipulation des Systems ist auch sicherzustellen, dass während eines Transportprozesses kein Auslesen von

Informationen oder kein Reverse Engineering der zu schützenden Systeme erfolgt, welches keine Auswirkungen auf die physische Repräsentanz der Systeme hat.

Grundsätzliche lassen sich die folgenden Bereiche zur Umsetzung von Sicherheitsmaßnahmen für 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 von technischen 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. im Produktdatenmanagement-System

Dokumentation des originalen Zustands der sicherheitsbedürftigen Subsysteme
- Nutzung von Entwicklungsumgebungen und Source-Code-Controlsystemen 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. dem Produktdatenmanagement-System

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 umfassen. Für die konkrete Ausprägung eines Sicherheitskonzeptes zur Absicherung der Lieferkette ist eine dedizierte Analyse notwendig, die das Systemdesign schützenswerter Systeme genauso beinhaltet wie die Gestaltung des kommerziellen Konsortiums und die dort etablierten Abhängigkeiten.

4.3.11 Schnittstelle Projekt/Rüstung

Beitrag BMVg (BAAINBw I4.1 – „HaFIS Projektelemente / Facharbeitsgruppen“)

"Basisdokumentation eines Projektleiters/einer Projektleiterin zum Thema 'vertrauenswürdige IT'"
Die Wirksamkeit der Projektarbeit und damit der Erfolg eines Projektes hängen entscheidend davon ab, dass allen Projektbeteiligten alle notwendigen Informationen nach Art und Umfang so zur Verfügung stehen, dass sie ihre Aufgaben erledigen können. Dem Informationsbedürfnis des Projektleiters/der Projektleiterin im BAAINBw kommt hierbei aufgrund seiner Aufgaben und besonderen Kompetenzen eine herausgehobene Stellung in Projekten zu.

Gemäß den aktuell gültigen Vorschriften ist der Projektleiter/die Projektleiterin im BAAINBw gesamtverantwortlich für die Umsetzung des Projekts im Leistungs-, Zeit- und Kostenrahmen und nimmt darüber hinaus innerhalb der Nutzungsphase die produktbezogenen Aufgaben eines Materialverantwortlichen für die Einsatzreife wahr. Diese Aufgaben schließen auch die frühzeitige Beantragung von Akkreditierungen sowie die Herstellung und Aufrechterhaltung der projektbezogenen und damit insbesondere der technischen IT-Sicherheit mit ein.

Letztlich ist ebenfalls er/sie es, der/die über eine Genehmigung zur Nutzung und deren ggf. später nötigen Aussetzung entscheidet oder entsprechende Entscheidungen vorbereitet. In diesem Spannungsfeld benötigt der Projektleiter/die Projektleiterin eine zu jeder Zeit aktuelle Dokumentation, die ihm/ihr erlaubt, proaktiv und mit entsprechendem zeitlichem Vorlauf seine Arbeits-/Zeit- und Finanzplanung durchzuführen.

Während die Industrie bzw. die Hersteller vertrauenswürdiger IT im Akkreditierungsprozess möglicherweise eine technisch tiefgehende Detaildokumentation bzgl. der einzusetzenden vertrauenswürdigen IT vorlegen müssen, benötigt ein Projektleiter/eine Projektleiterin hierzu eine ergänzende Dokumentation mit anderem Fokus. Ihn/Sie interessieren in seiner/ihrer Rolle weniger sehr detaillierte technische Darstellungen, sondern vor allem eine Überblicks- oder Architekturdokumentation, die ihn/sie in die Lage versetzt, das Gesamtsystem inkl. seiner Schnittstellen im Griff zu behalten und dazu valide Entscheidungen zu treffen.

Die Tiefe der Dokumentation des Projektleiters/der Projektleiterin variiert sicherlich mit dem Projekt. Handelt es sich um ein System, das im Wesentlichen aus handelsüblichen Komponenten integriert wird, ist die Dokumentation breiter und weniger tief als wenn das Projekt beispielsweise die Realisierung einer neuen Kryptokomponente zum Gegenstand hat. Die notwenige Dokumentation muss hierbei aktuell, klar formuliert sowie vollständig und übersichtlich sein und zudem alle Blickwinkel abdecken.

"Schnittstelle Projektleiter/Projektleiterin zur Industrie"

Kein Rüstungsprojekt lässt sich ohne den Rückgriff auf die richtigen Industrieunternehmen bewältigen. Die Bundeswehr und die Industrie stehen damit in einer wechselseitigen Abhängigkeit und den Projektleitern/Projektleiterinnen im BAAINBw und beim Auftragnehmer kommt dabei die wichtigste Schnittstellenfunktion zwischen den Partnern zu.

Operative Herausforderungen an dieser Schnittstelle können dabei immer dann entstehen, wenn man sich auf gegenseitige Zusicherungen verlassen muss. Im Bereich der vertrauenswürdigen IT kommt dieser Umstand aus Sicht eines Projektleiters/einer Projektleiterin insbesondere bei der Thematik der Zulassung der IT und möglicher Obsoleszenz zum Tragen. In einer solchen Situation muss er/sie frühzeitig einen entsprechenden Ersatz für die betroffene IT organisieren, um nicht die Genehmigung der Nutzung in Frage stellen zu müssen. Ist dies der Fall bei einem sehr breit genutzten IT-System entstehen hieraus ansonsten entsprechend große operative Probleme.

Aufgrund der langen Laufzeiten von Ausschreibungen und Vertragsschlüssen ist der Projektleiter/die Projektleiterin auf frühzeitige und umfassende Informationen der Industrie angewiesen, wenn z.B. droht, dass eingesetzte IT die Zulassung verlieren könnte. Gleichzeitig benötigt er/sie eine vollständige und regelmäßig aktualisierte Dokumentation, die solch mögliche Probleme frühzeitig aufzeigt und z.B. Zulassungstermine und Zulassungsauflagen präzise beschreibt. Eine transparente Kommunikation ist somit die Grundlage einer guten Zusammenarbeit.

Das Thema Informationssicherheit muss für beide Projektleiter/Projektleiterinnen eine ganz wesentliche Rolle bei der Umsetzung des Projektes spielen. Dabei soll die Industrie einerseits sichere Lösungen anbieten aber auch die bundeswehrseitigen Prozesse z.B. im Rahmen der Akkreditierung proaktiv und konstruktiv bedienen. Beide Projektleiter/Projektleiterinnen sind aber nicht zwingend Experten in Informationssicherheit. Deshalb wird der Projektleiter/die Projektleiterin auf Seiten der Bundeswehr durch einen/eine IT-SiBe Projekt unterstützt.

Jedes Projekt hat trotz aller guten Vorbereitung Risiken. Anforderungen können sich aufgrund neuerer Erkenntnisse ändern, im Akkreditierungsprozess kann Anpassungsbedarf festgestellt werden. Hier sind heute schon beide Seiten gefragt, eine schnelle Lösung zu finden, damit das Projekt dann auf korrigierter Basis weiterarbeiten kann. Die Bundeswehr muss hier auch finanziell in den Projekten eine gewisse Flexibilität haben, der Auftragnehmer muss schnell ein akzeptables Angebot beibringen. Dies kann durch Verwendung standardisierter und zertifizierter Komponenten sowie Vermeidung proprietärer Entwicklung begünstigt werden.

"Sichere Lieferketten - Verständnis Projektleiter/Projektleiterin Industrie"

Der Eingriff in die Lieferkette ermöglicht Angreifern eines Systems eine ganze Reihe möglicher Angriffsoptionen, die insbesondere durch staatliche bzw. nachrichtendienstliche Akteure genutzt werden können. Lieferketten sind somit ein lohnendes Ziel und ihr Schutz ist entsprechend wichtig.
Problematisch in Hinblick auf die Lieferketten von IT für militärische Anwendungen ist, dass sich auf dem weltweiten Markt viele Bauteile und auch einige Baugruppen nur aus Nicht-NATO bzw. Nicht-EU Staaten beziehen lassen.

Auch ist die Marktmacht der Bundeswehr und der beauftragten Industrie nicht ausreichend, um Hersteller von benötigten COTS-Produkten zur Offenlegung ihrer Hard- und Softwarearchitektur und deren Funktionsweise oder aber sogar zu Änderungen an deren Arbeitsweise zu bewegen.
Es lassen sich also nicht alle Teile der Lieferkette bzw. alle Produkte entsprechend sicher ausgestalten.

Der derzeit übliche Lösungsansatz ist der Einsatz von Architekturen bei denen die Informationen auch bei der Verwendung von ggf. unsicheren Anteilen sicher gekapselt werden sollen. Allgemein anerkannt ist die Auffassung, dass diese Vorgehensweise zwar das Risiko reduzieren aber nicht ausschließen kann. Hier wird die Industrie die verbleibenden Restrisiken auch offen benennen müssen. Denn nur dann kann zielgerichtet im Gesamtsystem ein Maßnahmenmix realisiert werden, um das Risiko soweit zu reduzieren, wie es erforderlich und wirtschaftlich ist.

4.3.12 IT-Sicherheitsüberprüfung von IT-Systemen und Zulassung für den VS-Betrieb

Beitrag BMVg (WTD 81 – GF 210 – PZITSichhBw)

Das Prüfzentrum für IT-Sicherheit in der Bundeswehr (PZITSichhBw) ist die einzige nach ISO/IEC 17025:2005 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannte Prüfstelle im Zuständigkeitsbereich des BMVg. Das PZITSichhBw wurde am 1. Oktober 1992 mittels Erlass durch das BMVg an der Wehrtechnischen Dienststelle 81 (WTD 81) eingerichtet und war damit eine der Grundlagen für die fachliche Zusammenarbeit mit dem BSI. Im Rahmen dieser Tätigkeit werden IT-Sicherheitsprodukte nach Common Criteria (CC) 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.

Den Schwerpunkt der Evaluierungstätigkeiten des PZITSichhBw bilden die sogenannten Rot-Schwarz Gateways zur Trennung von Sicherheitsdomänen. Das standardisierte Verfahren nach CC zur Gewährleistung der IT-Sicherheit umfasst sowohl formale Prüfungen als auch tiefgehende technische Untersuchungen der einzelnen Bestandteile eines Produktes, welche mit Hilfe der im PZITSichhBw vorhandenen Prüf- und Testsysteme zuverlässige und anerkannte Ergebnisse liefern.

Neben der Untersuchung von IT-Produkten im Rahmen von Evaluierungen führt das PZITSichhBw auch technische Prüfungen von nicht-zulassungspflichtigen IT-Produkten und gesamten IT-Systemen im Bereich der wehrtechnischen Forschung und Technologie (F&T) Stufe 2 und der Projekte nach CPM durch. Im Fokus dieser Prüfungen steht die Bewertung der IT-Sicherheit im Hinblick auf die verfahrensbezogene Freigabe durch den Projektleiter/die Projektleiterin bzw. die Akkreditierung durch die DEUmilSAA. Prüfaspekte sind dabei die Umsetzung von IT-Sicherheitsmaßnahmen gemäß dem IT-Sicherheitskonzept, aber auch die Einhaltung geltender nationaler und gegebenenfalls auch internationaler Vorgaben. Bei Projekten nach CPM bietet das PZITSichhBw in allen Phasen Beratungsleistungen hinsichtlich des Projektelements „IT-Sicherheit“ an.

Die Bedrohungen auf dem Gebiet der Informationstechnik haben in den vergangenen Jahren signifikant zugenommen und an Bedeutung gewonnen. Dies liegt zum einen am wachsenden Sicherheitsbewusstsein, aber auch an der stetig wachsenden Anzahl der Schwachstellen, die immer wieder Hersteller, Betreiber von IT-Systemen sowie auch den Nutzer vor neue Herausforderungen stellen. Das wahrscheinlich bekannteste Beispiel aus dem Jahr 2017 war die großflächige Infektion von Windows-Systemen durch die Ransomware „WannaCry“. Diese Schadsoftware wurde im Mai 2017 der breiten Öffentlichkeit bekannt, als aufgrund der Infektion großer IT-Systeme, wie z.B. von Krankenhäusern und der Deutschen Bahn AG, zahlreiche Dienste nicht mehr zur Verfügung gestellt werden konnten. Ursache für die rasante Verbreitung der Schadsoftware war eine Schwachstelle im SMB-Protokoll der Version 1. Der Hersteller Microsoft verteilte bereits ab 14. März 2017 Sicherheitsupdates, welche die Schwachstelle beheben sollten. Dies zeigt die Bedeutung eines effektiven und effizienten Patchmanagements und Netzwerkschutzes.

Die hohe Anzahl von IT-Systemen und die zunehmende Vernetzung, auch mit anderen nationalen und internationalen Institutionen, macht die Bundeswehr zu einem besonders interessanten Ziel von Cyberangriffen. Zur frühzeitigen Risikominimierung bietet das PZITSichhBw schon in der Analysephase des CPM umfassende Beratungs- und Prüfleistungen an. Das Ziel dieser Dienstleistungen in Form einer IT-Sicherheitsprüfung ist es, neben der Einhaltung von Vorgaben und Vorschriften, derartige Mängel aufzudecken und aufzuzeigen. Eine IT-Sicherheitsprüfung durch das PZITSichhBw bietet die Möglichkeit, ein System von einer neutralen Stelle in Hinblick auf die IT-Sicherheit prüfen und

bewerten zu lassen. Dazu soll ein möglichst umfassender Blick auf den Zustand eines Systems ermöglicht werden und im Gesamtkontext mit allen angeschlossenen bzw. anzuschließenden Systemen betrachtet werden. Ziel ist die Risikominimierung für das System und die damit verbundenen Systeme. Die Beauftragung erfolgt durch den Verantwortlichen für das IT-System.

Im Vorfeld der Beauftragung ist zu eruieren, welcher Prüfaufwand benötigt wird und in wie weit zusätzliche organisatorische Maßnahmen zu treffen sind. Wichtig dabei ist die terminliche Abstimmung zwischen dem Auftraggeber und dem Prüfteam, um einen optimalen Zeitansatz und Prüftermin zu finden, zu dem der Aufbau und die Konfiguration des Systems abgeschlossen sind.

Bei der Prüfung werden verschiedene Aspekte in die Arbeit der Prüfteams einbezogen. Zum einen muss die Vorschriftenlage berücksichtigt werden. Wichtigste Vorschrift der IT-Sicherheit in der Bundeswehr ist die Zentrale Dienstvorschrift A-960/1. Außerdem fließen weitere interne Vorschriften und Regelungen sowie Vorgaben des BMI, beispielsweise die Verschlusssachenanweisung, in die Untersuchung mit ein.

Die wichtigste Arbeitsgrundlage für die Vorbereitung und Durchführung einer IT-Sicherheitsprüfung ist das jeweilige projektbezogene IT-Sicherheitskonzept (IT-SichhKProj). Dieses dokumentiert und beschreibt die getroffenen IT-Sicherheitsmaßnahmen (technisch, personell, infrastrukturell, organisatorisch) sowie die Bewertung des Restrisikos, um die Integrität, Vertraulichkeit und Verfügbarkeit des IT-Systems zu gewährleisten.

Des Weiteren muss ein tiefgreifendes Verständnis für den Untersuchungsgegenstand geschaffen werden. Dazu können bspw. Netzbetriebskonzepte, Netzwerkpläne und Datenschutzkonzepte dienen. Alle angeforderten Dokumente müssen mindestens sechs Wochen vor Prüfungsbeginn zur Prüfungsvorbereitung vorliegen. Daraus wird eine Prüfspezifikation erstellt. Hierbei werden Maßnahmen aus den Dokumenten extrahiert, um diese später mit dem IST-Zustand des jeweiligen Systems zu vergleichen. Der Fokus liegt hierbei auf den technischen Maßnahmen sowie deren Wirksamkeit. Neben den Maßnahmen werden die nationalen Vorgaben der IT-Sicherheit für Konfiguration und Betrieb geprüft, welche das CSOCBw regelmäßig aktualisiert und veröffentlicht. Diese Vorgaben gibt es derzeit für Microsoft Windows-Betriebssysteme, Managed Switches und IP-Router, Symantec Endpoint Protection sowie Webbrowser.

Je nach Aufgabe und Einsatzumgebung können zusätzliche Vorgaben in die Prüfspezifikation einfließen. Dafür stellt bspw. das NCIRC der NATO verschiedenste Konfigurationsvorgaben bereit, welche weit über den Umfang der Konfigurationsvorgaben des CSOCBw hinausgehen und unter anderem auch Konfigurationsvorgaben für Datenbanken und Storages mitbringen.

Bestandteil der Prüfung ist außerdem die Feststellung, ob wirklich nur die Systemkomponenten genutzt werden, die für die Auftragserfüllung notwendig sind. Insbesondere im Netzwerkbereich werden häufig mehr Dienste angeboten als notwendig sind. Mit entsprechenden Netzwerkanalysetools lassen sich derartige Services darstellen und deren mögliche Schwachstellen aufdecken. Das konsequente Abstellen unnötiger Dienste minimiert die Angriffsfläche für potentielle Außen-, aber auch Innentäter. Besonderes Augenmerk wird ferner auf die Aktualität der Systeme sowie das Patchmanagement gelegt. Es wird auch berücksichtigt, ob die Handhabung des Systems durch den Nutzer korrekt durchgeführt wird. Als Beispiel lässt sich die Bedienung von Backup-Software aufführen. Die beste Backup-Software hilft nichts, wenn die Datensicherungen fehlschlagen und das Administrationspersonal nicht informiert wird. Während der Prüfung sind die Prüfer im Dialog mit dem vor Ort befindlichen Administrationspersonal, um mit dem Prüfer Fragen zu thematisieren und in

Zusammenarbeit mit den Administratoren die IT-Sicherheit in ihrem Zuständigkeitsbereich zu verbessern. Im Rahmen der Abschlussbesprechung wird ein vorläufiger Überblick über die IT-Sicherheit des Systems gegeben und kritische Mängel angesprochen, um deren zeitnahe Abstellung zu erwirken.

Nach der Prüfungsdurchführung werden die Ergebnisse der einzelnen Tests ausgewertet, aggregiert und bewertet. Um die Sicherheit der Systeme zu verbessern, werden im Bericht die einzelnen Prüfergebnisse erläutert und gegebenenfalls Empfehlungen zur Beseitigung von Mängeln gegeben.

4.3.13 Akkreditierung von IT-Systemen

Beitrag BMVg (DEUmilSAA)

Der Begriff „Akkreditierung“ leitet sich aus dem Lateinischen „accredere“ für „Glauben schenken“ oder „vertrauen“ ab. Er bedeutet, dass eine anerkannte Instanz einer anderen das Erfüllen gewisser Eigenschaften bescheinigt.

Im Geschäftsbereich des BMVg ist hinsichtlich der Akkreditierung von Systemen in Bezug auf Informationssicherheit diese anerkannte Stelle die DEUmilSAA. Der Ursprung der Tätigkeiten geht auf das Jahr 2006 zurück, als zwischen dem Bundesministerium des Innern (BMI) als der zuständigen nationalen Sicherheitsbehörde und dem BMVg ein Ressortabkommen unterzeichnet wurde. Dieses regelte, dass das damalige Referat A6 im IT-Amt der Bundeswehr für die IT Sicherheitsakkreditierung der Systeme im Geschäftsbereich des BMVg zuständig ist und somit dort entsprechende Aufgaben wahrnimmt, die ansonsten dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zufallen.
Die Bezeichnung DEUmilSAA stammt aus dem internationalen Bereich der NATO. So beschränkte sich die Akkreditierung ursprünglich auch nur auf Systeme, welche eingestufte NATO Informationen verarbeiten. Sie bestand im Wesentlichen aus einer Vorortprüfung, die idealtypisch vor Inbetriebnahme des Systems erfolgte. Die Aufgaben als DEUmilSAA wurden zu Beginn nur durch zwei Mitarbeiter wahrgenommen. Daher blieb die Akkreditierung zunächst nur auf sehr wenige Systeme beschränkt.

Das Ressortabkommen von 2006 besitzt auch heute noch Gültigkeit, wobei – aufgrund verschiedener Umstrukturierungen – nunmehr die Gruppe DEUmilSAA im Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) der Rechtsnachfolger des damaligen Referates IT-AmtBw A6 ist.
Jedoch wurde im Laufe der Jahre der Umfang der zu akkreditierenden Systeme ausgeweitet.
So ist eine Akkreditierung nunmehr grundsätzlich für sämtliche IT durchzuführen und somit gleichzeitig die Voraussetzung für die Freigabe von IT.

Ausgangspunkt jeder Akkreditierung ist das Informationssicherheitskonzept, welches durch das realisierende Projekt bzw. in Einzelfällen durch die nutzende oder betreibende Dienststelle zu erarbeiten ist. Es beschreibt die für das System relevanten Aspekte der Informationssicherheit. Der erste Schritt einer Akkreditierung umfasst stets die Prüfung bzw. Mitzeichnung des Informationssicherheitskonzeptes. Dabei wird anhand der Papierlage die Beachtung und Umsetzung der Vorgaben zur Informationssicherheit bewertet. Basierend darauf legt DEUmilSAA fest, in wie weit und in welchem Umfang eine Prüfung des Systems vor Ort erfolgt. Sie wird unter Leitung der DEUmilSAA zum Teil mit Unterstützung durch weitere Stellen im ZCSBw vorgenommen. Technische Schwachstellenanalysen werden durch Teams der Abteilung Prüfung- und Unterstützung, Prüfungen auf kompromittierende elektromagnetische Abstrahlung durch das ebenfalls dort angesiedelte Abstrahlprüfzentrum der Bundeswehr vorgenommen. Daneben unterstützen auch Stellen wie das Bundesamt für den Militärischen Abschirmdienst (BAMAD) die Akkreditierung.

Über die rein technischen Aspekte der IT-Sicherheit hinaus werden im Rahmen der Prüfungen auch Aspekte im Hinblick auf Organisation, Personal sowie Infrastruktur betrachtet, die sich im Sinne einer umfassenden Informationssicherheit aus den Anforderungen des Geheimschutzes, des Datenschutzes und der militärischen Sicherheit ergeben.

Eine weitere Aufgabe der DEUmilSAA besteht in der Beratung der gemäß Customer Product Management (CPM) zuständigen Stellen, i.d.R. der Integrierten Projektteams (IPT) sowie im

Besonderen der Projekte des Bundesamtes für Ausrüstung, Informationstechnik und Nutzung (BAAINBw), hinsichtlich aller Aspekte der Informationssicherheit. Somit können in den Projekten frühzeitig die Weichen gestellt werden, damit die Aspekte der Informationssicherheit umfassend berücksichtigt werden. Seitens der IPT wurde diese Dienstleistung der DEUmilSAA bisher noch nicht in größerem Umfang in Anspruch genommen. Der zu erwartende signifikante Anstieg dieser zusätzlichen Beratungsleistung wird durch die DEUmilSAA bis zum Abschluss des personellen Aufwuchses (2022) im Rahmen ihrer IOC (initial operational capability) mit derzeit etwa zwanzig Dienstposten nur eingeschränkt leistbar sein. Gerade in dem Bereich der Beratung ist ein umfangreicher personeller Aufwuchs der DEUmilSAA vorgesehen.

Neben den oben dargestellten Aufgaben ist die DEUmilSAA auch international in sogenannten Security Accreditation Boards tätig. Hier werden die im Rahmen internationaler Einsätze zu beachtenden Vorgaben im Zusammenhang mit dem Umgang eingestufter Informationen sowie bzgl. der Akkreditierungsprüfungen abgestimmt. Dabei vertritt DEUmilSAA die deutschen Interessen.

Darüber hinaus ist die DEUmilSAA der zentrale Ansprechpartner der Bundeswehr gegenüber dem BSI im Zusammenhang mit dem Einsatz zugelassener Produkte. Das BSI ist im Rahmen seiner Aufgaben für die Prüfung und Zulassung von Produkten mit sicherheitsrelevanten Funktionalitäten, z.B. Kryptogeräten, zuständig. Gerade wenn neue Produkte einer Zulassung bedürfen, ist dies oftmals mit einem sehr hohen Abstimmungsaufwand zwischen Hersteller, Projekt und BSI verbunden, wobei DEUmilSAA koordinierend tätig ist.

Abschließend ist festzustellen, dass die DEUmilSAA mit ihren Aufgaben als zentrale Kontroll- und Beratungsinstanz für Informationssicherheit darauf hinwirkt, dass Mindeststandards in den Systemen der Bundeswehr umgesetzt und somit nationale als auch internationale Vorgaben eingehalten werden. Darüber hinaus können durch DEUmilSAA Themen, die projektübergreifend und damit oftmals für das gesamte IT-System der Bundeswehr kritisch sind, aufgenommen und an den Chief Information Security Officer Bundeswehr (CISOBw) sowie an die für Vorgaben in der Bundeswehr zuständigen Stellen weitergegeben werden, damit dort generelle Lösungsmöglichkeiten für die gesamte Bundeswehr gefunden und durchgesetzt werden.

4.3.14 Zukünftige Anwendungsgebiete

Beitrag Industrieverbände (BDSV und Bitkom)

Großdatenmengenverarbeitung („**Big Data Analytics**“) beschreibt die Datenverarbeitung aus Datenmengen in verteilten Datenbanken in Größenordnungen die aktuelle Tabellenkalkulationen nicht mehr bewältigen können. Eingesetzt wird Big Data Analytics in der Auswertung beispielsweise im Rahmen der Multi-Sensor-Datenverarbeitung, Suchmaschinen, Datenauswertung bei Vorratsdatenspeicherung, in komplexen, verteilten Überwachungssystemen, in Entscheidungsunterstützungssystemen und in Navigationssystemen. Die Daten liegen meist nicht in strukturierter Form vor und werden oft erst zum Auswertungszeitpunkt über verschiedene Datenquellen verbunden, um neue Erkenntnisse zu gewinnen. Hier entstehen neue Berufsfelder wie der Data Scientist, aber auch die eingesetzte Technologie unterscheidet sich in ihren Grundzügen von den klassischen relationalen Datenbanken, die nach wie vor in Transaktionssystemen zum Einsatz kommen.

Hochleistungsrechnen („**High Performance Computing**“) ist das parallel verteilte Rechnen von komplexen Modellen, die mit konventioneller Rechenleistung in angemessener Zeit nicht zu bewältigen sind. Eingesetzt werden Hochleistungsrechnen und Massive Parallel Processing oder Symmetric Multiprocessing zur Berechnung wissenschaftlicher Modelle und Simulationen, beispielsweise in der Meteorologie, Physik, Astronomie, Biologie und in der Klimaforschung, aber auch in wirtschaftlichen Bereichen, wie Festigkeits- und Verformungsuntersuchungen, Strömungsberechnungen und im Hochfrequenzhandel an den Finanzmärkten, um nur einige Beispiele zu nennen Militärische Nutzung findet das Hochleistungsrechnen im Kontext C2, vor allem im vernetzten Schlachtfeld (NetOpFü) und C4ISR, um beispielsweise im Lagebild Situation unter Eintrag chemischer und biologischer Kampfstoffe zu verarbeiten. Sicherheitskritisch ist vor allem die Logistik der Systeme, da Chipsätze und Hochleistungsrechentechnik in der Regel außerhalb der EU produziert werden. Die Software und Algorithmen liegen auch schwerpunktmäßig im geistigen Eigentum nicht-europäischer Hersteller oder basieren zumindest lizenzrechtlich auf quelloffenen („open-source“) Bibliotheken, erstellt außerhalb Europas. Da es alleine schon aus wirtschaftlichen Gesichtspunkten wohl unrealistisch ist, mittelfristig Hersteller von Halbleitertechnologie mit Weltmarktrelevanz inkl. Forschung, Fertigung und Entwicklung wieder (vollständig) in Europa oder gar Deutschland anzusiedeln, wird die kontinuierliche Prüfung und Sicherstellung der Versorgung als solche, als auch die kontinuierliche Sicherung gegen angreifbare bzw. ausnutzbare Schwachstellen ein Hauptfokus für die Absicherung der Systeme sein müssen. Die Entdeckungen der Schwachstellen MELTDOWN und SPECTRE geben Anlass zu einer Neubewertung, inwieweit Hersteller aber auch Integratoren und Anwender überhaupt selbst noch in der Lage sind bzw. sein werden, die Komplexität noch sicher zu gestalten und was dies im Resultat für zukünftige Entwicklungen aber auch die Absicherung in Nutzung befindlicher Technologie bedeutet.

Militärische Nutzung von HPC und Big Data Analytics findet auch im Bereich Modellbildung und Simulation statt. Insbesondere die in der TK "M&S" beschriebenen Anwendungsfelder "Analyse und Planung" und "Beschaffung" sollten im Hinblick auf den hier notwendigen Anwendungsfall weiterentwickelt werden, um durch geeignete, noch zu entwickelnde Simulationsmodelle, mögliche Sicherheitslücken schon in der Designphase zu entdecken und die Systeme aus IT-Sicherheitssicht zu optimieren, möglichst durch ein resilientes Design, das nicht nur gegen aktuell bekannte, sondern prinzipiell mögliche Bedrohungen geschützt ist. Deswegen ist m.E. Modellbildung und Simulation von IT-Sicherheit (auf unterschiedlichen Detailebenen) als Schlüsselfähigkeit zu sehen. Verfahren der künstlichen Intelligenz (Artifical Intelligence) insbesondere maschinelles Lernen (**Machine Learning**) also der kognitive Erkenntnisgewinn aus Daten erfahren wieder eine erhöhte Aufmerksamkeit, durch

den Einsatz bei Sprach und Bilderkennung. Durch die verbesserte Rechen-, Speicher- und Übertragungskapazität heutiger Systeme ist man in der Lage neuronale Netze in einer Tiefe und Qualität auf Basis von Massendaten (Big Data) zu trainieren (lehren), dass sie den Turing Test für die Erkennung in einzelnen Disziplinen bestehen. Im militärischen Umfeld sind Bildererkennung oder überhaupt Mustererkennung in Drohnensystemen nicht mehr wegzudenken. Die Prüfung und Verifikation der Algorithmen der Großdatenverarbeitung im Rahmen künstlicher Intelligenz, autonomer Systeme und maschinellen Lernens ist eine neue Anforderung. Im Einsatz autonomer Systeme muss reproduzierbar verstanden werden und nachgewiesen werden können, warum Systeme wie entscheiden werden. Maschinelles Lernen erfolgt nicht unbedingt deterministisch. Daher ist die Prüfung und Verifikation eine große Herausforderung.

Das Ein-Chip-System (**„System on a Chip"** oder **SoC**) beschreibt integrierte Schaltkreise, bei der eine Vielzahl von programmierbaren Funktionen hoch-integriert auf einen Chip implementiert werden. Eingesetzt werden diese Chips in Datenerfassungsgeräten, in der Steuerungs- und Automatisierungstechnik und der Avionik sowie perspektivisch in sog. intelligenten Sensoren als auch vernetzten und autonomen mobilen Systemen.

Diese vier Technologien finden sich in verschiedenen Kombinationen in den Anforderungen der meisten Systeme von künstlicher Intelligenz. Autonome oder teilautonome Systeme benötigen immer gewisse Formen der Mustererkennung und –vorhersage und sind als lernende Systeme angelegt.
Aus Sicht der Informationssicherheit sind zu Grunde liegende Technologien zu bewerten und perspektivisch nach Bedeutung im operativen Einsatz einzuschätzen. Grundsätzlich gilt, Geschwindigkeit und Latenz im operativen Einsatz sind entscheidend dafür, wer Vorteile in der Entscheidungsunterstützung und daraus resultierenden Wirkung hat. Unterstützung durch o.g. Technologien wird entscheidend die Augenhöhe mit anderen internationalen Streitkräften bestimmen.

Die Suche und der Einsatz von qualifiziertem Personal, das diese Technologien versteht und untersucht, ist bereits eine Herausforderung. Die Qualifikation liegt dabei deutlich über reiner Anwendungskompetenz hinaus. Die Möglichkeit eigener Technologiezentren und Aufbau von vertrauenswürdiger Fertigung z.B. innerhalb der EU ist dabei zu betrachten.

Anforderungen an die Sicherung gegen Angriffe und Sabotage aus Sicht der Informationssicherheit sind unabhängig von der geographischen Lozierung bei komplexen Systemen hoch. Als Konsequenz muss das Thema sicherer Versorgungs- und Lieferketten intensiv adressiert werden. Eine weitere Herausforderung wird die Etablierung von Lebenszyklusunterstützungsprozessen sein, die immerhin so agil sein müssen, dass sie mit den Iterationen der Weiterentwicklung der o. a. Technologien Schritt halten können.

Nach aktuellem Wissensstand wären ausreichend leistungsstarke **Quantencomputer** unter anderem in der Lage, nach heutigem Stand der Technologie gängige kryptografische Verfahren zu brechen bzw. entscheidend zu schwächen. Daher arbeiten Kryptologen schon seit geraumer Zeit an sogenannter Post-Quantum Kryptografie, die auch dem leistungsfähigsten Quantencomputer widerstehen soll.
Handlungsbedarf hinsichtlich Quantumcomputing wurde bereits mehrfach auf Seiten der Industrie und des BMVg identifiziert, im Rahmen mehrerer Initiativen adressiert und wird seitens GB BMVg im Rahmen mehrerer F&T-Maßnahmen betrachtet. Aus diesem Grund erfolgt im Rahmen des EK2 keine weitergehende Detailbetrachtung.

4.3.14.1 Moving Target Defence (MTD)

Beitrag BMVg (UniBwM FI CODE)

Der Wettlauf zwischen Angreifern und Verteidigern im Cyberraum hat einen beispiellosen Reifegrad und Komplexität erreicht. Während die Verteidiger neue Detektions- und Reaktionswerkzeuge einsetzen, entwickeln Angreifer verschiedene Techniken und Methoden, um diese Mechanismen zu umgehen. Mit den derzeitigen State-of-the-Art-Ansätzen sind die Verteidiger maßlos unterlegen, da der Angreifer nur eine Schwachstelle ausnutzen, der Verteidiger jedoch das gesamte System schützen muss. Das Ziel der Verteidiger ist es dieser Asymmetrie des Angriffs entgegen zu wirken indem die Angriffsfläche ständig verändert wird, um es den Angreifern zu erschweren, die aktuelle Position des Zieles (der Daten) zu erkennen.

Täuschungstechniken gehören traditionell zu den bevorzugten Methoden der Angreifer. Überraschung und Unsicherheit bieten dem Angreifer einen inhärenten Vorteil gegenüber dem Verteidiger, der den nächsten Zug des Angreifers nicht vorhersagen kann. Moving Target Defense (MTD) zielt genau darauf ab, eine asymmetrische Unsicherheit auf der Angreiferseite zu erzeugen, indem die Angriffsfläche, durch Schwachstellen im System definiert dynamisch verändert wird. MTD-Ansätze ermöglichen das Erstellen, Analysieren, Evaluieren und Implementieren von Mechanismen und Strategien, um die Angriffsfläche zu Dynamisieren und die Verfügbarkeit und das Ausnutzen von Schwachstellen und Angriffsmöglichkeiten zu begrenzen.

Heutzutage bevorzugen die meisten Institutionen geordnete Strukturen, die statisch, vorhersehbar und überschaubar sind. Dies gilt speziell für den Bereich der Infrastruktur. Es mag sinnvoll erscheinen, da es die Wartung und die Reaktionsfähigkeit optimiert. Doch gleichzeitig bietet diese Situation eine Spielwiese für Angreifer. Sobald ein Angreifer sich Zugang zu einem solchen Netz erschleichen konnte, ist es in der Regel ziemlich leicht, sich in das bestehende Betriebssystem einzunisten und von dort aus rasch mehrere Teile der Infrastruktur zu kompromittieren.

Aktuell werden im Forschungsumfeld MTD-Techniken auf verschiedenen auf drei Ebenen erforscht; auf Netzebene, Betriebssystemebene und auf Anwendungsebene. Hierbei werden sowohl neue MTD-Techniken theoretisch formuliert, als auch bestehende Ansätze und MTD-Strategien evaluiert und verbessert.

4.4 Einordnung in IT-Architektur und Wertschöpfungskette

Beitrag Industrieverbände (BDSV und Bitkom)

Die betrachteten Themenfelder erstrecken sich über die gesamte Wertschöpfungskette und umfassen unterschiedliche Aspekte der IT-Architektur.

Gemäß der aktuellen Einschätzung wird die Wertschöpfungskette im Bereich der Software durchgängig beherrscht, im Bereich Hardware sind Schwerpunktkompetenzen vorhanden (z.B. Design und Entwicklung sowie Integration) aber bezüglich der umfänglichen Abdeckung von IT außerhalb von Spezialthemen wie z.B. Krypto besteht Handlungsbedarf um z.B. vertrauenswürdige Fertigung und Prüfung durchgängig und nachhaltig ermöglichen zu können.

Querschnittliche Aufgabenstellungen wie die Absicherung von Lieferketten, der sichere Betrieb von IT und auch die Lebenszyklusunterstützung betreffen die gesamte Wertschöpfungskette und erstrecken sich analog dazu über alle Aspekte der IT-Architektur – direkt oder indirekt. Hier ist grundsätzliches konzeptionelles Verständnis vorhanden aber die Fähigkeiten und deren Anwendung sind abhängig vom Anwendungsfall (z.B. Hochsicherheitsprodukte vs. COTS-IT) unterschiedlich ausgeprägt.

4.5 Bewertung Beitrags- und Zukunftsfähigkeit

Beitrag Industrieverbände (BDSV und Bitkom)

Während im Umfeld der COTS-IT die Beitragsfähigkeit der nationalen Industrie vor dem Hintergrund des globalen COTS-Weltmarkt nur bedingt ausgeprägt ist, wird die Beitragsfähigkeit für spezifische vertrauenswürdige IT als Bestandteil von Büro- oder auch Missions-IT als hoch angesehen. Um diese Beitragsfähigkeit zu erhalten aber auch die Zukunftsfähigkeit für z.B. neue Anwendungsfelder und Technologien auszubauen ist ein abgestimmtes und zielgerichtetes Vorgehen notwendig. Im Bereich der Hardware ist die Optimierung der Abdeckung der kompletten Wertschöpfungskette, auch unter Einbezug europäischer und globaler Ansätze, notwendig.

Neben der Beherrschung von Schlüsseltechnologien ist als Grundlage einer nachhaltigen Beitrags- und Zukunftsfähigkeit die weitere Etablierung und Entwicklung von Schlüsselfähigkeiten (z.B. Integration, Adaption) unerlässlich um z.B. Systeme bestehend aus Komponenten unterschiedlicher Vertrauenswürdigkeit unter Wahrung von Verhältnismäßigkeit, Wirtschaftlichkeit aber auch der notwendigen Wirksamkeit bereitstellen und im Lebenszyklus unterstützen zu können.

In Bezug auf zukünftige Themenfelder wie z.B. die Konzeption, Realisierung und Nutzung von analytischen Verfahren und künstlicher Intelligenz/maschinellem Lernen wird die konzeptionelle bzw. wissenschaftliche Beitragsfähigkeit als hoch angesehen. Die Erlangung einer marktrelevanten und nachhaltigen Beitrags- und damit Zukunftsfähigkeit in diesen entstehenden Anwendungsfeldern und Marktsegmenten wird als machbar und zielführend angesehen.

Sowohl im Bereich der Forschung- und Entwicklung als auch der Realisierung sind die nationalen Ressourcen – naturgemäß – begrenzt. Im Interesse einer Beitragsfähigkeit zu den rein nationalen Interessen aber auch im Hinblick auf den internationalen Markt und einer wettbewerbsfähigen

Zukunftsfähigkeit ist eine Fokussierung und die Vermeidung nicht zielführender Redundanzen zu erwägen.

5 Handlungsempfehlung

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

Grundsätzlich stehen der kommerzielle globalisierte Massemarkt und der nationale Bedarf im sicherheitssensitiven Umfeld hinsichtlich der Rahmenbedingungen und Anforderungen in einem Spannungsverhältnis. Dies betrifft sowohl die Anforderungen als auch die Marktmechanismen. Hierzu wird aus Sicht des EK2 empfohlen, mögliche Synergien unter Berücksichtigung der Sicherheits- und Wirtschaftlichkeitsaspekte zu nutzen und zu fördern, aber im gleichen Maße auch entschlossen Maßnahmen zur weiteren Etablierung und Aufrechterhaltung von nationalen bzw. europäischen Fähigkeiten zu ergreifen.

Begleitend zur Entwicklung einer gemeinsamen Vision und deren Umsetzung sollten die bereits als notwendig und zielführend identifizierten Handlungsfelder und erfolgsversprechenden Lösungsansätze mit kurzfristiger Umsetzbarkeit im Rahmen der etablierten Zuständigkeiten und Kooperationsmodelle angegangen werden.

Neben spezifischen technischen Handlungsfeldern (z.B. Ausbau Kompetenz und Fähigkeit bzgl. Hardware oder prägbaren Zukunftstechnologien wie Künstlicher Intelligenz) ist die Etablierung und Beherrschung von als Pendant zur Schlüsseltechnologie Cyber/IT und der Ausbau der Kompetenzen aber auch des Umsetzungsgrad querschnittlicher Fähigkeiten wie der durchgängigen Absicherung von Lieferketten und der Lebenszyklusunterstützung essentieller Erfolgsfaktor.

Wichtige Grundlage hierzu ist Erlangung der Fähigkeit zur quantitativen und qualitativen Bemessung des Bedarfes an Absicherungsniveau, sowohl im Hinblick auf das benötige Maß an Vertrauenswürdigkeit als auch z.B. Verfahrensstärke und Wirksamkeit, und die resultierende monetäre Bemessung. Dies bedingt auch die weitere Präzisierung der nationalen Forderungen hinsichtlich Schlüsseltechnologie Cyber/IT und deren nationaler Ausprägung bzw. Operationalisierung versus multinationaler, europäischer oder internationaler/globaler Optionen.

Unter den eingangs in Kapitel 4 gemachten Bemerkungen zu den Randbedingungen ist zu nennen, dass unter Beachtung technisch-wirtschaftlicher Aspekte und im rechtlich zulässigen Rahmen bereits einige Lösungsansätze existieren und auch zur Anwendung kommen, um das Spannungsfeld abzubauen. So z.B. besteht bzgl. der Umweltanforderungen die Möglichkeit des Einsatzes von marktgängiger IT in gekapselten Umgebungen, die die Umweltanforderungen durch Klimatisierung und Vibrationsdämpfung auf den Bereich der geringeren Umweltanforderungen des Massenmarktes reduzieren (z.B. Kabinen, Container, Shelter, Transport- und Lagerbehälter) sowie bzgl. der Abstrahlsicherheit unter Beachtung des Zonenmodells die Möglichkeit der Nutzung der Schirmung von Infrastruktur und Gebäuden sowie der Freiraumdämpfung anstelle der Verwendung von in sich hoch geschirmten und abstrahlarmen IT-Komponenten.

5.1 Entwicklung „Vision“

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

Aktuell ist die Herausforderung nach der Verfügbarkeit ausreichend vertrauenswürdiger IT als nationale Schlüsseltechnologie und die Etablierung entsprechender Schlüsselfähigkeiten weder gesamtstaatlich noch durch einzelne Ressorts oder die Industrie umfassend lösbar.

Daraus abgeleitet entsteht zunächst der Bedarf einer Vision zur Adressierung der Herausforderung auf Basis der aktuell und zukünftig absehbaren Herausforderungen. Neben einer solchen Vision sind ebenfalls Erfolgskriterien für die Operationalisierung der Vision als auch Kalibrierung notwendig.

Auf dieser Grundlage sollte ein Plan zur Umsetzung der Vision auf Basis einer zweckmäßigen und gesetzmäßigen Arbeitsteilung zur Umsetzung mittel- und kurzfristiger Maßnahmen inkl. regulatorischem Handlungsbedarf entwickelt werden.

5.1.1 Schnittstelle Projekt/Rüstung

Beitrag BMVg (BAAINBw I4.1 – „HaFIS Projektelemente / Facharbeitsgruppen“)

"Basisdokumentation eines Projektleiters/einer Projektleiterin zum Thema 'vertrauenswürdige IT'"
Neben einer technisch tiefgehenden Detaildokumentation zu ihren Produkten liefert die Industrie eine ergänzende Dokumentation für zentrale Entscheider im Rüstungsprozess.
Im Rahmen dieser Dokumentation können sich abhängig vom konkreten Produkt folgende Informationen als zweckmäßig erweisen:

- Architekturübersichten
- Grundlegende Übersicht über die wesentlichen IT-Sicherheitsmaßnahmen und der dazu eingesetzten Produkte
- Schnittstellen und deren Absicherung
- Liste der eingesetzten Produkte mit Ansprechpartnern (schnelle Reaktionsmöglichkeit bei Bekanntwerden von Schwachstellen)
- Zulassungsunterlagen, belastbare - insbesondere zeitliche - Prognosen bei laufenden Zulassungsverfahren
- Zeitliche Ausplanung der Aktivitäten im Rahmen der Akkreditierung

"Schnittstelle Projektleiter/Projektleiterin zur Industrie"
Die Projektleiter/Projektleiterinnen aus Rüstung und Industrie pflegen als wichtigste Schnittstelle zwischen den Organisationen eine transparente Kommunikation. Notwendige Informationen fließen frühzeitig und umfassend in beide Richtungen. Aussagen zur Reife eines Produkts oder der Fortschritt im Zulassungsverfahren sind belastbar, Risiken werden offen angesprochen werden und die gemeinsame Zeitplanung ist verlässlich. Das Thema Informationssicherheit hat einen hohen Stellenwert und die Projektleiter/Projektleiterinnen beider Seiten werden durch entsprechende Experten/Expertinnen unterstützt. Der Akkreditierungsprozess wird vom Auftragnehmer/von den Auftragnehmerinnen proaktiv begleitet und hat auf beiden Seiten die nötige Management-Attention. Eskalationsmechanismen sind eingerichtet und werden auch schnell genutzt. Es besteht die Möglichkeit, Verträge schnell und zielgerichtet anzupassen.

"Sichere Lieferketten - Verständnis Projektleiter/Projektleiterin Industrie"
Die Industrie identifiziert die aus den Lieferketten bestehenden Risiken und bietet kundenspezifische Mitigationsmaßnahmen an. Die Bundeswehr bewertet diese unter Berücksichtigung des Schutzbedarfs der Informationen im System und der Wirtschaftlichkeit.

5.1.2 IT-Sicherheitsüberprüfung von IT-Systemen und Zulassung für den VS-Betrieb

Beitrag BMVg (WTD 81 – GF 210 – PZITSichhBw)

Das PZITSichhBw ist eine nach ISO/IEC 17025:2005 anerkannte BSI Prüfstelle zur Durchführung von Evaluierungen nach Common Criteria (CC). Diese Evaluierung ist die Grundvoraussetzung für eine Zulassung von IT-Sicherheitsprodukten für den VS-Betrieb durch das Bundesamt für Sicherheit in der Informationstechnik (BSI).
Dazu verfügt das PZITSichhBw, welches an der WTD 81 im Geschäftsfeld 210 „IT-Sicherheit“ etabliert ist, über eigene Labor- und Testeinrichtungen. Des Weiteren übernimmt das PZITSichhBw eine Beratungsfunktion für Vorhaben und Projekte in allen Phasen des CPM hinsichtlich des Projektelements „Informationssicherheit, IT-Architektur/-Standardisierung und Datenschutz.

Zukünftig wird das PZITSichhBw die Aufrechterhaltung der Anerkennung durch das BSI nach der neuen Norm ISO/IEC 17025:2017 anstreben. Es wird seine Zusammenarbeit in Bezug auf die Durchführung von Evaluierungen mit dem BSI, der DEUmilSAA und den nicht behördlichen Prüfstellen, welche beim BSI anerkannt sind, verstärken.
Darüber hinaus wird das PZITSichhBw IT-Sicherheitsüberprüfungen in der Analysephase Teil 2 sowie in der Realisierungsphase von IT-Projekten intensivieren. Dies dient als wesentlicher Beitrag zur Risikominimierung für die Projekte des BAAINBw. Zudem werden die bereits etablierten Kooperationen mit anderen Behörden, Instituten, Universitäten und der Industrie vertieft.

5.1.3 Akkreditierung

Beitrag BMVg (DEUmilSAA)

Der formale und inhaltliche Wechsel von der IT-Sicherheit zur Informationssicherheit ist vollzogen.
Die DEUmilSAA hat die mit der Final Operational Capability vorgesehene Zielstruktur eingenommen, verfügt über die dazu notwendige organisatorische, technische, personelle und infrastrukturelle Basis und steht nach wie vor mit allen relevanten nationalen und internationalen Stellen im fachlichen Austausch.

Für alle Systeme der Bundeswehr mit IT-Anteilen erfolgt eine Akkreditierung durch die DEUmilSAA.
Nationale und international anzulegende Standards zur Informationssicherheit werden in sämtlichen Systemen der Bundeswehr vollständig umgesetzt.

5.1.4 Moving Target Defence (MTD)

Beitrag BMVg (UniBwM FI CODE)

Obwohl die aktuellen MTD-Ansätze sehr vielversprechend erscheinen, ist die Forschung auf diesem Gebiet erst am Anfang. Eine der Problemstellungen, die zukünftig erforscht werden muss, ist die Definition der Angriffsfläche und der möglichen Transformationen der Angriffsfläche bzw. der Schwachstellen, die auf dynamische und zufällige Weise ausgenutzt werden können. Ferner stellt sich weiterhin die Frage der Redundanz von heterogenen Komponenten, um genügend Transformationsraum zur Verfügung zu stellen. Da sich die gesamte Angriffsfläche stetig verändert, ist die Aktualität bzw. die Festlegung der Zeitpunkte, wann wichtige Transformationen durchgeführt werden wichtig, um das gesamte System zu schützen und intrusiven Aktionen entgegenzuwirken. Darüber hinaus ist die funktionale Äquivalenz der Transformation sicherzustellen. Da MTD-Ansätze sowohl auf der Netz-, Betriebs- und Anwendungsebene durchgeführt werden können, ist eine Kooperation zwischen den MTD-Ansätzen sowie Integration mit bestehenden Abwehrmechanismen wie u.a. Firewalls und Intrusion Detection Systemen (IDS) erforderlich. Auch hier besteht weiterhin erheblicher Forschungsbedarf.

Der Einsatz von MTD-Ansätzen auf der Netzebene (IP-Ebene) bezieht sich u.a. auf die Obfuskation (Verschleierung, Änderung) von IP-Adressen. Hierfür kann u.a. eine hardware-basierte Lösung eingesetzt werden, die in der Infrastruktur eingebettet wird und für Netzpartner unsichtbar bleibt. Das Prinzip entspricht dem sogenannten Zero-Trust-Ansatz im Bereich von IT-Sicherheit. Hierbei kann ein Angreifer zwar via TCP/IP noch in das System gelangen, wird aber über die Zeit isoliert, so dass er andere Geräte im Netz nicht gefährden kann, da die anderen Geräte zufällig immer wieder ihre IP-Adresse ändern und so die Informationen des Angreifers obsolet werden. Neben der IP-Adresse können Ports geändert, geöffnet, geschlossen sowie Port Traffic verschleiert werden, um die Netztopologie möglichst umfänglich zu dynamisieren. Hierfür wird am FI CODE an einer Klassifizierung gearbeitet, um anschließend an eine Auswahlhilfe eine Testumgebung aufbauen zu können.

Der Vorteil von MTD liegt darin, dass gesammelte Informationen an Aktualität und Relevanz verlieren und somit für den Angreifer unbrauchbar werden. Sobald man aber mit dem Gedanken spielt, neue Hardware in existierende Infrastruktur zu bringen, trifft man meist auf Widerstand seitens der Administratoren. Doch dieser Widerstand ist grundlos, denn die oben beschriebene hardware-basierte MTD-Lösung funktioniert unabhängig von der Infrastruktur. Für sie spielt es keine Rolle, ob Patches oder Updates auf das zugrundeliegende System angewendet werden. Genau diese Eigenschaft macht die hardware-basierte MTD Lösung so attraktiv.

Software-Defined-Networking (SDN) ermöglicht ferner, die starre, monolithische Netzarchitektur flexibler zu gestalten, und bessere Kontrolle, Sicherheit und Vertrauen zu erlangen. Somit ermöglichen SDN-basierte MTD-Ansätze den Prozess der Analyse der Angriffsfläche nicht nur zu verzögern, sondern Antworten schicken, die den Angreifer irritieren. Da die MTD-Ansätze sehr komplex sind, sowohl in der Verteidigung als im Angriff, ist der Einsatz von Machine-Learning-Ansätzen, z.B. für die Automatisierung von Netzkonfigurationen, erforderlich.

5.2 Zuordnung Handlungsbedarf

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

Im Grundsatz sind die Zuständigkeiten und Verantwortungen durch die – auf geltenden Regulierungen basierenden - gegebenen Strukturen auf Seiten des GB BMVg, der Industrie, der Institutionen der Forschung und Lehre verteilt und etabliert. Die Erfahrungen der letzten Jahre im Umfeld Cyber/IT zeigen allerdings, dass jene gewachsenen Strukturen zur Zielerreichung nicht ausreichend sind.

Die federführenden Ressorts der inneren und äußeren Sicherheit, die Industrie (vertreten durch die Verbände) und die Institutionen auf Seiten Forschung und Lehre sollten prüfen, auf welche Weise der identifizierte Handlungsbedarf zielführend und effektiver bzw. effizienter adressiert und das Ergebnis erreicht werden kann. Ein wichtiger Schritt ist hier mit der Etablierung der Agentur für Innovation in der Cybersicherheit (Cyberagentur, AIC) und der Agentur zur Förderung von Sprunginnovationen bereits gemacht. Weitere Ansätze und deren Operationalisierung hinsichtlich der in diesem Dokument identifizierten Handlungsfelder sollten im Rahmen der bestehenden Dialogformate betrachtet, priorisiert und dann gemeinsam umgesetzt werden.

5.2.1 Schnittstelle Projekt/Rüstung

Beitrag BMVg (BAAINBw I4.1 – „HaFIS Projektelemente / Facharbeitsgruppen“)

"Basisdokumentation eines Projektleiters/einer Projektleiterin zum Thema 'vertrauenswürdige IT'"
Die Dokumentation für den Projektleiter/die Projektleiterin wird vertraglich vereinbart und deren Erstellung auftragnehmerseitig mit entsprechender Management-Attention begleitet.

"Schnittstelle Projektleiter/Projektleiterin zur Industrie"
Formen der Zusammenarbeit zwischen Auftragnehmer und Auftraggeber, z.B. die dazu erforderlichen Gremien werden vertraglich vereinbart und dann im weiteren Projektverlauf mit Leben gefüllt.

"Sichere Lieferketten - Verständnis Projektleiter/Projektleiterin Industrie"
Die Industrie beobachtet ständig Entwicklungen auf dem Weltmarkt und im Bereich Open Source, die das Potenzial haben, die Sicherheit weiter zu verbessern. Hier finden sich bereits heute in verschiedenen Formaten Experten aus der etablierten Industrie, der Gründerszene und der Bundeswehr zusammen.

5.2.2 IT-Sicherheitsüberprüfung von IT-Systemen und Zulassung für den VS-Betrieb

Beitrag BMVg (WTD 81 – GF 210 – PZITSichhBw)

Die Anerkennung durch das BSI wird aufrecht erhalten und die Umstellung auf die Vorgaben der neuen Norm ISO/IEC 17025:2017 wird durchgeführt werden.Zudem wird die Einbindung von anerkannten Prüfstellen im Unterauftrag sowie der Industrie intensiviert und erweitert werden.

Um auch den zukünftigen Anforderungen der Bedarfsdecker und -träger gerecht zu werden, sind weiterhin stets Maßnahmen notwendig, um die fachliche Kompetenz des PZITSichhBw zu erhalten, zu erweitern und langfristig sicherzustellen. Dazu gehören insbesondere die Bearbeitung von Forschungs- und Technologievorhaben.

Zukünftig werden hier verstärkt die Themenfelder Schwachstellenanalyse von Software (z.B. Android- oder iOS- Applikationen) und Hardware (z.B. FPGA) sowie vertrauenswürdige IT-Plattformen betrachtet.

5.2.3 Akkreditierung

Beitrag BMVg (DEUmilSAA)

Aktuell erfolgt bundeswehrintern eine Neuausrichtung in Bezug auf Informationssicherheit. Diese verfolgt einerseits die Ausweitung der Aktivitäten auf diesem Feld sowie andererseits die Verbesserung bisheriger Prozesse und des Ressourceneinsatzes hierfür.

Entsprechende Festlegungen erfolgen im Rahmen der aktuellen Überarbeitung der Zentralen Dienstvorschrift A-960/1 Informationssicherheit in der Bundeswehr. Demgemäß wird sich die Akkreditierung durch DEUmilSAA im ZCSBw zukünftig auf alle Systeme der Bundeswehr mit IT Anteilen erstrecken. Damit wird die entsprechende Vorgabe der IT-Strategie des Geschäftsbereichs BMVg (s. dort Abschnitt 5.3.7) umgesetzt und es werden zukünftig sämtliche Systeme einer Bewertung hinsichtlich ihrer Informationssicherheit unterzogen.

Dabei kann die Prüfung – je nach Kritikalität des Systems – sich ggf. auf das zu erstellende Informationssicherheitskonzept beschränken, sofern ausreichende Maßnahmen zur Qualitätssicherung im Hinblick auf die Informationssicherheit umgesetzt wurden. Weitergehende Prüfungen erfolgen vor Ort in der Einsatzumgebung des Systems: Diese können mit Unterstützung durch andere Stellen der Bundeswehr, den Prüf- und Unterstutzungsteams sowie dem Abstrahlprüfzentrum des ZCSBw oder dem BAMAD, durchgeführt werden. Sie umfassen technische Schwachstellenanalysen, Prüfungen zur Abstrahlsicherheit oder zur Lauschabwehr.

Wichtig für eine aussagekräftige Lagebewertung der Informationssicherheit wird zukünftig sein, dass auf Seiten der Projekte, also insbesondere des BAAINBw, als Input eine Übersicht über sämtliche für eine Akkreditierung relevanter Systeme besteht. Nur so kann der erreichte Abdeckungsgrad der Akkreditierung für die Systeme der Bundeswehr festgestellt werden. Mit der beabsichtigten Neuausrichtung soll DEUmilSAA sukzessive über die IOC und IOC+ bis zur Einnahme FOC (final operational capability) im Jahr 2022 vor dem Hintergrund der großen Anzahl von Projekten und Systemen weiterentwickelt werden.

In der jetzigen Übergangsphase (IOC+) werden seitens DEUmilSAA bereits zusätzliche Aufgaben im Bereich der Akkreditierung übernommen. Mit FOC in 2022 werden sich diese Aufgaben noch ausweiten gerade auch im Hinblick auf die frühzeitige Beratung.

5.2.4 Moving Target Defence (MTD)

Beitrag BMVg (UniBwM FI CODE)

Wie bereits oben erwähnt, bedarf es vor dem praktischen Einsatz von MTD-Techniken noch weiteren Forschungsbedarf.

Am Forschungsinstitut CODE an der Universität der Bundeswehr München, laufen bereits Forschungsprojekte im Bereich Moving Target Defense.

Das Hauptziel der Projekte ist es, eine starke akademische Forschung im Bereich MTD zu etablieren, sowie neue Forschungsfelder im Bereich MTD zu identifizieren. Es sollen hierbei auch fundamentale neue Forschungsaktivitäten im Bereich MTD vorangetrieben werden. Obwohl die MTD-Ansätze sehr vielversprechend erscheinen, ist die Forschung auf diesem Gebiet erst am Anfang. Einige wissenschaftliche Fragestellungen seien hier genannt:

- **Definition der Angriffsfläche und der möglichen Transformationen**: MTD-Ansätze sollten es ermöglichen alle Schwachstellen, die auf dynamische und zufällige Weise ausgenutzt werden könnten, zu transformieren (komplett, teilweise). Insbesondere sollten Schwachstellen in kritischen Ressourcen (Komponenten mit hoher Kritikalität) identifiziert werden. Dabei stellen sich unterschiedlich Forschungsfragestellungen. Wie kann die Kritikalität der Ressourcen (Netzkomponenten), die sich durch die topologischen, zeitlichen und funktionalen Abhängigkeiten verändert adäquat automatisch identifiziert werden? Wie kann die Angriffsfläche transformiert werden (komplett, teilweise)?
- **Redundanz**: Die Netztopologie muss ausreichend heterogene und redundante Komponente beinhalten, damit die Netzelemente genügend Transformationsraum haben.
- **Aktualität**: Da nicht die gesamte Angriffsfläche verändert werden kann (durch die Komplexität des Systems), sollten MTD-Ansätze, die zu einem Zeitpunkt wichtigsten Transformationen durchführen, um das gesamte System zu schützen und intrusiven Aktionen entgegenzuwirken. Was sind die "wichtigsten" Transformationen zum gewissen Zeitpunkt? Was sind intrusive Aktionen, die die MTD-Transformation auslösen sollten? Was passiert, wenn eine MTD-Transformation fehlgeschlagen ist?
- **Funktionale Äquivalenz**: Obwohl es notwendig ist, Netzelemente (virtuell) zu transformieren, muss die Funktionalität des gesamten geschützten Systems weiterhin zur Verfügung stehen. Neben der Funktionalität ist die vereinbarte Dienstgüte (Quality of Service, QoS), die in Service Level Agreements vereinbart ist, einzuhalten. Wie kann das erfolgen, insbesondere auch im Hinblick auf die Dienstgütegarantien?
- **Kooperation und Integration**: Wenn im angestrebten System eine Vielzahl von MTD-Mechanismen implementiert ist, müssen die MTD-Ansätze in einer kooperativen Weise zusammenarbeiten, um sich nicht gegenseitig zu behindern. Ferner müssen diese mit bestehenden Abwehrmechanismen wie u.a. Firewalls, Intrusion Detection und Prevention Systemen integriert werden. Wie erfolgt die Kooperation und wie die Integration?

Wesentliche Ziele sind die Identifizierung, Bewertung, Auswahl und Weiterentwicklung von MTD-Technologien insbesondere für den Bedarfsträger Cyber- und Informationsraum (CIR):

- Identifikation und Bewertung von State-of-the-Art im Bereich MTD
- Generierung von Auswahlhilfen von MTD-Technologien zur Härtung hochsicherer Netze und Systeme
- Identifikation von Forschungsbedarf für MTD in Hochsicherheitsapplikationen

Des Weiteren wurde am Forschungsinstitut CODE an der UniBw M eine Professur im Bereich Sichere Softwareentwicklung zum 1.10.2017 berufen. Eine Forschungsaktivität dieser Professur ist unter anderem die Diversifizierung von Software bereits zur Compilezeit der Programme. Dadurch, dass Programme in verschiedenen Instanzen ein unterschiedliches „Aussehen und internes Verhalten“ (Speicherabbild, Programmfluss, etc.) aufweisen, kann ein Angriffsvektor für eine Instanz eines Programmes nicht auf eine andere Instanz desselben Programmes übertragen werden.

Die Forschungsgebiete in der sprachbasierten Sicherheit, mit Schwerpunkten im Bereich Software Diversity, Control-Flow Integrity, JavaScript und Information-Flow Tracking sind hochaktuell und dienen der Erforschung neuer Angriffsvektoren, bzw. deren Abschwächung. Erste Ergebnisse dieser Arbeiten zeigen, dass durch die Anwendung von MTD-Techniken zur Compilezeit sogar hardware-basierte Angriffe auf die Prozessoren, wie. z.B. SPECTRE und MELTDOWN, abgeschwächt, bzw. verhindert werden können.

5.3 Empfohlene Maßnahmen

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

Im Folgenden Abschnitt werden die aus Sicht des EK2 identifizierten Handlungsempfehlungen zur Adressierung der identifizierten Handlungsfelder erläutert. Hierbei handelt es sich im Sinne der Mandatierung des EK2 um fachliche Empfehlungen die keinerlei Vorfestlegung oder Absprache im vertraglichen oder vergaberechtlichen Sinne darstellen, siehe hierzu die Erläuterungen in den Kapiteln 1 bis 0.

(1) Einbringung von den wesentlichen nationalen Sicherheitsinteressen betreffenden Anteile von Cyber/IT in den Katalog der nationalen Schlüsseltechnologien sowie Einführung und übergreifend abgestimmte Definition des Begriffs der Schlüsselfähigkeiten im Kontext Cyber/IT und Entwicklung einer gemeinsamen Vision (siehe Abschnitt 0).

(2) Detailierung notwendiger Schlüsselfähigkeiten als Pendant zur Schlüsseltechnologie Cyber/IT und der Ausbau der Kompetenzen als Grundlage zur dauerhaften und nachhaltigen Etablierung und Beherrschung benötigter Schlüsselfähigkeiten.

(3) Schaffung der methodischen Grundlage und Erlangung der praktischen Fähigkeit zur quantitativen und qualitativen Bemessung des benötigten Absicherungsniveaus auf Basis eines wissenschaftlich fundierten und allgemein anerkannten Verfahrens für die Fälle, die nicht von der VSA bzw. anwendbaren internationalen Standards (z.B.: STANAG, Common Criteria) abgedeckt sind. Der für dieses Absicherungsniveau erforderliche Aufwand muss auch in Relation zu der damit erzielten Vertrauenswürdigkeit, Verfahrensstärke und Wirksamkeit gesetzt werden können. Dies bedingt auch die weitere Präzisierung der nationalen Forderungen hins. der Schlüsselfähigkeiten im Kontext Cyber/IT und deren Realisierung im nationalen und internationalen Kontext.

(4) Detailbetrachtung der identifizierten spezifischen technischen Handlungsfelder (z.B. Ausbau Kompetenz und Fähigkeit bzgl. vertrauenswürdiger Hardware, Software und prägbarer Zukunftstechnologien) mit dem Ziel der Ableitung fachlicher Schritte. Dies kann auch möglicherweise notwendige Standardisierungen und Regelungen wie auch beratende Empfehlungen hinsichtlich zielführender Maßnahmen als Grundlage für eine mögliche Umsetzung beinhalten.

(5) Detailbetrachtung der identifizierten querschnittlichen Handlungsfelder wie der durchgängigen Absicherung von Lieferketten und der Lebenszyklusunterstützung hinsichtlich Cyber/IT mit dem Ziel der Ableitung fachlicher Schritte. Dies kann auch möglicherweise notwendige Standardisierungen und Regelungen wie auch beratende Empfehlungen hinsichtlich zielführender Maßnahmen als Grundlage für eine mögliche Umsetzung beinhalten.

(6) Detailbetrachtung von bereits laufenden Forschungs- und Entwicklungsvorhaben im internationalen Umfeld mit Bezug zu den identifizierten Handlungsfeldern hinsichtlich der Nutzbarkeit (siehe auch Abschnitt 5.4).

(7) Detailbetrachtung der Möglichkeiten und Handlungsalternativen zur initialen Etablierung einer Austauschplattform zwischen GB BMVg und den Industriepartnern (nationalen bzw. kritischen Liefer- und Versorgungskette) zum Austausch von Informationen hins.

Erkenntnissen zu sicherheitskritischen Schwachstellen in Produkten/Technologien. Der Umgang mit diesen Informationen/Erkenntnissen soll die Optimierung des Risikomanagements und eine nachhaltige Verbesserung des Absicherungsniveaus unter Beachtung der klaren Trennung zwischen Auftraggeber und Auftragnehmer ermöglichen.

(8) Detailbetrachtung und Initiierung Umsetzung der kurz- und mittelfristigen Verbesserungsvorschläge und Maßnahmen (siehe auch Abschnitte 5.3.1, 5.3.2 und 5.1.3).

5.3.1 Schnittstelle Projekt/Rüstung

Beitrag BMVg (BAAINBw I4.1 – „HaFIS Projektelemente/Facharbeitsgruppen“)

"Basisdokumentation eines Projektleiters/einer Projektleiterin zum Thema 'vertrauenswürdige IT'"
In den Projekten der Bundeswehr wird dem Grunde nach bereits heute eine entsprechende Dokumentation beauftragt und als Entscheidungsgrundlage genutzt. Je nach Ausbildungsstand und Erfahrungshorizont der handelnden Personen können hier aber Unterschiede in der Effizienz der konkreten Umsetzung nicht ausgeschlossen werden. In der Aus- und Fortbildung sollte sowohl auf Seiten der Industrie als auch auf Seiten der Bundeswehr der Blick für die Berücksichtigung des Themas Informationssicherheit auch in der Managementdokumentation geschärft werden.

"Schnittstelle Projektleiter/Projektleiterin zur Industrie"
Analog zu dem IT-SiBe Projekt sollte es auch auf Auftragnehmerseite immer einen der Projektleitung direkt zugeordneten IT-SiBe geben, der die Bundeswehrvorschriften beherrscht und für eine reibungslose Nachweiserbringung sorgt.

Darüber hinaus muss es für den Auftragnehmer schnelle Wege zum Informationsaustausch mit den Experten der Bundeswehr geben, um z.B. bei Bekanntwerden von Schwachstellen sofort reagieren zu können. Durch die Bundeswehr sollte auch ein schneller Austausch mit den Experten an der WTD 81 und im ZCSBw ermöglicht werden.
Zukünftige Zusammenarbeitsmodelle sollten eine offene Kommunikation berücksichtigen und formalisieren.

"Sichere Lieferketten - Verständnis Projektleiter/Projektleiterin/Industrie"
Der eingeschlagene Weg sollte weiterverfolgt werden und die Forschung und Entwicklung noch weiter intensiviert werden. Europa ist bereits heute bekannt für seine Experten im Bereich Informationssicherheit. Die Industrie ist gefragt, dieses zu erhalten und auszubauen. Arbeitsplätze müssen konkurrenzlos attraktiv sein, um ein Abwerben unserer Experten durch Unternehmen beispielsweise aus dem Silicon Valley zu verhindern.

5.3.2 IT-*Sicherheitsüberprüfung* von IT-Systemen und Zulassung für den VS-Betrieb

Beitrag BMVg (WTD 81 – GF 210 – PZITSichhBw)

Um die „Vision“ (Kapitel 5.1.2 für den Bereich der IT-Sicherheitsüberprüfungen sowie die Zulassung zum VS-Betrieb zu ermöglichen ist der zugehörige Handlungsbedarf (Kapitel 0) notwendig.

5.3.3 Akkreditierung

Beitrag BMVg (DEUmilSAA)

In Bezug auf die DEUmilSAA sind bereits alle Maßnahmen veranlasst und auf der Zeitachse ausgeplant, um die diesbezüglich in Kapitel 5.1.3 artikulierte Vision plangemäß anhand der Maßnahmen gemäß Kapitel 0 umzusetzen. Weitere noch zu veranlassende Maßnahmen bestehen derzeit nicht.

5.3.4 Moving Target Defense (MTD)

Beitrag BMVg (UniBwM FI CODE)

MTD ist ein neues und bahnbrechendes Paradigma, das auf Polymorphie basiert. Im Rahmen der Netzsicherheit können hier die Parameter und die Konfiguration der Netze und Systeme dynamisch verändert werden, wodurch es für den Angreifer schwieriger und komplexer wird diese zu attackieren. Diese Netze müssen weiterhin einem Security-Monitoring unterzogen werden. SDN kann hierbei einen enormen Beitrag leisten. Hochsichere IT-Umgebungen und auch militärische Netze können mit passenden MTD-Techniken effektiver gegen Angriffe abgesichert werden, auch kann im Falle eines erfolgreichen Eindringens in ein militärisches Netz die laterale Ausbreitung durch ein dynamisches Netzlayout eingedämmt oder verhindert werden.

Basierend auf der Technologie von SDN ergeben sich aber auch Möglichkeiten für dynamische Netzstrukturen. Durch die Trennung der Netzfunktionalität in SDN-Controller und SDN-Switches ermöglicht SDN die Kontrolle über die Datenflows und damit die Möglichkeit der Entwicklung einer sicheren, vertrauenswürdigen und resilienten Netzinfrastruktur. Eine sichere und vertrauenswürdige Kommunikationsinfrastruktur ist sowohl für die militärische als auch zivile Nutzung essentiell. Daher sind das Anwendungspotential und die Relevanz für die Bundeswehr sehr hoch.

Aufbauend auf der Generierung von Auswahlhilfen von MTD-Technologien zur Härtung hochsicherer Netze und Systeme sollten MTD-Technologien lokal getestet und evaluiert werden. Hierbei sollen wissenschaftliche Fragestellungen, wie Vertrauen, analysiert werden. Zusätzlich müssen Taktiken und Strategien entworfen werden, um zukünftigen Angriffen, gerade auf hochsichere Netzinfrastrukturen, effektiv entgegenwirken zu können.

Das Ziel ist es ein dynamisches Netz mit passenden Strategien und Taktiken zu haben, um es Angreifern möglichst schwer zu machen. Durch die zentrale Kontrolle, Orchestrierung des MTD inklusive dynamische situative Abläufe, insbesondere bei Angriffen, mit dem richtigen Timing, aber zugleich auch möglichst automatisierte Wartung der Systeme soll die Angriffsfläche möglichst klein gehalten werden.

5.4 Analyse/Einordnung in internationalen Kontext

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

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.

Hinsichtlich der Europäischen Entwicklung sicherer Hardware hinsichtlich High Performance Computing ist z.B. exemplarisch das EU Vorhaben EuroHPC oder auch die Open Risc-V Initiative zu nennen:

European High Performance Joint Undertaking

Beim European High-Perfomance Computing Joint Undertaking (EuroHPC JU) handelt es sich um ein im Jahre 2017 initiiertes Programm der EU, in dem europäische Ressourcen zur Entwicklung eines europäischen Portfolios von High-Performance-Computern gebündelt werden. Ziel von EuroHPC ist die Ermöglichung weltmarktfähiger europäischer vertrauenswürdiger High Performance Computing Technologie unter Nutzung offener Standards, um so eine Alternative zu asiatischen und amerikanischen Produkten bieten zu können. Hierbei ist die Absicht, die gesamte Wertschöpfungskette vertrauenswürdig abzudecken. Typische Anwendungsgebiete sind sowohl die Verwendung in der Industrie (Massenmarkt, z.B. Embedded Edge Computing in Fahrzeuge, HPC-Plattformen für „klassische“ Big Data & Analytics Anwendungen) als auch die Nutzung durch BOS der Mitgliedsstaaten im Rahmen hoheitlicher Aufgaben. Teil des Programms ist die European Processor Initiative (ePI), welche die notwendigen Mikroprozessoren und damit im Zusammenhang stehenden HW- und SW-Elemente umfasst, d.h. Spezifikation, Design und Realisierung abdeckt (siehe 6.2.15 und 16).

Open RISC-V Initiative

Ausgehend von den Mitgliedern der RISC-V Foundation wurde die Initiative ins Leben gerufen, um aufbauend auf der ohnehin schon offenen RISC-V Prozessor-Architektur neben den kommerziellen Implementierungen von Systemplattformen und Softwareanteilen auch weitere offene Implementierungen (sowohl von Software als auch Silikon) und damit ein höheres Niveau an Sicherheit und Transparenz zu ermöglichen. Auf diesem Weg soll den Mitgliedern ermöglicht werden mittels RISC-V basierter Technologie Lösungen für Anwendungsfälle wie z.B. Sicherheitsanwendungen, Beschleunigung von AR/VR, Simulation etc. anbieten zu können. Ferner soll so auch die Möglichkeit zur Evaluierung und Verifikation auf tiefer technischer Ebene verbessert werden (siehe 6.2.17).

Weiterhin finden Aktivitäten unter dem Dach der Europäischen Verteidigungsagentur (EDA) und NATO statt, auf die im Rahmen dieses Dokuments einstufungsbedingt nicht im Detail eingegangen werden kann. Exemplarisch seien hier folgende Aktivitäten genannt:

Military multi-Agent System For APT Detection (MASFAD)

Hierbei liegt eine von der EDA finanzierte und inzwischen abgeschlossene 18-monatige Studie (ca. Januar 2014 bis Juli 2015) zur Entwicklung eines Demonstrators zur Erkennung von Advanced Persistent Threats (APT) vor (siehe 6.2.18). Diese fand in einem Konsortium mit der niederländischen Organisation für angewandte naturwissenschaftliche Forschung Toegepast Natuurwetenschappelijk Onderzoek (TNO) mit dem Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) statt. Hauptauftragnehmer war die Royal Military Academy (RMA).

Malware Information Sharing Platform (MISP)

Bei MISP handelt es sich um eine von der EDA co-finanzierte Open Source Plattform (siehe 6.2.19), mit der

- Anzeichen für eine Kompromittierung bei gezielten Angriffen,
- Informationen über Schwachstellen und deren mögliche Ausnutzung (z.B. Finanzbetrug) und
- Bedrohungsanalysen

gesammelt, geteilt, gespeichert und korreliert werden können.

Artikel "NATO and EU discuss defense against hybrid warfare" vom 14.03.2019

Gegenstand des Artikels (siehe 6.2.20) ist ein Gespräch der stellvertretenden Generalsekretärin Rose Gottemoeller mit dem britischen EU-Kommissar für die Sicherheitsunion, Sir Julian King, vom 14.03.2019 über die engere Zusammenarbeit von NATO und EU zur Abwehr hybrider Kriegsführung.

Der Artikel konstatiert bereits eine enge Zusammenarbeit von NATO und EU in der Domäne Cyber z.B. durch Übungen und den Echtzeitinformationsaustausch über Cyber-Bedrohungen. Er führt darüber hinaus aus, dass breit angelegte Gespräche geführt wurden, die weiter verbesserte Warn- und Informationsaustauschsysteme sowie die *„supply chain security of IT products"* betreffen.

Im Rahmen der Prüfung weiterer Aktivitäten (z.B. auf der Basis der im Abschnitt 5.3 empfohlenen Maßnahmen bzw. der Ausführungen des Kapitel 3) sollten auch die bereits laufenden internationalen Aktivitäten im Kontext detailliert hinsichtlich der Nutzbarkeit analysiert und ggf. entsprechend eingebracht werden.

5.5 Ausblick

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

Der Gesprächskreis 4 „Innovation Cyber/IT“ bewirkt unter anderem auf strategischer Ebene einen kontinuierlichen Abgleich der aktuellen Trends aus Sicht der Industrie, vertreten durch BDSV/Bitkom, mit den im Verteidigungsressort gesetzten fähigkeitsbezogenen Schwerpunkten im Bereich Cyber/IT. Die Entscheidung über die Ausrichtung wehrtechnischer F&T sowie die Initiierung und Steuerung konkreter Maßnahmen richtet sich ausschließlich am Bedarf der Bundeswehr aus und wird vollumfänglich von diesem gesteuert.

Die fähigkeitsbezogenen Schwerpunkte im Bereich Cyber/IT 2018/2019 wurden zuletzt gemäß Vereinbarung auf der vierten Sitzung des Gesprächskreises 4 vom 19.03.2019 aktualisiert und sind als strategischer, übergeordneter und unverbindlicher Gesamt-Ausblick zu verstehen. Dieses Dokument greift diesen hiermit mit der aktualisierten Übersicht "Fähigkeitsbezogene Schwerpunkte für die Ausrichtung wehrtechnischer F&T im Bereich Cyber/IT 2019/2020" gemäß nachfolgender Abbildung auf.

Vertrauenswürdige IT leistet einen Beitrag für jedes der dargestellten Anwendungsfelder, da sie als Enabler von jeglicher mit IT bereitgestellter Fähigkeiten zu verstehen ist.

Abbildung 4: Fähigkeitsbezogene Schwerpunkte für die Ausrichtung wehrtechn. F&T im Bereich Cyber/IT 2019/2020

Für eine Bewertung und Entscheidung über weitere gemeinsame Aktivitäten und Untersuchungen ist es daher zweckmäßig, die Übereinstimmungen der Themen in den einzelnen Anwendungsfeldern entsprechend zu berücksichtigen.

6 Anhang

6.1 Urheberschaft

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 sowie die Compliance relevante Herkunftstransparenz durch zu Beginn eines Abschnittes in kursiver Schrift ausgewiesene Urheberschaft und Verantwortlichkeit hingewiesen. Diese wird im Rahmen dieses Kapitels nochmals gesammelt zusammengefasst dargestellt:

Gemeinsame Kapitel/Abschnitte von BMVg und den Industrieverbänden sind:

- 1 Vorwort
- 2 Zielsetzung des Expertenkreises
- 3 Ergebnisse im Überblick
- 5 Handlungsempfehlung
- 5.1 Entwicklung „Vision“
- 5.2 Zuordnung Handlungsbedarf
- 5.3 Empfohlene Maßnahmen
- 5.4 Analyse/Einordnung in internationalen Kontext
- 5.5 Ausblick

BMVg bzw. GB BMVg verantwortet folgende Kapitel/Abschnitte:

- 4.1.2 Software am Beispiel des Heartbleed-Bug
- 4.2 Randbedingungen der im GB BMVg und im kommerziellen Massenmarkt eingesetzten IT-Produkte
- 4.3.11 Schnittstelle Projekt/Rüstung
- 4.3.12 IT-Sicherheitsüberprüfung von IT-Systemen und Zulassung für den VS-Betrieb
- 4.3.13 Akkreditierung von IT-Systemen
- 4.2.14.1 Moving Target Defence (MTD)
- 5.1.1 Schnittstelle Projekt/Rüstung
- 5.1.2 IT-Sicherheitsüberprüfung von IT-Systemen und Zulassung für den VS-Betrieb
- 5.1.3 Akkreditierung
- 5.1.4 Moving Target Defence (MTD)
- 5.2.1 Schnittstelle Projekt/Rüstung
- 5.2.2 IT-Sicherheitsüberprüfung von IT-Systemen und Zulassung für den VS-Betrieb
- 5.2.3 Akkreditierung
- 5.2.4 Moving Target Defence (MTD)
- 5.3.1 Schnittstelle Projekt/Rüstung
- 5.3.2 IT-Sicherheitsüberprüfung von IT-Systemen und Zulassung für den VS-Betrieb
- 5.3.3 Akkreditierung
- 5.3.4 Moving Target Defense (MTD)

Die Industrieverbände BDSV und Bitkom verantworten folgende Kapitel/Abschnitte:

- 4.1.1 Hardware am Beispiel von MELTDOWN und SPECTRE
- 4.1.3 Hardwarenahe Software/Firmware am Beispiel des Exploits BadUSB
- 4.3.1 Embedded IT
- 4.3.2 IT-Komponenten Land-, Luft- und Seefahrzeuge

- 4.3.3 IT-Bausteine und -funktionen in IT-Sicherheitsprodukten inkl. HW für das mil. Umfeld – Fokus sichere Netzwerkschnittstelle
- 4.3.4 IT-Bausteine und -funktionen in IT-Sicherheitsprodukten inkl. HW für das mil. Umfeld – Fokus Verschlüsselung
- 4.3.5 IT-Bausteine und -funktionen in IT-Sicherheitsprodukten inkl. HW für das mil. Umfeld – Fokus Security Gateways
- 4.3.6 Absicherung potentiell unsicherer Betriebssysteme und Laufzeitumgebungen
- 4.3.7 Absicherung Middleware
- 4.3.8 Realisierung sicherer Führungsinformationssysteme (C4ISR)
- 4.3.9 Sicherer Betrieb komplexer IT-Umgebungen
- 4.3.10 Absicherung der Lieferketten
- 4.3.14 Zukünftige Anwendungsgebiete
- 4.4 Einordnung in IT-Architektur und Wertschöpfungskette
- 4.5 Bewertung Beitrags- und Zukunftsfähigkeit

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

- Atos Information Technology GmbH
- Airbus Defence and Space GmbH
- genua GmbH
- Hensoldt Sensors GmbH
- INFODAS Gesellschaft für Systementwicklung und Informationsverarbeitung mbH
- itWatch GmbH
- Rheinmetall Electronics GmbH
- Rohde & Schwarz GmbH & Co. KG
- secunet Security Networks AG
- SAP Deutschland SE & Co. KG
- Software AG
- T-Systems International GmbH
- Utimaco IS GmbH

6.2 Referenzen und Quellen

1. Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr vom 13. Juli 2016; siehe https://www.bmvg.de/de/themen/weissbuch
2. https://www.heise.de/newsticker/meldung/Wie-sich-Spectre-und-Meltdown-auf-kuenftige-CPU-Designs-auswirken-4142229.html
3. http://www.heise.de/security/artikel/So-funktioniert-der-Heartbleed-Exploit-2168010.html vom 10.04.2014
4. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Heartbleed_Bug_16042014.html
5. Ramon Mörl, Andreas Koke: BadUSB, aktuelle USB Exploits und Schutzmechanismen, Tagungsband zum 14. Deutschen IT-Sicherheitskongress, Bundesamt für Sicherheit in der Informationstechnik, 2015, ISBN 978-3-922746-94-2, S. 289
6. www.fireeye.com/blog/de-threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
7. DIN EN 60529; VDE 0470-1:2014-09 Schutzarten durch Gehäuse (IP-Code) (IEC 60529:1989 + A1:1999 + A2:2013); Deutsche Fassung EN 60529:1991 + A1:2000 + A2:2013
8. https://www.adz.de/ip-schutzklassen-uebersicht.html?file=tl_files/downloads/de/sonstiges/Schutzarten_Schutzarten_nach_DINEN60529.pdf
9. DEPARTMENT OF DEFENSE - TEST METHOD STANDARD - ENVIRONMENTAL ENGINEERING CONSIDERATIONS AND LABORATORY TESTS“, Version MIL-STD-810G vom 31. Oktober 2008 öffentlich verfügbar unter https://www.atec.army.mil/publications/Mil-Std-810G/Mil-Std-810G.pdf
10. Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz – SÜG vom 20. April 1994 (BGBl. I S. 867), das zuletzt durch Artikel 4 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2732) geändert worden ist)
11. Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) vom 31. März 2006 in der Fassung vom 26. April 2010 (GMBl 2010, S. 846)
12. https://m.heise.de/security/meldung/Hunderttausende-Infineon-Sicherheits-Chips-weisen-RSA-Schwachstelle-auf-3864691.html
13. VS-Anforderungsprofile BSI: https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/ZugelasseneProdukte/VS-Anforderungsprofile/VS-Anforderungsprofile_node.html
14. https://open.sourcemap.com/maps/57d0d127dd3780d6272b3f8c
15. https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking
16. https://ec.europa.eu/digital-single-market/en/news/european-processor-initiative-consortium-develop-europes-microprocessors-future-supercomputers
17. https://riscv.org/
18. http://www.sic.rma.ac.be/research/RUAI/proj363.html abgerufen am 30. April 2019
19. https://www.misp-project.org/ abgerufen am 30.04.2019
20. https://www.nato.int/cps/en/natohq/news_164603.htm?selectedLocale=en abgerufen am 30.04.2019
21. Strategiepapier der Bundesregierung zur Stärkung der Verteidigungsindustrie in Deutschland - Berlin, 8. Juli 2015; https://www.bmwi.de/Redaktion/DE/Artikel/Branchenfokus/Industrie/branchenfokus-sicherheits-und-verteidigungsindustrie.html

22. Jerome H. Saltzer and Michael D. Schroeder. The Protection of Information in Computer Systems. Proceedings of the IEEE, 63(9), September 1975.
23. J. Liedtke. On mu-kernel construction. In Proceedings of the 15th ACM Symposium on Operating Systems Principles, Dezember 1995.
24. H. Poschmann, Gefälschte Bauteile, Elektroniknet.de/Halbleiter, 2012, https://www.elektroniknet.de/halbleiter/gefaehrliche-zuverlaessigkeits-und-funktionskiller-91915.html
25. https://de.wikipedia.org/wiki/Rowhammer
26. https://de.wikipedia.org/wiki/Schutzart

6.3 Abkürzungsverzeichnis

ADIC	Agentur für Innovation in der Cybersicherheit (Cyberagentur)
APT	Advanced Persistent Threat
AR	Augmented Reality
BAAINBw	Bundesamt für Ausrüstung Informationstechnik und Nutzung der Bundeswehr
BAMAD	Bundesamt für den Militärischen Abschirmdienst
BDSV e.V.	Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V.
Bitkom e.V.	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BMVg	Bundesministerium der Verteidigung
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BSI	Bundesamt für Sicherheit in der Informationstechnik
Bw	Bundeswehr
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CC	Common Criteria
CERT	Computer Emergency Response Center
CIR	Cyber- und Informationsraum
CISO	Chief Information Officer
CIT	Cyber/IT
COTS	Commercial-Off-The-Shelf
CPM	Customer Product Management
CPU	Central Processing Unit
CSOC	Cybersecurity Operations Centre
DEUmilSAA	Deutsche militärische Security Accreditation Authority
DIN	Deutsches Institut für Normung
DLBO	Digitalisierung landbasierter Operationen
EDA	European Defence Agency
eIDAS	electronic Identification, Authentication and trust Services
EK	Expertenkreis
EN	Europäische Norm
ePI	European Processor Initiative
ESARIS	Enterprise Security Architecture für Reliable IT Services
EU	Europäische Union
FIPS	Federal Information Processing Standard
FKIE	Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie
FOC	Final Operational Capability
FPGA	Field Programmable Gate Array
FüInfoSys	Führungsinformationssystem
F&T	Forschung und Technologie
GB	Geschäftsbereich
GF	Geschäftsfeld
GK	Gesprächskreis
GMBl	Gemeinsames Ministerialblatt
GPS	Global Positioning System
HD	High Definition
HSM	Hardware Security Module
HW	Hardware

ICIT	Innovation Cyber/IT
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFF	Identification Friend or Foe
IKT	Informations- und Kommunikationstechnik
IOC	Initial Operational Capability
IoE	Internet of Everything
IP	Internet Protocol
IPSec	Internet Protocol Security
IPT	Integriertes Projektteam
IRTF	Internet Research Task Force
ISO	International Organization for Standardization
IT	Informationstechnologie
JU	Joint Undertaking
Kdo	Kommando
MASFAD	Military multi-Agent System For APT Detection
mil	militärisch
MTD	Moving Target Detection
M&S	Modellbildung und SImulation
NATO	North Atlantic Treaty Organization
NetOpFü	vernetzte Operationsführung
NIST	National Institute of Standards and Technology
PCBA	Printed Circuit Board Assembly
PKI	Public Key Infrastructure
PRNG	Pseudo Random Noise Generator
PZITSichhBw	Prüfzentrum für IT-Sicherheit in der Bundeswehr
RFC	Request for Comment
RISC	Reduced Instruction Set Computer
RMA	Royal Military Academy
RSA	Rivest Shamir Adleman
SAA	Security Accreditation Authority
SDN	Software Defined Networking
SMB	Server Message Block
SoC	System on a Chip
SOC	Security Operation Center
SSID	strategische Steuerung des Industriedialoges
SSL	Secure Socket Layer
StS	Staatssekretär
Sts'in	Staatssekretärin
SÜG	Sicherheitsüberprüfungsgesetz
SW	Software
TCP	Transmission Control Protocol
TEMPEST	Temporary Emanation of Spurious Transmission
TLS	Transport Layer Security
TNO	Toegepast Natuurwetenschappelijk Onderzoek
TPM	Trusted Platform Module
USB	Universal Serial Bus

VPN	Virtual Private Network
VR	Virtual Reality
VS	Verschlusssache
VSA	Verschlusssachenanweisung
WTD	Wehrtechnische Dienststelle
XML	eXtensible Markup Language
ZCSBw	Zentrum für Cybersicherheit in der Bundeswehr