Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS

Mai 2026

Technologiebetrachtung

Anforderungen und Empfehlungen für eine sichere verteilte Verarbeitung schützenswerter Informationen

1 Einführung und Problemstellung

In jedem betrieblichen Umfeld gibt es Informationen, die aus verschiedenen Gründen schützenswert sind (beispielsweise, weil sie klassifiziert sind). Dabei kann sich die Schutzwürdigkeit auf verschiedene Sicherheitsziele beziehen, wie z. B. die Vertraulichkeit, die Authentizität und/oder die Verfügbarkeit. Die Schutzwürdigkeit kann die ganze Lebensdauer einer Information umfassen. Insbesondere muss die Information während ihrer Speicherung, Verarbeitung[1] und Übertragung durchgehend und in Bezug auf alle relevanten Sicherheitsziele geschützt sein. Während es für die sichere Speicherung und Übertragung praxistaugliche technologische Lösungen gibt, die auch flächendeckend eingesetzt werden können, ist das bei der Verarbeitung nicht immer der Fall. Hier gibt es zwar Lösungsansätze, allerdings sind diese Ansätze nicht für den flächendeckenden Einsatz gedacht bzw. dafür (noch) nicht geeignet. Das gilt umso mehr, je stärker die Verarbeitung verteilt und durch verschiedene Parteien stattfinden muss, wie z. B. im Rahmen von Kommunikations- und Kollaborationsplattformen, die es in verschiedensten Formen und Ausprägungen gibt.[2] Neben dem asynchronen Austausch von Informationen z. B. mittels elektronischer Nachrichten (E-Mail) unterstützen solche Plattformen meist auch den synchronen Informationsaustausch im Rahmen von Sprach- und/oder

[1] Obwohl die Begriffe «Bearbeitung» und «Verarbeitung» im Umgang mit Informationen und Daten oft synonym verwendet werden, gibt es doch einen subtilen Bedeutungsunterschied: Eine «Verarbeitung» bezieht sich meist auf das automatisierte Zusammentragen und Auswerten sowie Umwandeln von Daten in nützliche Informationen (wie z. B. auch der früher oft verwendete Begriff einer «elektronischen Datenverarbeitung» suggeriert). Mit einer «Bearbeitung» ist eher das aktive Ändern, Korrigieren oder Anpassen von konkreten Datensätzen gemeint. Allgemein bedeutet «bearbeiten» eher, etwas zu ändern oder eine Aufgabe zu lösen, während sich «verarbeiten» mehr auf das Umwandeln von Materialien (z. B. Holzverarbeitung) oder Informationen bezieht. Entsprechend wird in diesem Dokument meist der Begriff «Verarbeitung» verwendet. Nur wenn es darum geht, konkrete Daten oder Datensätze zu ändern, korrigieren oder anzupassen, wird von einer «Bearbeitung» gesprochen.

[2] Beispiele von umfassenden Kommunikations- und Kollaborationsplattformen sind Microsoft Teams, Google Workspace und Nextcloud, während Slack, Confluence, SharePoint und Miro exemplarische Plattformen mit eher spezifischen Funktionalitäten sind.

Videokommunikation. Aus diesen unterschiedlichen Kommunikationsmöglichkeiten ergeben sich neue und zum Teil auch unterschiedliche Anforderungen an die Plattformen, die es zu berücksichtigen gilt.

In dieser Technologiebetrachtung werden die Anforderungen an eine sichere verteilte Verarbeitung von schützenswerten Informationen zusammengestellt, eine geeignete Zielarchitektur vorgeschlagen, und Empfehlungen für entsprechende Entwicklungs- und Beschaffungsprojekte abgegeben. Aufgrund der erwähnten Verfügbarkeit von technologischen Lösungen für die sichere Speicherung und Übertragung von schützenswerten Informationen werden diese Themen nicht bzw. nur am Rande erwähnt.

2 Anforderungen

Für die sichere verteilte Verarbeitung schützenswerter Informationen gibt es strategische, technische und organisatorische Anforderungen, die im Folgenden zusammengestellt und kurz skizziert sind.

2.1 Strategische Anforderungen (S)

S-1 Datensouveränität

Die Souveränität hinsichtlich der schützenswerten Informationen muss sichergestellt und gewährleistet sein, d. h. die Organisation oder das Unternehmen muss jederzeit die alleinige Hoheit und Kontrolle über ihre Daten haben.[3] Die IT-Infrastruktur, die zur Speicherung, Verarbeitung und Übertragung dieser Daten eingesetzt wird, muss diesem Anspruch Rechnung tragen.

S-2 Einfachheit und Überprüfbarkeit

Die sichere verteilte Verarbeitung schützenswerter Informationen muss auf eine einfache und überprüfbare (d. h. nachvollziehbare) Art und Weise erfolgen bzw. möglich sein.[4] Die Überprüfbarkeit bedingt unter anderem auch, dass für die Verarbeitung möglichst offene Protokolle und Systeme eingesetzt werden, die idealerweise mit quelloffener Software umgesetzt sind.

2.2 Technische Anforderungen (T)

T-1 Kryptografische Absicherung

Schützenswerte Informationen müssen mithilfe geeigneter kryptografischer Verfahren während der ganzen Lebensdauer und gegenüber allen Parteien durchgehend geschützt sein.[5] Die dazu erforderlichen kryptografischen Schlüssel müssen im Rahmen einer ausschliesslich von der Organisation oder dem Unternehmen

---

[3] Bei der Datensouveränität gibt es mindestens zwei verschiedene Aspekte, die gleichermassen zu berücksichtigen sind: Einerseits geht es um die Vertraulichkeit und Integrität der schützenswerten Informationen, andererseits um die Verfügbarkeit und den Zugang zu diesen Informationen.

[4] Dazu gehört auch, dass Komponenten, die aus irgendwelchen Gründen nicht überprüft werden können, transparent ausgewiesen sind.

[5] Für die Konzipierung von kryptografischen Verfahren ist zu berücksichtigen, dass wo immer möglich symmetrische Kryptografie eingesetzt werden sollte. Asymmetrische Kryptografie sollte nur dort zum Einsatz kommen, wo sie mangels Alternativen erforderlich ist (d. h. insbesondere für den Schlüsselaustausch in grossen Systemen und/oder für digitale Signaturen). Die Sicherheit asymmetrischer Kryptografie ist grundsätzlich mehr und auch retrospektiv wirkenden Bedrohungen ausgesetzt und ist deshalb schwieriger über eine längere Zeitspanne zu gewährleisten. Beispielsweise werden asymmetrisch verschlüsselte Daten heute abgegriffen und können in Zukunft möglicherweise mit einem Quantencomputer entschlüsselt werden können. In diesem Zusammenhang spricht man von einem sogenannten «Harvest Now, Decrypt Later» (HNDL)-Angriff.

kontrollierten Schlüsselverwaltung[6] bereitgestellt werden und während ihrer ganzen Lebensdauer geschützt sein. Dabei darf es keine Generalschlüssel mit Zugriff auf alle Informationen geben. Stattdessen müssen die Schlüssel für die Ver- und Entschlüsselung möglichst kleiner Datenbestände ausgelegt sein.[7] Falls für Notfälle «Recovery Keys» erforderlich sind, dürfen diese Schlüssel nur dazu dienen, dass die jeweiligen Schlüsselbesitzer die Informationen entschlüsseln können. Zudem müssen Prozesse definiert und dokumentiert sein, wie diese Schlüssel im Bedarfsfall freigegeben und benutzt werden dürfen.[8]

T-2 Authentifikation

Personen und Prozesse, die auf schützenswerte Informationen zugreifen bzw. diese verarbeiten können, müssen zuverlässig identifiziert und stark authentifiziert sein.

T-3 Zugriffskontrolle

Der Zugriff und die Verarbeitung von schützenswerten Informationen müssen auf explizit berechtigte[9] Personen und Prozesse, sowie im Bedarfsfall auch auf zugelassene Geräte, geografische Regionen, Gebiete und Zonen in Abhängigkeit der Zeit eingeschränkt werden können. Zugriffe und Zugriffsversuche müssen lückenlos protokolliert werden. Dabei ist sicherzustellen, dass Protokolle nicht unberechtigterweise ausgelesen oder manipuliert werden können. Neben diesen Aufzeichnungen müssen auch die umgesetzten Zugriffskontrollmechanismen wirksam vor Manipulation geschützt sein.

T-4 Verwendungskontrolle

Für schützenswerte Informationen muss definiert und klar deklariert sein, welche Verwendungszwecke (z. B. Bearbeitung, Übersetzung, Teilen usw.) zulässig sind. Diese Deklarationen müssen für Personen einfach ersichtlich und intuitiv verständlich sein (z. B. mit Hilfe von sichtbaren digitalen Wasserzeichen) sowie für automatisierte Prozesse maschinell interpretierbar sein. Zudem dürfen die Informationen nur für solche Verarbeitungen verfügbar und zugänglich sein. Werden Informationen unzulässig verwendet, muss die Verwendung in entsprechenden Aufzeichnungen auf eine möglichst nicht abstreitbare Art und Weise ersichtlich sein bzw. aus solchen hervorgehen.

2.3 Organisatorische Anforderungen (O)

O-1 Bearbeitungsrichtlinien und Supportprozesse

Für alle Aufgaben, welche die verteilte Verarbeitung schützenswerter Informationen betreffen, müssen Bearbeitungsrichtlinien[10] und Supportprozesse (z. B. für das Berechtigungsmanagement, die Ausbildung die Schulung usw.) sowie entsprechende Zuständigkeiten und Verantwortlichkeiten definiert sein.

---

[6] In jedem Sicherheitskonzept, in dem kryptografische Verfahren eingesetzt werden, stellt die Schlüsselverwaltung die Achillesferse dar. Entsprechend ist diesem Thema bei der Sicherheitskonzipierung eine grosse Beachtung zu schenken.

[7] Im Bereich der Datenkommunikation bedeutet das z. B., dass das eingesetzte kryptografische Protokoll sinnvollerweise «Forward Secrecy» und allenfalls auch «Post-Compromise Security» anbieten können muss.

[8] In diesem Prozess muss auch geklärt sein, wie mit einem «Recovery Key» nach seiner Verwendung umgegangen werden muss. Ausserdem musssichergestellt werden kann, dass er nicht kopiert und später missbraucht werden kann.

[9] Eine explizite Berechtigung kann z. B. sinnvollerweise in Form einer «Allow»-List erfolgen.

[10] Die Umsetzungsrichtlinien müssen verständlich formuliert sein und effizient umgesetzt werden können.

O-2 Organisation

Die Organisation oder das Unternehmen muss so aufgestellt und organisiert sein, dass sie die gemäss O-1 definierten Bearbeitungsrichtlinien und Supportprozesse umsetzen und jederzeit einhalten kann.

3 Zielarchitektur

Aufgrund der in Kapitel 2 zusammengestellten Anforderungen an eine sichere verteilte Verarbeitung schützenswerter Informationen wird in diesem Kapitel eine Zielarchitektur vorgeschlagen, die diesen Anforderungen möglichst gut entspricht bzw. diese möglichst umfassend abdecken kann. In dieser Architektur stellen die zur Verarbeitung der schützenswerten Informationen eingesetzten IT-Komponenten ein konsistentes und in sich geschlossenes Untersystem der gesamten IT-Infrastruktur der Organisation oder des Unternehmens dar. Dieses Untersystem umfasst auch die benutzerseitigen Geräte und Client-Systeme. Im Idealfall können die schützenswerten Informationen dieses Untersystem nicht bzw. nur auf kontrollierbare (und auch effektiv kontrollierte) Art und Weise verlassen.

Die Grundprämisse der Zielarchitektur besteht darin, dass schützenswerte Informationen permanent jeweils nur an einem Ort gehalten[11] und über kontrollierte und gesicherte Endgeräte und Kommunikationskanäle eingesehen und bearbeitet werden können. Sie können nicht nach Belieben kopiert und verteilt werden. Das gilt auch für die Aufzeichnung von synchroner Sprach- und/oder Videokommunikation, wobei die Kommunikation selbst sinnvollerweise Ende-zu-Ende (E2E) verschlüsselt[12] ist (E2E wird nachfolgend in diesem Kapitel noch vertiefter thematisiert). Entsprechend ist zwar die Verarbeitung über viele Endgeräte verteilt, die eigentliche Verteilung der schützenswerten Informationen ist aber eingeschränkt (d. h. schützenswerte Informationen werden jeweils nur an einem Ort gehalten, weil Kopien die Angriffsfläche nur vergrössern würden und deshalb möglichst vermieden werden sollten).

Gemäss dieser Grundprämisse muss es im Untersystem gut geschützte und authentifizierte Server-Systeme[13] geben, auf denen die schützenswerten Informationen gehalten und gegenüber anderen Systemen verfügbar gemacht werden. Um der Anforderung S-1 «Datensouveränität» zu entsprechen, müssen diese Systeme entweder selbst (d. h. «On Premises» bzw. in einem eigenen Rechenzentrum) betrieben werden oder es muss anderweitig sichergestellt sein, dass der Betreiber der Systeme die Informationen insbesondere während ihrer Verarbeitung nicht einsehen oder manipulieren kann.[14] Das ist eine grosse technische Herausforderung, die mit kryptografischen Verfahren im Bereich der voll homomorphen Verschlüsselung zwar angegangen aber noch nicht praxistauglich gelöst werden kann, weil die Leistungsfähigkeit der entsprechenden Verfahren noch zu gering ist.

---

[11] Dabei kann die Information auch dezentral auf einem Endgerät gehalten und anderen Endgeräten von dort aus verfügbar gemacht werden.

[12] Der Begriff der E2E-Verschlüsselung macht primär bei der Übertragung von Informationen Sinn. Bei der Speicherung macht E2E-Verschlüsselung nur dann Sinn, wenn man eine Partei als die zwei Enden einer Übertragung versteht, d. h. die Partei überträgt die Informationen in einen Speicher und empfängt sie zu einem späteren Zeitpunkt wieder aus dem Speicher. Bei der Verarbeitung von Informationen macht der Begriff keinen Sinn.

[13] Der Begriff «Server-System» bezieht sich hier auf die Funktion, schützenswerte Informationen halten und verfügbar machen zu können. Der Formfaktor ist dabei nicht relevant, so dass ein Smartphone in diesem Sinne ebenfalls ein Server-System darstellen kann. Dabei scheint die Gefahr einer Datenhaltung an nur einem Ort darin zu bestehen, dass dieser Ort bzw. das entsprechende Server-System ein grösseres Ziel für Angriffe darstellt. Dieses Argument muss aber relativiert werden, weil ein Angriff bei einer dezentralen Datenhaltung an jedem Ort stattfinden kann, und die effektive Gefahr damit eher grösser ist.

[14] Für die sichere Speicherung und Übertragung der Informationen gibt es praxistaugliche Lösungen (s. Kapitel 1)

Mit Confidential Computing [1] steht aber eine Technologie zur Verfügung, mit der hardwaremässig sichergestellt werden kann, dass ein nicht vertrauenswürdiger Betreiber die Informationen, die auf Server-Systemen verarbeitet werden, selbst nicht einsehen kann. Dies jedenfalls, solange man dem Hardware-Hersteller vertrauen kann. Wie jede Technologie ist aber auch Confidential Computing nicht frei von Schwachstellen und Verwundbarkeiten, so dass sie unter bestimmten Umständen und insbesondere unter Zuhilfenahme von physischen Zugriffsmöglichkeiten angegriffen werden kann und auch schon angegriffen worden ist. Blindes Vertrauen in die Sicherheitsangaben und -versprechen der Hersteller ist hier nicht zielführend und muss hinterfragt werden. Trotzdem können auf der Basis dieser Technologie Lösungen konzipiert werden, bei denen der Betrieb der Server-Systeme ausgelagert werden kann und nicht zwingend in einem eigenen Rechenzentrum stattfinden muss. Allerdings müssen die Nutzbarkeit und Adäquatheit dieser Technologie im Einzelfall geprüft und bestätigt werden.

Gemäss Anforderung T-1 «Kryptografische Absicherung» müssen schützenswerte Informationen während ihrer Speicherung und Übertragung kryptografisch so abgesichert sein, dass Einsichtnahmen und Manipulationen durch Dritte (einschliesslich der Betreiber der Server-Systeme) ausgeschlossen sind. Die entsprechenden Technologien stehen heute zur Verfügung, wobei die Schlüsselverwaltung im Sinne von «Control Your Own Key» (CYOK) oder «Hold Your Own Key» (HYOK) in der Verantwortung der Organisation oder des Unternehmens liegen muss.[15] Darüber hinaus kann die oben erwähnte Verarbeitung von Informationen, wenn sie nicht in einem eigenen physisch abgesicherten Perimeter (z. B. Rechenzentrum) erfolgt, wenigstens auf der Basis von Confidential Computing gegenüber dem Betreiber abgesichert sein. Selbstverständlich ist aber der Betrieb in einem eigenen Perimeter aus Sicherheitssicht besser und entsprechend zu bevorzugen.

Mit ebenfalls gut geschützten Endgeräten, die in diesem Zusammenhang Client-Systeme darstellen, dürfen authentifizierte Personen und Prozesse gemäss Anforderung T-2 «Authentifikation» über kontrollierte Kommunikationskanäle auf die Informationen zugreifen, d. h. diese einsehen und/oder bearbeiten.[16] Dabei erfolgt die Einsichtnahme oder Bearbeitung grundsätzlich auf dem Server-System, so dass ein Herunterladen auf das Client-System und eine lokale Verarbeitung auf dem Client-System im Idealfall vermieden werden kann. Mithilfe von Virtualisierungstechnologien (wie z. B. Sandboxen) kann die Sicherheit der Client-Systeme weiter gestärkt und verbessert bzw. eine Exfiltration von Informationen erschwert werden.

Selbstverständlich müssen auf dem Server-System gemäss Anforderungen T-3 «Zugriffskontrolle» und T-4 «Verwendungskontrolle» eine Zugriffs- und eine Verwendungskontrolle umgesetzt sein. Für Zugriffskontrollen gibt es viele standardmässig in die Betriebssysteme der Server-Systeme integrierte verfügbare Lösungen. Verwendungskontrollen sind in der Regel nicht standardmässig verfügbar und müssen im Einzelfall mit spezifischen Regelwerken umgesetzt werden. Beispielsweise kann hier zu verhindern versucht werden, dass schützenswerte Informationen aus einem Server-System bzw. aus dem Untersystem exfiltriert werden. Dazu können serverseitig Kommunikationskanäle deaktiviert oder mit Hilfe von «Data Leakage Prevention»-Systemen und/oder «Watermarking»- bzw. «Fingerprinting»-Technologien überwacht

---

[15] Im Gegensatz zu CYOK und HYOK hat der Betreiber bei «Bring Your Own Key» (BYOK), bei dem die Organisation oder das Unternehmen die Schlüssel dem Betreiber übergibt, und Schlüsseln, die direkt vom Betreiber verwaltet werden, selbst direkten Zugriff auf die Schlüssel und damit auch auf die unverschlüsselten Informationen. Das Gleiche gilt auch in den Fällen, bei denen der Betreiber aus Gründen der Gewährleistung der Verfügbarkeit neben den mit CYOK und HYOK verwalteten Schlüsseln noch eigene Schlüssel besitzt, mit denen die verschlüsselten Informationen auch entschlüsselt werden können. Diese direkten Zugriffsmöglichkeiten hat ein Betreiber bei CYOK und HYOK nicht.

[16] Man beachte, dass die verwendeten Authentifikationsverfahren kritisch sind und entsprechend stark sein müssen. Insbesondere müssen die Schlüssel an Personen gebunden und nicht einfach exportierbar sein. Zudem sind Authentisierungsprotokolle zu bevorzugen, die im Sinne von Anhang B von [2] Phishing-resistent sind.

und bestmöglich kontrolliert werden. Wenn eine Verhinderung der Vervielfältigung der Informationen mit einem System nicht zufriedenstellend möglich ist, muss sie durch physische Schutzmöglichkeiten ergänzt werden. In jedem Fall müssen die Informationen so gekennzeichnet sein, dass eine Benutzerin oder ein Benutzer selbst einfach die erlaubten Verwendungszwecke ableiten kann. Zudem muss bei der Protokollierung der Zugriffe und Verwendungen sichergestellt sein, dass aus den entsprechenden Protokollen keine direkten Rückschlüsse auf die effektiven Inhalte der schützenswerten Informationen gezogen werden können. Das kann über eine kryptographische Absicherung oder Tokenisierung erfolgen.

Wenn schützenswerte Informationen von einem Server-System an ein anderes System oder im Rahmen einer synchronen Sprach- und/oder Videokommunikation übertragen werden, ist eine E2E-Verschlüsselung erforderlich, d. h. es darf keine übergeordnete Stelle geben, die die dazu erforderlichen kryptografischen Schlüssel verteilt oder auf diese zugreifen kann. Die entsprechenden Kommunikationsprotokolle sind in Theorie und Praxis hinreichend gut bekannt (z. B. TLS, Signal, …). Das Zielsystem kann ein anderes Server-System oder ein Client-System sein. In jedem Fall muss dieses System aber gut geschützt und integraler Bestandteil des zu schützenden Untersystems sein.

Aus übergeordneter Sicht muss das Gesamtsystem, mit dem die Zielarchitektur umgesetzt wird und mit dem eine sichere verteilte Verarbeitung schützenswerter Informationen ermöglicht wird, gemäss Anforderung S-2 «Einfachheit und Überprüfbarkeit» möglichst einfach und überprüfbar gestaltet sein. Das wird durch den Einsatz von offenen Protokollen und Systemen sowie der Nutzung von quelloffener Software vereinfacht. Darüber hinaus muss gemäss den Anforderungen O-1 «Bearbeitungsrichtlinien und Supportprozesse» und O-2 «Organisation» klar sein, wie das System zu nutzen ist, wie die entsprechenden Zuständigkeiten und Verantwortlichkeiten definiert sind bzw. wie sie in der Organisation oder vom Unternehmen erteilt sind. Dabei muss es möglich sein, im Bedarfsfall auch weitergehende geografische und physische Einschränkungen vorzusehen. Auf der technischen Seite müssen Werkzeuge bereitgestellt werden, damit die organisatorischen Anforderungen möglichst einfach und automatisiert umgesetzt werden können.

4 Empfehlungen

Für Projekte, die auf die Entwicklung einer Lösung für die sichere verteilte Verarbeitung von schützenswerten Informationen abzielen, wird die in Kapitel 3 skizzierte Zielarchitektur empfohlen. Grundsätzlich müssen dazu schützenswerte Informationen auf speziell geschützten Server-Systemen gehalten und über gesicherte Endgeräte eingesehen und bearbeitet werden. Eine Verteilung der Informationen darf nur in begründeten Fällen (z. B. im Rahmen synchroner Kommunikationsbeziehungen) erfolgen und muss dann über E2E-verschlüsselte Kommunikationskanäle auf ebenfalls gesicherte Systeme erfolgen. Eine korrekte und zweckmässige Verwendung der Informationen kann dann über komplementäre Massnahmen sichergestellt sein. Beispielsweise sollte eine unkontrollierte Exfiltration von Informationen erkannt und wirksam verhindert werden.

Bei Beschaffungsprojekten ist die Einhaltung der Zielarchitektur grundsätzlich auch vorzusehen. Allerdings ist das schwieriger als bei einem Entwicklungsprojekt. Auf dem Markt verfügbare Kommunikations- und Kollaborationsplattformen sind meist auf den Austausch von Informationen ausgelegt und stellen im besten Fall einen gesicherten Austausch sicher – allerdings meist ohne weitergehende Absicherungsmöglichkeiten der Client-Systeme und ohne Verwendungskontrolle im Sinne von Anforderung T-4. Hier sind die strategischen Anforderungen besonders wichtig, weil die Gewährleistung der Datensouveränität und die Einhaltung von Sicherheitsanforderungen in offenen Umgebungen grundsätzlich einfacher sicherzustellen sind. Proprietäre Lösungen neigen zu Komplexität und bieten aufgrund dieser Komplexität nicht nur

einen «Lock-In»-Effekt, sondern insgesamt auch eine grosse Angriffsfläche. Damit wird die Absicherung des Untersystems im Sinne der Zielarchitektur unnötig erschwert. Zudem ist die Überprüfbarkeit solcher Lösungen aufgrund der nicht quelloffenen Software in der Praxis oft nicht gegeben oder stark eingeschränkt.

Abkürzungen

BYOK	Bring Your Own Key
CYOK	Control Your Own Key
E2E	Ende-zu-Ende
HNDL	Harvest Now, Decrypt Later
HYOK	Hold Your Own Key
TLS	Transport Layer Serurity

Referenzen

[1] BACS, Technologiebetrachtung Confidential Computing, 5. Mai 2025
[2] BACS, Cybersicherheits- und Resilienzmethode (CSRM) – Eine strukturierte Vorgehensweise zur Stärkung der Cybersicherheit und Resilienz, Entwurf