Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

24. November 2025

Cybersicherheits- und Resilienzmethode (CSRM)

Eine strukturierte Vorgehensweise zur Stärkung der Cybersicherheit und Resilienz

Inhaltsverzeichnis

1 Einleitung

In diesem Dokument schlägt das Bundesamt für Cybersicherheit BACS eine strukturierte Vorgehensweise zur Stärkung der Cybersicherheit und Resilienz von Organisationen und Unternehmen unabhängig von ihrer Grösse und Branchenzugehörigkeit vor, die im Folgenden als Cybersicherheits- und Resilienzmethode (CSRM) oder (kurz) Methode bezeichnet wird.[1]

Die CSRM orientiert sich an einschlägigen Standards, Empfehlungen und Best Practices, wie insbesondere dem NIST Cybersecurity Framework (CSF) [2] und den IT-Sicherheitsvorgaben, welche in der Bundesverwaltung erfolgreich umgesetzt werden.[2] Sie verzichtet auf eine vollständige Risikoanalyse, wie sie in vielen Rahmenmodellen für den Umgang mit Cyberrisiken[3] vorgesehen ist, und zielt auf eine möglichst einfache und pragmatische Stärkung der Cybersicherheit und -resilienz ab [6 – 8]. Dazu wird ein erweiterter Grundschutzansatz verfolgt, wobei der Grundschutz über eine Menge von als Basisanforderungen formulierten Best Practices definiert ist (vgl. Anhang C), die grundsätzlich immer umzusetzen sind. Darüber hinaus sind je nach Schutzbedarf noch weitere technische und organisatorische Massnahmen (TOMs) zu implementieren, wobei sich der Schutzbedarf aus einer Bewertung der Auswirkungen von möglichen IT-Sicherheitsbedrohungen auf die wichtigen Tätigkeiten und entsprechenden Geschäfts- und Produktionsprozesse der Organisation oder des Unternehmens ergibt.

Die Methode zeichnet sich durch folgende wesentliche Eigenschaften und charakteristische Merkmale aus:

- Sie basiert auf internationalen Standards (insbesondere dem NIST CSF) und einem IT-Sicherheitsverfahren mit Vorgaben, die sich innerhalb der Schweizerischen Bundesverwaltung bewährt haben.
- Ihre übergeordneten Ziele sind die Sicherstellung der wichtigen Tätigkeiten und entsprechenden Geschäfts- und Produktionsprozesse, der Schutz der Werte der Organisation oder des Unternehmens, die Einhaltung von Gesetzen und anderen regulativen Vorschriften, sowie der Schutz vor Un-, Stör- und Ausfällen. Falls erforderlich sind dazu neben den TOMs, mit denen die Basisanforderungen erfüllt werden können, auch noch weitere (zusätzliche) TOMs umzusetzen.
- Obwohl sie auf eine vollständige Risikoanalyse und dabei insbesondere auch auf eine Quantifizierung von Risiken verzichtet, ist sie risikobasiert und fusst auf einer qualitativen Bewertung von IT-Sicherheitsbedrohungen und entsprechenden Auswirkungen.

---

[1] Für die Begriffe «Cybersicherheit» und «Resilienz» wird an dieser Stelle auf Anhang A und [1] verwiesen.

[2] https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund.html

[3] Beispiele sind ISO/IEC 27005 [3], NIST Risk Management Framework (RMF, https://csrc.nist.gov/projects/risk-management/) [4] und NIST SP 800-30 [5] mit den entsprechenden Hilfsmitteln. Eine umfassendere Übersicht über aktuell verfügbare und in der Praxis eingesetzte Rahmenmodelle für den Umgang mit Cyberrisiken ist von der European Union Agency for Cybersecurity (ENISA) ausgearbeitet worden und ist unter https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework verfügbar.

- Sie geht davon aus, dass beliebig viele Hard- und Softwarekomponenten zu Informatikschutzobjekten[4] aggregiert werden können. Diese Aggregationsmöglichkeit stellt eine insbesondere für den praktischen Einsatz wichtige Erweiterung und Präzisierung der gängigen Rahmenmodelle für den Umgang mit Cyberrisiken dar und erlaubt eine kohärente und nachvollziehbare Allokation von Ressourcen für die Umsetzung von geeigneten TOMs.
- Sie ermöglicht eine Berichterstattung, die es Organisationen und Unternehmen erlaubt, pro Geschäfts- oder Produktionsprozess bzw. Produkt die Sicherheits- und Resilienzeigenschaften transparent auszuweisen und damit gegenüber Kunden und der Gesellschaft Vertrauen zu schaffen.

Mittelfristig soll die CSRM eine Alternative für den vom Bundesamt für wirtschaftliche Landesversorgung BWL entwickelten und für Teile der Schweizer Wirtschaft – insbesondere die Betreiber kritischer Infrastrukturen im Strom- und Gassektor – von den jeweiligen Regulatoren als verbindlich erklärten IKT-Minimalstandard [9] bieten.

Abbildung 1: NIST Cybersecurity Framework (© N.Hanacek/NIST)

Nachfolgend wird an verschiedenen Textstellen auf das in Abbildung 1 schematisch dargestellte NIST CSF verwiesen. Dies gilt namentlich für die in Anhang C zusammengestellten Basisanforderungen. Damit soll insbesondere auch den Nutzern des IKT-Minimalstandards der Umstieg auf die CSRM erleichtert werden [10].

Im nächsten Kapitel wird die Methode in einer übersichtsmässig dargestellt, bevor in den nachfolgenden Kapiteln 3 – 7 die einzelnen Schritte vertieft werden. In Kapitel 8 werden die Prüfziele für eine Beurteilung und einen Leistungsvergleich aufgezeigt, und in Kapitel 9 werden die laufenden und zukünftige Arbeiten rund um die CSRM skizziert. Schliesslich sind die verwendeten Begriffe, die Sicherheitsstufen für

[4] An dieser Stelle ist der Begriff «Informatikschutzobjekt» noch nicht definiert. Wie später ausgeführt, handelt es sich bei einem Informatikschutzobjekt um eine Menge von Informatikmitteln (wie z. B. Hard- und Softwarekomponenten), die einem gemeinsamen und definierten Zweck dienen und deshalb auch logisch zusammengehören.

Authentifikationsverfahren, -mittel und -dienste, sowie die Basisanforderungen in den Anhängen A, B und C zusammengestellt.

2 Übersicht

Wie erwähnt basiert die CSRM auf einem (erweiterten) Grundschutzansatz. Das heisst, dass im Rahmen eines Grundschutzes Basisanforderungen postuliert werden, die grundsätzlich für jedes Informatikschutzobjekt mit geeigneten TOMs umzusetzen sind (vgl. Anhang C).[5]

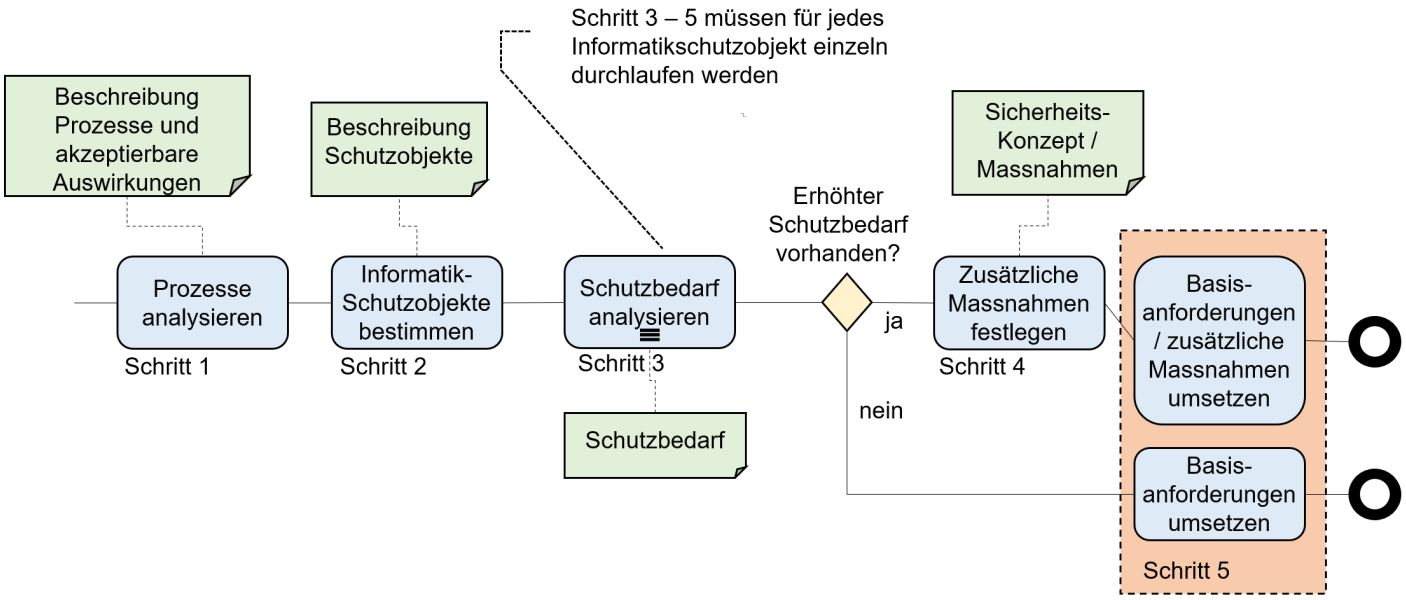

Abbildung 2: BPMN-Spezifikation der CSRM

Über den Grundschutz hinausgehend basiert die Methode auf einem Vorgehen in fünf Schritten, das sich allerdings auf architektonische Sicherheitsbetrachtungen für die Informatikschutzobjekte beschränkt.[6] Die Schritte der CSRM sind in Abbildung 2 mithilfe der Business Process Model and Notation (BPMN) spezifiziert und können folgendermassen zusammengefasst und umschrieben werden:

- **Schritt 1 (Analyse der wichtigen Tätigkeiten):** Damit die Methode sinnvoll eingesetzt werden kann, muss die Organisation oder das Unternehmen ihre wichtigen

[5] Die Umsetzung der Basisanforderungen ist für alle Informatikschutzobjekte grundsätzlich verbindlich. Je nach Organisation bzw. Unternehmen können begründete und dokumentierte Ausnahmen möglich sein, wobei die entsprechenden Ausnahmebewilligungsverfahren und -prozesse transparent und klar definiert sein müssen.

[6] Verwundbarkeiten und Schwachstellen in spezifischen Implementierungen und Produkten müssen separat und ausserhalb der Methode – z. B. im Rahmen eines Verwundbarkeitsmanagements – betrachtet und behandelt werden. Ein solches Verwundbarkeitsmanagement muss auf der betrieblichen Ebene abgedeckt werden und ist nicht Gegenstand der CSRM.

Tätigkeiten und die sie ermöglichenden Geschäfts- und Produktionsprozesse mit ihren Zielen und Abhängigkeiten kennen und im Detail verstehen. Entsprechend stellt diese Analyse den ersten Schritt im Rahmen der CSRM dar.

- **Schritt 2 (Informatikschutzobjektbestimmung):** Die zur Ausübung der im ersten Schritt analysierten Tätigkeiten und Prozessen eingesetzte IT-Infrastruktur muss im zweiten Schritt in eine Menge von Informatikschutzobjekten aufgeteilt werden, die im weiteren Verlauf der CSRM dann einzeln betrachtet und dokumentiert werden. Dabei kann sich ein Informatikschutzobjekt aus verschiedenen Informatikmitteln, wie Hard[7]- und Softwarekomponenten, sowie darin gespeicherten, verarbeiteten und übertragenen Daten zusammensetzen, die alle einem gemeinsamen und definierten Zweck dienen und deshalb auch logisch zusammengehören (z. B. eine Fachanwendung zur Abwicklung eines Geschäfts- oder Produktionsprozesses oder eine prozessübergreifende Plattform). Die nachfolgenden Schritte 3 – 5 beziehen sich dann jeweils auf ein Informatikschutzobjekt und sind für jedes Objekt einzeln zu durchlaufen.
- **Schritt 3 (Schutzbedarfsanalyse):** Für jedes in Schritt zwei identifizierte Informatikschutzobjekt muss in Schritt drei auf der Basis der gespeicherten, verarbeiteten und übertragenen Daten und unter Berücksichtigung des eigentlichen Zwecks des Informatikschutzobjektes bestimmt werden, ob sein Schutzbedarf erhöht ist oder nicht. Das ist grundsätzlich ein binärer Entscheid, der unabhängig von den Basisanforderungen des Grundschutzes zu treffen ist.
- **Schritt 4 (Sicherheitskonzipierung):** Für jedes Informatikschutzobjekt mit gemäss Schutzbedarfsanalyse erhöhtem Schutzbedarf muss in Schritt vier ermittelt werden, welche über die Erfüllung der Basisanforderungen des Grundschutzes hinausgehenden zusätzlichen TOMs erforderlich bzw. sinnvoll sind, und wie diese umzusetzen sind. Um diese TOMs auszuwählen, ist eine vertiefte Analyse des Informatikschutzobjektes und seiner spezifischen Gegebenheiten (vorzugsweise auf der Basis einer Bedrohungsmodellierung) erforderlich. Das Resultat ist ein Sicherheitskonzept, in dem sowohl das Informatikschutzobjekt mit seinem Schutzbedarf als auch das hierfür angestrebte Sicherheitsdispositiv dokumentiert sind.
- **Schritt 5 (Umsetzung):** Für jedes Informatikschutzobjekt müssen im fünften und letzten Schritt die TOMs zeitnah umgesetzt und in den regulären Betrieb überführt werden, die entweder der Erfüllung der Basisanforderungen des Grundschutzes dienen oder im IT-Sicherheitskonzept als zusätzliche TOMs ausgewiesen sind.

Die organisatorische und administrative Ausgestaltung der CSRM, sowie die entsprechenden Zuständigkeiten und Verantwortlichkeiten hängen von der betrachteten Organisation bzw. vom betrachteten Unternehmen ab und können im Rahmen dieses Dokumentes nicht allgemeingültig festgelegt werden. Sicherlich ist es aber zweckmässig und empfehlenswert, von der Geschäftsleitung ein Sicherheitsleitbild, welches die Methode zur Anwendung empfiehlt oder verpflichtet, zu erlassen und ein Sicherheitskonzept in geeigneter Form der jeweiligen Geschäftsleitung zur Kenntnis zu bringen bzw. von dieser genehmigen zu lassen. Damit kann insbesondere auch dem Umstand

[7] Unter dem Begriff von Hardwarekomponenten sind auch Peripheriegeräten subsummiert, d. h. externe Geräte, die an ein IT-System angeschlossen werden, um dessen Funktionalität zu erweitern, wie z. B. Tastaturen, Mäuse, Drucker, Monitore und externe Datenspeicher.

Rechnung getragen werden, dass die Gesamtverantwortung für die Cybersicherheit in jedem Fall bei der Geschäftsleitung liegt.

In den nachfolgenden Kapiteln werden die fünf Schritte der CSRM, d. h. die Analyse der wichtigen Tätigkeiten, die Informatikschutzobjektbestimmung, die Schutzbedarfsanalyse, die Sicherheitskonzipierung und die Umsetzung vertieft und weiter ausgeführt.

3 Schritt 1: Analyse der wichtigen Tätigkeiten

Die Analyse der für die Organisation oder das Unternehmen wichtigen Tätigkeiten und damit zusammenhängenden Geschäfts- und Produktionsprozessen stellt den Ausgangspunkt der CSRM dar. In einem Pharmaunternehmen stellen z. B. die Herstellung und der Vertrieb von Medikamenten wichtige Tätigkeiten dar, während es in der IT-Industrie eher die Entwicklung und Wartung von Software und die Beratung von Kunden sind. In jedem Fall müssen die wichtigen Tätigkeiten durch geeignete Geschäfts- und Produktionsprozesse (im Folgenden summarisch als Prozesse bezeichnet) unterstützt werden, wobei es bei Geschäftsprozessen um die Erbringung von (Dienst-) Leistungen und bei Produktionsprozessen um die Herstellung von Gütern geht. Diese Prozesse variieren von Organisation zu Organisation und von Unternehmen zu Unternehmen, und müssen entsprechend auf die Organisation oder das Unternehmen zugeschnitten und bestmöglich verstanden sein, damit die CSRM sinnvoll eingesetzt werden kann.

3.1 Durchführung

Die Analyse der wichtigen Tätigkeiten (Schritt 1) umfasst im Wesentlichen zwei Teilschritte: Zuerst müssen die Prozesse[8] bestimmt werden, die für die Ausübung der wichtigen Tätigkeiten der Organisation oder des Unternehmens relevant sind (Teilschritt 1), bevor diese Prozesse dann im Hinblick auf die Cybersicherheit und Resilienz analysiert und dokumentiert werden können (Teilschritt 2).

Teilschritt 1: Bestimmung der relevanten Prozesse

Im ersten Teilschritt müssen die Prozesse bestimmt werden, die für die Ausübung der wichtigen Tätigkeiten der Organisation oder des Unternehmens relevant und damit für die Erreichung der strategischen und wirtschaftlichen Ziele unverzichtbar sind. Für die Bestimmung dieser Prozesse können bereits vorhandene Prozessbeschreibungen bzw. -dokumentationen, Handbücher und Standard Operating Procedures (SOPs) herangezogen, Interviews und Workshops mit (an den Prozessen beteiligten) Mitarbeitenden durchgeführt, und/oder die Abläufe und Arbeitsschritte bestehender Prozesse beurteilt und durchgespielt werden.[9] Die Zahl der relevanten Prozesse wird überschaubar sein und von der Organisation oder des Unternehmens abhängen. Normalerweise wird sie im Bereich von ein paar wenigen bis einem Dutzend liegen, wobei

[8] Obwohl die Formulierung hier in der Mehrzahl ist, kann es sein, dass es in bestimmten Organisationen oder Unternehmen nur einen relevanten Geschäfts- oder Produktionsprozess gibt.

[9] Dabei können die bestehenden Prozesse auch auf ihre Gültigkeit (Aktualität) hin überprüft werden.

in grösseren Organisationen oder Unternehmen diese Normwerte natürlich auch überschritten werden können.

Teilschritt 2: Analyse und Dokumentation der Prozesse

Die in Teilschritt 1 bestimmten Prozesse müssen in Teilschritt 2 im Hinblick auf die Cybersicherheit und Resilienz vertieft – d. h. analysiert und dokumentiert – werden. Dabei haben sich die Analyse und Dokumentation vor allem auf die Ziele (Prozessziele) und Daten (Prozessdaten) eines Prozesses zu beziehen, die beide systematisch erfasst werden müssen.

- Die **Prozessziele** geben an, was mit einem Prozess konkret erreicht werden soll. Sie bestehen aus einem Haupt- oder Primärziel und mehreren Neben- oder Sekundärzielen. Während das Primärziel im Zentrum des betrachteten Prozesses steht, haben die Sekundärziele wichtige Rahmenbedingungen für diesen Prozess sicherzustellen. Bei einem Geschäftsprozess wird z. B. die effiziente Erbringung einer (Dienst-) Leistung das Primärziel sein, während es bei einem Produktionsprozess eher um die Herstellung von Gütern in den erforderlichen Mengen geht. Ergänzend dazu kann es bei einem Sekundärziel um die Sicherheit des Prozesses,[10] den Schutz vor Stör- und Unfällen (im Sinne von «Safety»), die Sicherstellung von geistigem Eigentum oder die Einhaltung von Gesetzen, Vorschriften, Standards und Best Practices (im Rahmen der «Compliance») gehen. Zusammen mit den (primären und sekundären) Prozesszielen müssen auch die maximal zulässigen Abweichungen im Hinblick auf die in Schritt 3 durchzuführende Schutzbedarfsanalyse festgelegt werden. Dabei kann der Spielraum für Abweichungen klein oder nicht vorhanden sein (wie z. B. im Rahmen der «Compliance»).
- **Prozessdaten** sind Metadaten über einen Prozess, die diesen zwar summarisch aber dennoch möglichst vollständig beschreiben, um die nachfolgenden Schritte der CSRM zu ermöglichen bzw. zu vereinfachen. Beispiele sind Daten über folgende Prozesskomponenten:
  - Eingaben (z. B. Materialien, Lieferanten, Dienstleistungen, usw.)
  - Erforderliche Ressourcen (z. B. IT-Systeme, Maschinen, Geräte, usw.)
  - Konkrete Arbeitsschritte und Abläufe
  - Rahmenbedingungen (z. B. Fristen, Durchlaufzeiten, usw.) und einzuhaltende Regeln (z. B. gesetzliche und interne Vorschriften, Standards, Qualitätsvorgaben, usw.)
  - Abhängigkeiten (z. B. von anderen Prozessen)
  - Probleme und Störungen, die auftreten können und mit denen allenfalls gerechnet werden muss (z. B. Umweltschäden, Unfälle, Abfluss von Betriebsgeheimnissen, usw.)[11]

---

[10] Die die Sicherheit betreffenden Sekundärziele von Geschäfts- oder Produktionsprozessen werden im Folgenden zusammenfassend als Schutzziele bezeichnet. Als IT-Schutzziele werden die IT-relevanten Beiträge zu den Schutzzielen bezeichnet.

[11] Hier geht es nicht um die Durchführung einer Risikoanalyse. Zu beurteilen ist, ob die genannten Probleme und Störungen im Prozessverlauf grundsätzlich und unabhängig von möglichen Bedrohungen auftreten können.

- Ausgaben und Ergebnisse (z. B. Dienstleistungen oder herzustellende Güter)

Zum Teil können Prozessdaten bereits als Primär- oder Sekundärziel genannt sein, wie z. B. herzustellende Güter als Primärziel eines Produktionsprozesses oder Umweltschäden, die es im Rahmen eines Sekundärzieles zu minimieren gilt. Prozessdaten sind immer dann relevant und müssen miterhoben werden, wenn sie für die Sicherung des Prozesses wesentlich sind.

3.2 Ergebnisse

Die von den wichtigen Tätigkeiten abgeleiteten und weiter analysierten Prozesse müssen in verständlicher Form beschrieben und dokumentiert sein. Für jeden Prozess besteht die Dokumentation aus einer grafischen Darstellung (z. B. Fluss- oder BPMN-Diagramm) sowie einer strukturierten (z. B. tabellarischen) Beschreibung der Prozessziele (mit maximal zulässigen Abweichungen) und den Prozessdaten gemäss Abschnitt 3.1. Natürlich können auch unstrukturierte Zusatzinformationen in die Dokumentation mit aufgenommen werden, insbesondere wenn diese geeignet sind, die nachfolgenden Schritte der CSRM zu unterstützen bzw. zu vereinfachen.

4 Schritt 2: Informatikschutzobjektbestimmung

Auf Basis der im ersten Schritt analysierten wichtigen Tätigkeiten müssen im zweiten Schritt die Informatikschutzobjekte bestimmt werden, die von den entsprechenden Prozessen benötigt werden. Die dazu erforderliche Aufteilung der IT-Infrastruktur (bestehend aus Hard- und Softwarekomponenten, Daten und anderen Informatikmitteln) in eine Menge von Informatikschutzobjekten ist eine schwierige (architektonische) Aufgabe. Auf der einen Seite muss sie von den relevanten Prozessen und einer explizit oder implizit gegebenen Unternehmensarchitektur ausgehen («Top-Down»-Ansatz). Auf der anderen Seite kann sich eine sinnvolle Aggregation verschiedener Hard- und Softwarekomponenten zu einem Informatikschutzobjekt auch aus einem Zusammenwirken dieser Komponenten bei der Erfüllung einer gemeinsamen Funktion (z.B. Plattformen, Cloud-Dienstleistungen, Datenbanken, usw.) ergeben («Bottom-Up»-Ansatz). Das Berücksichtigen und Abwägen beider Ansätze ist anspruchsvoll und in keinem der gängigen Rahmenmodelle für den Umgang mit Cyberrisken thematisiert. Stattdessen wird in diesen Dokumenten oft von «Assets» gesprochen, d. h. «Vermögenswerten», die zwar inventarisiert werden müssen, für die aber nicht spezifiziert ist, ob es sich um einzelne Informatikmittel oder um aggregierte Informatikschutzobjekte handelt. In diesem Sinne stellt die Informatikschutzobjektbestimmung auch eine für den praktischen Einsatz wichtige Erweiterung und Präzisierung dieser Rahmenmodelle dar. Insbesondere kann damit die übergrosse Zahl von Informatikmitteln und «Assets» auf eine überschaubare Zahl von (aggregierten) Informatikschutzobjekten reduziert und damit der Gesamtaufwand optimiert werden.

Man beachte, dass es für die Informatikschutzobjektbestimmung nicht nur eine richtige Lösung gibt, sondern viele mit jeweils unterschiedlichen Vor- und Nachteilen. Die Zuordnung von Informatikmitteln zu Informatikschutzobjekten ist nicht eindeutig und entsprechend wird es (viele) Informatikmittel geben, die gleichzeitig Bestandteil verschiedener Informatikschutzobjekte sind. Damit werden sich Informatikschutzobjekte überschneiden, wobei es ein Ziel sein muss, die Zahl der Überschneidungen, d. h. die Zahl der Informatikmittel, die gleichzeitig Bestandteil verschiedener

Informatikschutzobjekte sind, möglichst klein zu halten (auch weil Überschneidungen ein konsistentes Vorgehen bei der Auswahl und Umsetzung von TOMs erschweren). Auf der anderen Seite kann es auch den Fall geben, dass in einer kleinen Organisation oder einem kleinen Unternehmen, die gesamte IT-Infrastruktur als ein einziges Informatikschutzobjekt aufgefasst und betrachtet werden kann.

4.1 Durchführung

Grundsätzlich gibt es verschiedene Möglichkeiten und Vorgehensweisen zur Bestimmung der Informatikschutzobjekte. Eine sinnvolle Vorgehensweise wird aber in der einen oder anderen Form immer aus den im Folgenden skizzierten drei Teilschritten bestehen.

Teilschritt 1: Bestimmung der Anwendungen (pro Prozess)

Für jeden Prozess müssen die Anwendungen ermittelt werden, die für die Erreichung der entsprechenden Primär- und Sekundärziele erforderlich sind. Im Hinblick auf Primärziele können das z. B. Anwendungen für das Lieferantenmanagement oder den elektronischen Handel sein, während es im Hinblick auf Sekundärziele eher Anwendungen im Bereich des Personals oder des Enterprise Resource Planning (ERP) sind. In jedem Fall resultiert aus diesem Teilschritt eine Liste von Anwendungen pro Prozess.

Teilschritt 2: Bestimmung der Informatikmittel (pro Anwendung)

Für jede der in Teilschritt 1 ermittelten Anwendungen müssen die von ihnen benötigten Informatikmittel bestimmt werden. Dabei kann es sich bei einem Informatikmittel um eine Hard- und/oder Softwarekomponente oder Daten handeln.[12] Die Art und Weise, wie Informatikmittel aggregiert werden können, hängt von der jeweiligen Anwendung ab. So wird eine Anwendung im Bereich ERP eher mit vereinfachten und entsprechend aggregierten Informatikmitteln umgehen können als eine Anwendung zur Prozesssteuerung. Grundsätzlich erfordert die Bestimmung der Informatikmittel ein grosses einschlägiges Fachwissen und Expertise der dafür zuständigen Personen.

Teilschritt 3: Überprüfung und Vereinfachung der Informatikschutzobjekte

Am Schluss muss überprüft werden, ob alle Hard- und Softwarekomponenten mindestens einer Anwendung und jede Anwendung mindestens einem Prozess zugeordnet sind. Diese Zuordnungen müssen nachvollziehbar und hinsichtlich weiterer Möglichkeiten der Aggregation und Vereinfachung geprüft sein, wie z. B. das Zusammenlegen mehrerer Anwendungen in eine anwendungsübergreifende Plattform. Eine Plattform bietet in der Regel eine Reihe von Querschnittsfunktionen an, die von mehreren Anwendungen gleichzeitig genutzt werden können. Schliesslich stellt jede so ermittelte Anwendung oder Plattform ein eigenständiges (aggregiertes) Informatikschutzobjekt dar. Die Zahl der Informatikschutzobjekte sollte auf maximal ein paar wenige Dutzend begrenzt sein.

[12] Bei der Softwarekomponente kann es sich um die Anwendung selbst handeln. Dabei kann es auch Sinn machen, die für die Anwendung erforderliche Software in mehreren Komponenten und Modulen zu beschreiben.

4.2 Ergebnisse

Die in diesem Schritt bestimmten Informatikschutzobjekte müssen auf eine sinnvolle Art und Weise aggregiert und dokumentiert sein. Dabei sollte eine Dokumentation mindestens die folgenden das Informatikschutzobjekt betreffenden Informationen umfassen:

(1) Eindeutiger Name oder Identifikator
(2) Kurze Beschreibung (inkl. allenfalls vorhandener Architekturskizzen und verwendeten Plattformen)
(3) Liste der Geschäfts- und Produktionsprozesse, denen das Informatikschutzobjekt zudient
(4) Summarisches Verzeichnis der verwendeten Hard- und Software
(5) Liste von sinnvoll gruppierten und aggregierten Ein- und Ausgabedaten, sowie Datenflüssen
(6) Verzeichnis der Personen und Gruppen, für die das Informatikschutzobjekt relevant sind oder relevant sein können
(7) Physische Gegebenheiten (z. B. Gebäude, Maschinen, usw.), die für die Cybersicherheit relevant sein können
(8) Allenfalls vorhandene Informationen zu Rahmenbedingungen (z. B. Lieferanten, geografische Anforderungen, usw.)

Natürlich können auch weitergehende Information in die Dokumentation des Informatikschutzobjektes mit aufgenommen werden, falls diese für die weiteren Überlegungen und Schritte nützlich sind.

5 Schritt 3: Schutzbedarfsanalyse

Für jedes der im zweiten Schritt bestimmten Informatikschutzobjekte muss im dritten Schritt der Schutzbedarf analysiert und festgelegt werden. Die Analyse basiert auf den im ersten Schritt ermittelten (Primär- und Sekundär-) Zielen der Prozesse, denen ein Informatikschutzobjekt zudient, sowie den dazugehörigen maximal zulässigen Abweichungen. Falls eine Verletzung eines oder mehrerer Ziele zu mindestens einer nicht zulässigen Abweichung führen kann, gilt der Schutzbedarf des Informatikschutzobjektes als erhöht. Nur bei erhöhtem Schutzbedarf müssen die IT-Sicherheitsbedrohungen im vierten Schritt weiter untersucht und ein Sicherheitskonzept erarbeitet werden. Bei nicht erhöhtem Schutzbedarf ist dieser Schritt nicht erforderlich und die Erfüllung der Basisanforderungen und die Umsetzung von entsprechenden TOMs sind dann ausreichend.

5.1 Durchführung

Damit die Schutzbedarfsanalyse eines Informatikschutzobjektes sinnvoll durchgeführt werden kann, muss zunächst ein Datenverzeichnis erstellt werden. Als Grundlage können die Ein- und Ausgabedaten dienen, die in Schritt zwei ausgewiesen worden sind (d. h. in Punkt (5) der Ergebnisse und Dokumentation des Informatikschutzobjektes). Das Verzeichnis muss die hauptsächlichen Daten enthalten, welche entweder vom Informatikschutzobjekt erzeugt, gespeichert, verarbeitet und/oder übertragen oder für die Bereitstellung des Informatikschutzobjektes benötigt werden. Dabei

sollten die Daten in sinnvoller Weise gruppiert und mit Attributen ergänzt werden. Ein solches Attribut könnte z. B. sein, ob die Datengruppe personenbezogene Daten enthält und damit dem Datenschutz unterliegt.

Für mindestens jede Datengruppe (des Datenverzeichnisses) und bei Bedarf auch für andere Informatikmittel (wie z. B. Hard- oder Softwarekomponenten) muss geprüft werden, welche Auswirkungen eine Kompromittierung im Hinblick auf die verschiedenen IT-Schutzziele haben kann. Konkret sind folgende Fragen zu beantworten: Was würde bei einer Verletzung eines bestimmten IT-Schutzzieles (z. B. Vertraulichkeit, Integrität, Verfügbarkeit, usw.) passieren und wie verträglich wäre das mit den für den zugrundliegenden Prozess festgelegten Zielen unter Berücksichtigung der zulässigen Abweichungen? Die Antworten auf diese Fragen werden sinnvollerweise tabellarisch zusammengestellt, wobei die Datengruppen und andere Informatikmittel als Zeilen und die Attribute zusammen mit den Auswirkungen bei einer Verletzung von IT-Schutzzielen als Spalten aufgeführt sind. In den Tabelleneinträgen können dann ausformulierte Texte oder Stichwörter stehen, wobei speziell markiert werden muss, an welchen Stellen die zulässigen Abweichungen überstiegen werden bzw. ein erhöhter Schutzbedarf resultiert. Damit ein Informatikschutzobjekt über einen erhöhten Schutzbedarf verfügt, ist ein einzelner Eintrag in der Tabelle ausreichend. Dennoch können detaillierte Ausführungen in der ganzen Tabelle helfen, die nachfolgende Sicherheitskonzeption zu verbessern.

Am Schluss muss eine Schutzbedarfsanalyse im Hinblick auf Plausibilität und Konsistenz geprüft werden. Insbesondere muss dabei kontrolliert werden, ob die ausgewiesenen möglichen Auswirkungen realistisch und die entsprechenden Bewertungen nachvollziehbar und gut begründet sind. Dazu sind gegebenenfalls auch weitere Stellen beizuziehen, wie z. B. die Datenschutzberaterin oder den Datenschutzberater bei der Nutzung personenbezogener Daten.

5.2 Ergebnisse

Grundsätzlich ist das Ergebnis einer Schutzbedarfsanalyse ein (binärer) Entscheid, ob ein Informatikschutzobjekt einen erhöhten Schutzbedarf aufweist oder nicht. Wie gesagt hilft bei einem positiven Befund aber auch eine möglichst vollständig ausgefüllte Tabelle bei der anstehenden Sicherheitskonzipierung. So wird die Auswahl geeigneter TOMs massgeblich davon abhängen, welche IT-Schutzziele bedroht sind und wie diese Bedrohungen konkret aussehen. In jedem Fall ist es sinnvoll, die Erkenntnisse aus der Schutzbedarfsanalyse in geeigneter Form in der Dokumentation des Informatikschutzobjektes aus Schritt zwei (Informatikschutzobjektbestimmung) nachzutragen.

6 Schritt 4: Sicherheitskonzipierung

Im vierten Schritt muss für jedes Informatikschutzobjekt mit erhöhtem Schutzbedarf ein Sicherheitskonzept erarbeitet werden. In diesem Konzept muss unter anderem festgelegt sein, welche über die Basisanforderungen des Grundschutzes erfüllenden TOMs hinausgehenden (zusätzlichen) TOMs erforderlich bzw. sinnvoll sind, und wie diese TOMs umzusetzen sind, ohne den Zweck der zugrunde liegenden Prozesse zu beeinträchtigen. Um solche TOMs auszuwählen ist eine vertiefte Analyse des Informatikschutzobjektes und seiner spezifischen Gegebenheiten erforderlich.

Aus dem ersten Schritt geht unter anderem hervor, welche Schutzziele für einen Prozess und damit auch für ein zudienendes Informatikschutzobjekt erreicht werden sollen und welche Abweichungen und entsprechende Auswirkungen damit nicht zulässig sind. Aus der im dritten Schritt durchgeführten Schutzbedarfsanalyse geht weiter hervor, welche dieser Auswirkungen grundsätzlich möglich sind. Für diese zwar möglichen aber eben nicht zulässigen Auswirkungen geht es darum, geeignete TOMs auszuwählen, um die Auswirkungen entweder zu beseitigen oder auf ein tragbares Mass zu reduzieren. Das ist der Gegenstand der in diesem Schritt durchzuführenden Sicherheitskonzipierung.

6.1 Durchführung

Die Sicherheitskonzipierung besteht im Wesentlichen aus drei Teilschritten: Einer Bedrohungsmodellierung, der Auswahl von geeigneten TOMs und der Erstellung eines Sicherheitskonzeptes. Für die zwei ersten Teilschritte stehen verschiedene methodische Ansätze zur Verfügung und die im Folgenden ausgeführten Ansätze sind in diesem Sinne nur als Empfehlungen zu verstehen. Wenn eine Organisation oder ein Unternehmen bereits Erfahrungen mit anderen Ansätzen hat, können diese natürlich auch genutzt werden.

Element	S	T	R	I	D	E	LM
Akteur	x		x				
Prozess	x	x	x	x	x	x	x
Datenfluss		x		x	x		
Datenspeicher		x		x	x		
Grundsätzliche Massnahmen	Authentifikation	Integritätsprüfung Härtung Nachrichtenauthentifikation	Protokollierung	Verschlüsselung Autorisierung Segmentierung	Redundanz Hochverfügbarkeit	Autorisierung Least Privilege	Autonomer Schutz der Komponenten

Tabelle 1: Relevante Bedrohungskategorien gemäss STRIDE-LM (mit grundsätzlichen Massnahmen)

Teilschritt 1: Bedrohungsmodellierung

STRIDE bzw. STRIDE-LM[13] ist ein Ansatz zur Bedrohungsmodellierung, der sich in der Praxis durchgesetzt und bewährt hat und entsprechend auch im Rahmen der

[13] STRIDE ist ein Modell von Sicherheitsrisiken, das ursprünglich von Loren Kohnfelder und Praerit Garg für die Bedrohungsmodellierung bei Microsoft entwickelt worden ist, und das heute weltweit eingesetzt wird [11]. Der Name ist ein Akronym (Kunstwort), das sich aus den Anfangsbuchstaben

CSRM empfohlen wird. Grundsätzlich wird dabei systematisch untersucht, welche Architekturelemente eines Informatikschutzobjektes welchen Bedrohungskategorien ausgesetzt sind, und wie diesen Bedrohungskategorien begegnet werden kann.[14] Wie im oberen (blau hinterlegten) Teil von Tabelle 1 dargestellt,[15] können die Architekturelemente als Zeilen und die Bedrohungskategorien als Spalten einer Matrix aufgefasst werden. Dabei gehen die grundlegenden Architekturelemente aus der Dokumentation des Informatikschutzobjektes hervor, wie z. B. Akteure, Prozesse, Datenflüsse und Datenspeicher. Für diese Elemente sind unterschiedliche Bedrohungskategorien aus STRIDE-LM relevant, wie z. B. «Spoofing» und «Repudiation» für Akteure. Die für ein bestimmtes Architekturelement relevanten Bedrohungskategorien sind in Tabelle 1 mit einem «x» markiert.

Teilschritt 2: Auswahl von geeigneten TOMs

Für jede für ein bestimmtes Architekturelement relevanten Bedrohungskategorien muss diskutiert werden, mit welcher (orange hinterlegten) grundsätzlichen Massnahme von Tabelle 1, respektive dazugehörenden konkreten TOMs, die Bedrohungen abgewehrt werden können. Für diese Auswahl sind keine wahrscheinlichkeitstheoretischen Abschätzungen und Berechnungen von Risiken erforderlich, sondern nur qualitative Betrachtungen und technologische Überlegungen in Form von Heuristiken[16]. Wenn z. B. eine relevante Bedrohung darin besteht, dass bestimmte Daten während ihrer Übertragung abgegriffen werden können, dann ist der durchgehende Einsatz von Verschlüsselungstechnologien eine sinnvolle und geeignete (technische) Massnahme, um diese Bedrohung abzuwehren. Eine ähnliche Heuristik gilt für eine Anbindung an das Internet: Wenn z. B. eine Fachanwendung als Informatikschutzobjekt über das Internet angesprochen werden kann, stellt der Einsatz einer Firewall in jedem Fall eine sinnvolle (technische) Massnahme dar.

---

der ursprünglich 6 Kategorien von Sicherheitsbedrohungen zusammensetzt, die im Rahmen von STRIDE unterschieden werden: Spoofing (Identitätsverschleierung), Tampering (Manipulation), Repudiation (Verleugnung), Information disclosure (Verletzung der Privatsphäre oder Datenabfluss), Denial of service (Verweigerung des Dienstes) und Elevation of privilege (Rechteausweitung). Im Rahmen von STRIDE-LM ist das Modell im Kontext des CSF und im Hinblick auf aktuelle Bedrohungen in Netzwerken um die Kategorie «Lateral Movement» (LM) ergänzt worden. Obwohl man diese Kategorie auch unter der «Rechteausweitung» subsummieren könnte, wird im Folgenden STRIDE-LM verwendet.

[14] In vielen Vorgehensmodellen werden Risiken mit einer Liste von tatsächlichen Bedrohungen wie Ransomware oder DDoS-Angriffe modelliert. Die im Rahmen von STRIDE postulierte Liste von Bedrohungskategorien vereinfacht dies, da sich die tatsächlichen Bedrohungen jeweils einer dieser Kategorien zuordnen lässt. Im Falle von Ransomware sind das z. B. «Information Disclosure» und «Denial of Service».

[15] Dieser Teil von Tabelle 1 ist von https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach übernommen und in der letzten Spalte ergänzt.

[16] Der Begriff «Heuristik» ist vom griechischen Wort «heuriskein» abgeleitet, das etwa mit «auffinden» oder «entdecken» übersetzt werden kann. Gesucht oder gefunden werden soll eine Lösung für ein Problem, das sich nicht mathematisch formulieren und mit Hilfe entsprechender Algorithmen genau lösen lässt, sondern nur annährend mit Hilfe von Erfahrungswerten, Faustregeln, gezielten Vereinfachungen und Abkürzungen. Ein (Lösungs-) Verfahren wird entsprechend als heuristisch bezeichnet, wenn es in der Lage ist, mit begrenztem Wissen und Zeit für ein Problem eine zumindest hinreichend gute oder plausible Lösung zu finden.

Mit heuristischen Betrachtungen ist also zu prüfen, ob durch den Einsatz von geeigneten TOMs aus den in Tabelle 1 aufgeführten grundsätzlichen Massnahmen die Angriffsfläche des Informatikschutzobjektes und ihren kritischen Elementen auf ein akzeptables Mass reduziert werden kann. Dabei sind präventiv und insbesondere auch detektiv und reaktiv wirkende TOMs so einzusetzen, dass sie sich gegenseitig auf eine sinnvolle Art und Weise ergänzen.

Teilschritt 3: Erstellung eines Sicherheitskonzeptes

Die so ausgewählten TOMs müssen im Rahmen eines Sicherheitskonzeptes weiter verfeinert und spezifiziert werden. Dabei kann man davon ausgehen, dass sich für bestimmte Situationen und «Use Cases» Konstellationen von geeigneten TOMs herausbilden werden, die geeignet sind und im Rahmen von «Best Practices» standardisiert werden können.

6.2 Ergebnisse

Als Ergebnis dieses Schrittes müssen alle ausgewählten TOMs im Rahmen eines Sicherheitskonzeptes und im Hinblick auf eine Umsetzung im nachfolgenden Schritt dokumentiert und spezifiziert sein. Dabei müssen die Spezifikationen hinreichend präzis sein, damit die TOMs auf der taktischen und betrieblichen Ebene auch sinnvoll eingesetzt und betrieben werden können.

7 Schritt 5: Umsetzung

Im fünften und letzten Schritt der CSRM müssen für jedes Informatikschutzobjekt die TOMs möglichst zeitnah (von aussen nach innen[17]) umgesetzt und nachvollziehbar dem Betrieb bzw. der zuständigen operativen IT-Sicherheit übergeben werden, die entweder der Erfüllung der Basisanforderungen des Grundschutzes dienen oder im Sicherheitskonzept dokumentiert und spezifiziert sind. Für erstere (d. h. für die TOMs, die der Erfüllung der Basisanforderungen des Grundschutzes dienen) muss in einem separaten Dokument beschrieben sein, wie die Umsetzung zu erfolgen hat bzw. wie sie erfolgt. Die Zuständigkeit für die Umsetzung muss für jede TOM klar ausgewiesen sein, d. h. es muss klar sein, ob eine TOM von der Organisation oder vom Unternehmen selbst oder von einem Lieferanten bzw. Kunden umzusetzen ist. In jedem Fall muss die operative IT-Sicherheit ihre eigenen Betriebsprozesse mit abdecken, wie z. B. das Vorfallmanagement, das Schwachstellenmanagement, das Lieferantenmanagement, das Berechtigungsmanagement und das Management der Sensibilisierungs- und Schulungsprogramme für die Mitarbeitenden. Diese Betriebsprozesse sind für die IT-Sicherheit von grosser Bedeutung.

In jedem Fall ist der Betrieb als zirkulärer Prozess zu verstehen, der eine permanente Überwachung und Nachbesserung von TOMs miteinschliesst. Idealerweise hat der Betrieb einem explizit oder implizit gegebenen Betriebsmodell zu folgen, dessen Form und Inhalt allerdings nicht primärer Gegenstand der CSRM und damit dieses

[17] Gemäss dieser Heuristik werden zuerst die Massnahmen umgesetzt, mit denen das Informatikschutzobjekt im Hinblick auf Zugriffe von aussen geschützt werden können, bevor die Massnahmen umgesetzt werden, die auf einen internen Schutz abzielen. Diese Heuristik bezieht sich entsprechend auf die Priorisierung bei der Umsetzung.

Dokumentes sind. Im einfachsten Fall kann ein solches Modell aus Vorgaben oder Richtlinien[18] an die Betriebsprozesse bestehen, die als Verfahren, Verantwortlichkeiten und Regeln, respektiv als einer Liste von regelmässig durchzuführenden Aktivitäten formuliert sind. TOMs, welche sich im Betrieb als nicht wirksam erweisen, müssen zeitnah zurückgezogen bzw. zurückgebaut werden.

8 Beurteilung und Leistungsvergleich

Die IT-Sicherheit ist eine Eigenschaft, die sich nur begrenzt messen und prüfen lässt [12, 13]. Obwohl das für die Cybersicherheit und die Cyberresilienz ähnlich ist [1], eignet sich letztere grundsätzlich besser als Zielfunktion und Grundlage einer Beurteilung und eines Leistungsvergleichs im Sinne eines Benchmarkings. Der Grund liegt darin, dass die Cyberresilienz – im Gegensatz zur IT-Sicherheit – zu einem erheblichen Teil aus überprüfbaren Bausteinen besteht (wie Fähigkeiten, Prozessen, Organisation und Wiederanlaufmechanismen), die sich in definierte Prüfziele überführen und bewerten lassen (siehe unten).

Eine Beurteilung und ein Vergleich der eigenen Cyberresilienz mit der von vergleichbaren Organisationen und Unternehmen schafft Transparenz über Stärken und Schwachstellen in Technik, Organisation, Prozessen und Unternehmenskultur. Sie unterstützt die Verantwortlichen dabei, Investitionen zu priorisieren, Verbesserungen gezielt umzusetzen und sich an anerkannten Standards sowie regulatorischen Vorgaben auszurichten. Auf diese Weise stärkt sie auch die Verlässlichkeit von Dienstleistungen für Kunden, Partner und die Gesellschaft insgesamt.

Die Beurteilung der Cyberresilienz einer Organisation oder eines Unternehmens hat sich sinnvollerweise an den folgenden (sechs) Prüfzielen zu orientieren:

1. Die wichtigen Geschäfts- und Produktionsprozesse müssen mit ihren Abhängigkeiten von Informatikschutzobjekten bekannt, dokumentiert und verstanden sein.
2. Zuständigkeiten und Verantwortlichkeiten müssen geklärt, sowie erforderliche Ressourcen zur Verfügung gestellt und im Rahmen einer Sicherheitskultur nachhaltig verankert sein.
3. Für alle Informatikschutzobjekte muss die Bedrohungslage analysiert und der Schutzbedarf geklärt sein.
4. Für alle Informatikschutzobjekte müssen geeignete TOMs umgesetzt und in einem konsistenten Sicherheitskonzept zusammengeführt sein.
5. Es muss sichergestellt sein, dass sicherheitsrelevante Vorfälle zeitnah erkannt und bewältigt werden können. Insbesondere müssen betroffene Systeme and Anwendungen rasch wiederhergestellt werden können.
6. Alle Abhängigkeiten und Risiken, die aus der Zusammenarbeit mit Dritten (z. B. aus Lieferketten oder durch Partner) entstehen, müssen kontrolliert werden

[18] Mit Richtlinien sind nicht Strategien oder Leitbilder gemeint, sondern konkrete Umsetzungsrichtlinien oder Einsatzrichtlinien (Acceptable Use Policies). Diese Richtlinien müssen nicht von jeder Organisation neu entwickelt werden, da sich diese für gleichartige Prozesse kaum unterscheiden werden. Branchenweite Vorlagen können ausgearbeitet und geteilt werden.

können, um Dominoeffekte zu vermeiden und die Resilienz von Wertschöpfungsketten zu sichern.

Diese Prüfziele bilden den Rahmen für einen ganzheitlichen Leistungsvergleich der Cyberresilienz. Sie stellen sicher, dass technische, organisatorische, prozessuale und auch kulturelle Aspekte gleichermassen berücksichtigt werden. In diesem Sinn hat das BACS Cybersicherheits- und Resilienzprüfkataloge entworfen, die zurzeit mit interessierten Organisationen und Unternehmen auch in Richtung unterstützende Hilfsmittel und Werkzeuge für die CSRM weiterentwickelt und ausgetestet werden.

9 Ausblick

Das CSRM kann als Managementsystem für die Cybersicherheit und Resilienz verstanden werden, das sich in eine ganze Serie von zwar ähnlichen aber in ihrer Ausrichtung doch unterschiedlichen Managementsystemen einreihen kann, wie z. B. Datenschutz-Managementsysteme (DSMS), Business-Continuity-Managementsysteme (BCMS), Cybersecurity-Mangementsysteme[19] (CSMS) und vor allem auch Informationssicherheitsmanagementsysteme (ISMS). Gemäss [14] kann ein ISMS als «ein aus Verfahren und Regeln bestehendes System» definiert werden, «das in einer Organisation oder einem Unternehmen eingesetzt werden kann, um die Informationssicherheit zu gewährleisten, d. h. konkrete Informationssicherheitsziele zu definieren und deren Erreichung zu planen, steuern und sicherzustellen».

In Tabelle 2 sind die verschiedenen Managementsysteme im Hinblick auf ihre Abdeckung der in Kapitel 8 aufgeführten Prüfziele der Cyberresilienz zusammengestellt [10]. Allerdings ist auch bei der CSRM die Abdeckung nicht in allen Bereichen vollständig, wie z. B. das Prüfziel 6 zeigt. Klassische BCM-Funktionen, wie Wiederanlaufplanung und sektorale Krisenkoordination, sind in der CSRM nicht in voller Tiefe enthalten. Hier müssen Organisationen ergänzend auf etablierte Methoden des BCM zurückgreifen.

Eine besondere Stärke des CSRM ist aber, dass es die Geschäfts- und Produktionsprozesse als essenzieller Ausgangspunkt nimmt für die Beurteilung des Schutzbedarfs. Risiken müssen immer im Kontext dieser Prozesse beurteilt werden. Dies ermöglicht es auch Anforderungen an den Datenschutz und Betriebsschutz (im Sinne von «Safety») im gesamten Prozess mitzuberücksichtigen.

Während die CSRM den methodischen Rahmen vorgibt, spezialisieren sich die genannten Managementsysteme auf einzelne Schwerpunkte: Ein ISMS ist z. B. weniger stark in den Prozessen verankert und zielt auf IT-Systeme (im Vergleich zu Industriellen OT-Systemen) ab. Es kann so Auswirkungen von Stör- und Unfällen weniger gut entgegentreten. Ein DSMS hingegen zielt – unabhängig von den eigentlichen Geschäfts- und Produktionsprozessen – auf den Schutz von Personendaten, das Melden von Datenschutzverletzungen und das Sicherstellen von vertraglichen Bestimmungen zum Schutz von Personendaten. Ein BCMS wiederum wirkt vor allem auf die Prüfziele 5 und 6, sowie dem Kennen der eigentlichen Geschäfts- und Produktionsprozesse.

[19] Damit sind insbesondere Managementsysteme im Bereich der OT gemeint, die nach einschlägigen Standards (z. B. IEC 62443) ausgerichtet sind.

Das CSRM bietet hier eine Konvergenz und ermöglicht den Aufbau eines Managementsystems, das ISMS, CSMS, DSMS und teilweise sogar BCMS vereint. Insbesondere kann es aber eine einfache und pragmatische Umsetzung eines ISMS ermöglichen.

Managementsystem	**Prüfziele der Cyberresilienz**					
	1	**2**	**3**	**4**	**5**	**6**
CSRM Cybersicherheits- und Resilienzmethode		20				21
ISMS Informationssicherheitsmanagementsystem			22	23		
DSMS Datenschutz-Management system						
BCMS Business Continuity Management System						

vollständig abgedeckt

teilweise abgedeckt

nicht abgedeckt

Tabelle 2: Abdeckung der Cyberresilienz (d. h. der Prüfziele der Cyberresilienz) durch gängige Managementsysteme

Das BACS begleitet den Einsatz der CSRM in ausgewählten Organisationen und Unternehmen, auch um es aufgrund von Erfahrungswerten laufend zu verbessern und mit Umsetzungsempfehlungen und -hilfen zu ergänzen. Das Hauptziel ist und bleibt die universelle Einsetzbarkeit. Branchenspezifische Gegebenheiten und Sonderfälle sind in der CSRM nicht standardmässig mit abgedeckt und werden allenfalls zu branchenspezifischen Erweiterungen und Umsetzungsempfehlungen führen.

[20] Die Methode, wie auch die anderen Managementsysteme besagt, dass idealerweise der Betrieb einem explizit oder implizit gegebenen Betriebsmodell zu folgen hat, dessen Form und Inhalt allerdings nicht primärer Gegenstand der CSRM sind.

[21] Das Lieferantenrisikomanagement wird als Basisanforderung des Grundschutzes vom CSRM erwartet, ist aber sonst nicht explizit ein Teil davon.

[22] Die Risikoidentifizierung in einem ISMS basiert auf den IT-Schutzzielen wie Vertraulichkeit, Verfügbarkeit und Integrität und nicht auf den akzeptierbaren Auswirkungen der Geschäfts- und Produktionsprozesse.

[23] Ein ISMS hat zum Ziel die Informationen zu schützen und nicht Datenschutzverletzungen zu verhindern oder Stör- und Unfällen vorzubeugen, deshalb ist es kein gesamtheitlicher Ansatz.

Abkürzungen

AAL	Authentication Assurance Level
BACS	Bundesamt für Cybersicherheit
BCM	Business Continuity Management
BCMS	BCM-System
BWL	Bundesamt für wirtschaftliche Landesversorgung
CCTV	Closed Circuit Television
CI/CD	Continuous Integration / Continuous Delivery
CSF	Cybersecurity Framework
CSMS	Cybersecurity-Mangementsystem
CSP	Cloud Service Provider
CSRM	Cybersicherheits- und Resilienzmethode
DSMS	Datenschutz-Managementsystem
DTI	Digitale Transformation und IKT-Lenkung
ENISA	European Union Agency for Cybersecurity
ERP	Enterprise Resource Planning
FIDO2	Fast IDentity Online 2
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IKT	Informations- und Kommunikationstechnologie
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Information Technology
JSON	JavaScript Object Notation
JWT	JSON Web Token
LM	Lateral Movement
MFA	Multi-Factor Authentication
MITM	Mallory in the middle
MVSP	Minimum Viable Secure Product
NCSC	Nationales Zentrum für Cybersicherheit
NIST	National Institute of Standards and Technology
OAuth	Open Authorization
OIDC	OpenID Connect
OT	Operational Technology
OTP	One-Time Password
PIN	Personal Identification Number
RFC	Request For Comments
RMF	Risk Management Framework
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SMS	Short Message Service
SOC	Security Operations Center
SOP	Standard Operating Procedure
SP	Special Publication
SSO	Single Sign-on
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege

TOM	Technische und Organisatorische Massnahme
TPM	Trusted Platform Module
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
XML	Extensible Markup Language

Referenzen

[1] BACS, Technologiebetrachtung «Cybersicherheit und -resilienz», November 2025

[2] NIST, The NIST Cyber Security Framework (CSF) 2.0, February 26, 2024

[3] ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks

[4] NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations — A System Life Cycle Approach for Security and Privacy, Dezember 2018

[5] NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, September 2012

[6] Rolf Oppliger und Andreas Grünert, How to Manage Cyber Risks: Lessons Learnt from Medical Science, IEEE Computer, Vol. 56, No. 1, Januar 2023, Seiten 117 – 119

[7] Rolf Oppliger und Andreas Grünert, How to Measure Cybersecurity and Why Heuristics Matter, IEEE Computer, Vol. 57, No. 2, Februar 2024, Seiten 111 – 115

[8] Andreas Grünert, James Bret Michael, Rolf Oppliger und Ruedi Rytz, Why Probabilities Cannot Be Used in Cyber Risk Management, IEEE Computer, Vol. 57, No. 10, Oktober 2024, Seiten 86 – 89

[9] BWL, Minimalstandard zur Verbesserung der IKT-Resilienz, 2023

[10] BACS, «CSRM im Vergleich mit bekannten Managementsystemen», November 2025

[11] Loren Kohnfelder und Praerit Garg, «The threats to our products», April 1, 1999

[12] Andreas Grünert, James Bret Michael, Rolf Oppliger und Ruedi Rytz, On the Measurability and Testability of IT Security, IEEE Computer, Vol. 58, No. 3, März 2025, Seiten 120 – 126

[13] BACS, «Mess- und Prüfbarkeit der IT-Sicherheit», 10. Juni 2025

[14] BACS, Technologiebetrachtung «Informationssicherheitsmanagement und ISMS», 2. Juli 2025

[15] NIST SP 800-63B, Digital Identity Guidelines – Authentication and Lifecycle Management, Juni 2017

[16] BACS, Technologiebetrachtung «Passkeys», 2025

Anhang A: Begriffe

In der Informatik bezeichnet man als Wissenspyramide das in Abbildung 3 dargestellte Modell, in dem schematisch dargestellt ist, wie aus Daten Informationen und Wissen (Aufwärtsrichtung) bzw. aus Wissen Informationen und Daten (Abwärtsrichtung) akquiriert werden kann. Zuweilen wird das Modell gegen unten noch um Zeichen und gegen oben um Weisheit bzw. Verständnis ergänzt. Daten setzen sich dann aus Zeichen zusammen und Weisheit bzw. Verständnis entsteht (auch) aus Wissen. In der Abwärtsrichtung gelesen kann man sagen, dass Wissen als Informationen und Informationen als Daten codiert werden können. Damit stellen Daten eine insbesondere für automatisierte Verarbeitungsprozesse ausgelegte Form codierter Informationen dar.

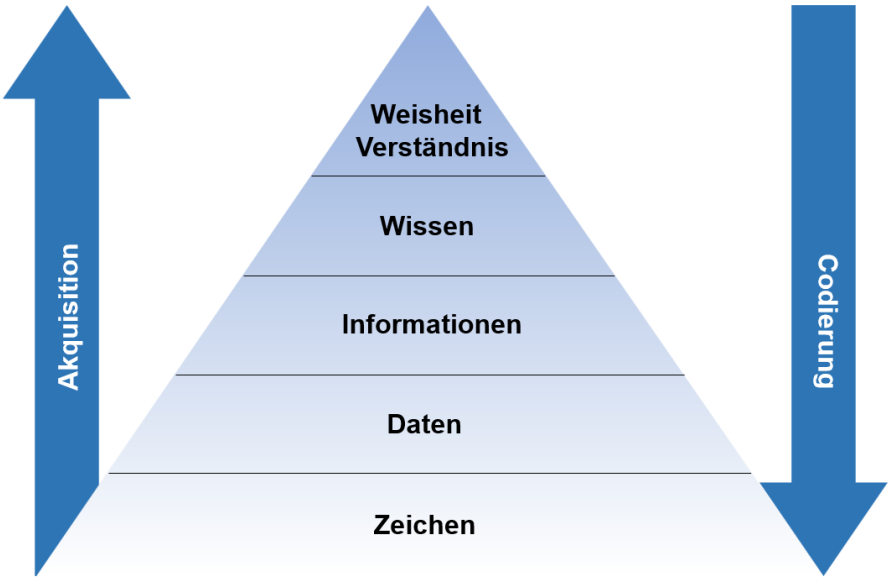

Abbildung 3: Wissenspyramide

Obwohl die Begriffe «Information» und «Daten» im Alltag oft synonym verwendet werden, ist die Gleichsetzung falsch und kann unter Umständen zu Unklarheiten oder sogar Missverständnissen führen. Auf der einen Seite werden nicht alle Informationen als Daten codiert. Wenn man z. B. ein persönliches Gespräch führt, kann man der Wortwahl, Mimik und Gestik Informationen entnehmen, die nicht bzw. höchstens summarisch in einer protokollarischen Aufzeichnung codiert werden. Auch sonst gibt es im täglichen Leben Szenen, die man zwar beobachten kann und die entsprechend informativ sind, die aber weder aufgezeichnet noch als Daten codiert werden. Auf der anderen Seite gibt es Daten, aus denen grundsätzlich keine Information akquiriert werden kann. Man denke hier etwa an zufällig erzeugte oder verschlüsselte Daten. Im zweiten Fall kann man unter bestimmten Voraussetzungen sogar mathematisch beweisen, dass aus verschlüsselten Daten ohne Kenntnis der verwendeten Schlüssel keinerlei Information abgeleitet werden kann.[24]

[24] Man spricht in diesem Zusammenhang auch etwa von «informationstheoretischer Sicherheit» der Verschlüsselung.

Aufgrund dieser Unterschiede sollten die Begriffe «Information» und «Daten» voneinander unterschieden werden, wobei sich die Unterscheidung dann auch auf die Begriffe Daten- bzw. Informationssicherheit vererbt.

- Bei der **Datensicherheit** geht es um die Gewährleistung der Sicherheit von Daten, die im Rahmen der IT bzw. in IT- und OT-Systemen gespeichert, (automatisiert) verarbeitet und übertragen werden. Dabei kann sich die Sicherheit auch auf verschiedene IT-Schutzziele beziehen, wie z. B. die Vertraulichkeit, Integrität und Verfügbarkeit der Daten.
- Demgegenüber geht es bei der **Informationssicherheit** um die Gewährleistung der Sicherheit von Informationen, die – wie oben erwähnt – auch ausserhalb der IT in nicht für automatisierte Verarbeitungsprozesse ausgelegter und entsprechend als Daten codierter Form existieren können. Persönliche Gespräche und Szenen aus dem täglichen Leben sind als Beispiele bereits genannt. Ein anderes Beispiel stellen Papierarchive mit handschriftlichen Notizen dar. Die so archivierten Dokumente sind zwar auch codiert, die entsprechende Codierung ist aber nicht für automatisierte Verarbeitungsprozesse ausgelegt (auch wenn heute zunehmend viele solche Dokumente im Hinblick auf automatisierte Verarbeitungsprozesse eingelesen und als Daten codiert werden).

Ähnlich, aber dennoch etwas breiter als die Datensicherheit ist der Begriff der **Informatik-** oder **IT-Sicherheit** ausgelegt. Neben der Gewährleistung der Sicherheit von Daten geht es hier auch um die Gewährleistung der Sicherheit von anderen Informatikmitteln, wie z. B. Hard- und/oder Softwarekomponenten. Dieser Aspekt spielt namentlich im Bereich der Operational Technology (OT) sowie bei der Verwendung von intelligenten Geräten, auch Internet-of-Things (IoT)[25] genannt, eine wichtige Rolle. Man beachte, dass OT und IoT zwar «normale» IT-Komponenten, -Protokolle und -Architekturen verwenden, dass sich aber die Auswirkungen bei einer Verletzung der Schutzziele Vertraulichkeit, Verfügbarkeit oder Integrität nicht nur auf Geschäfts- und Produktionsprozesse auswirken können (welche gegebenenfalls nicht aufrechterhalten werden können), sondern gegebenenfalls auch Auswirkungen auf die reale (physische) Welt haben (z. B. durch das Öffnen von Ventilen, Fenster oder dem Steuern eines mechanischen Vorganges) und so Unfälle und Verletzungen verursachen können. Die CSRM ermöglicht es,[26] OT- und IT- Systeme zu schützen und resilient zu gestalten und unterstützt so auch die methodische Konvergenz von IT und OT in der Cybersicherheit.

---

[25] Die Bedrohungen bei IoT-Geräten, welche eigenständig und exponiert sein können, unterscheiden sich von OT-Geräten und Komponenten, welche Teil einer redundant und mit zusätzlichen Safety-Systemen ausgestatten Umgebung sein sollten. Dies wirkt sich auch auf die Umsetzung der Basisanforderungen aus.

[26] Das CSRM ist darauf ausgelegt nicht nur auf die Geschäftslogik angewandt zu werden, sondern auch Produktions- und Betriebsführungssysteme, den Prozessleitsysteme, Steuerungs- und Überwachungssysteme sowie digitalen Aktoren und Sensoren von Industriellen Herstellungsprozessen. Dazu berücksichtigt Schritt 1 die Ziele bezüglich des Schutzes vor Stör- und Unfällen, Schritt 2 berücksichtigt die Komponenten von OT-Systemen als Teil der Schutzobjekte, Schritt 3 beurteilt, ob eine Verletzung der IT-Schutzziele zu einer Verletzung der Prozessziele inklusive des Schutzes vor Stör und vor Unfällen führen kann. Schlussendlich muss die Sicherheitskonzeption nach Schritt 4 und die Basisanforderungen auch bei OT-Systemen umgesetzt werden. Ein Vergleich dieser Methode zu den Modellen von IEC 62443 wird zurzeit ausgearbeitet.

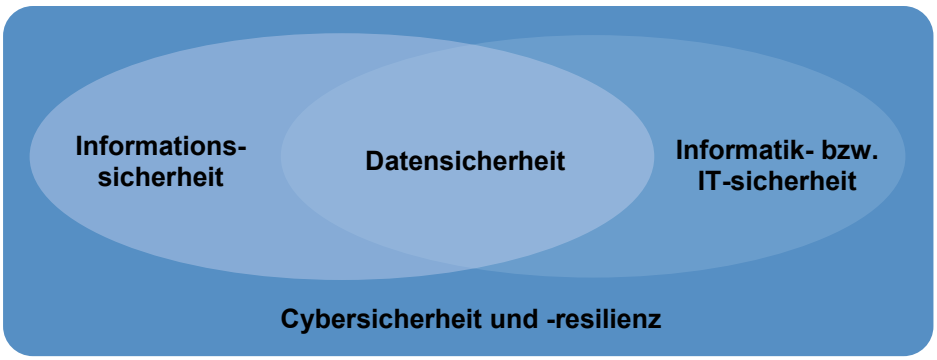

Abbildung 4: Sicherheitsbegriffe

Das Zusammenspiel von Informations-, Daten- und Informatik- bzw. IT-Sicherheit ist in Abbildung 4 schematisch dargestellt. Neben diesen Sicherheitsbegriffen gibt es noch die neueren Begriffe Cybersicherheit und -resilienz [1]. Dabei ist der Begriff **Cybersicherheit** nicht exakt definiert und lässt sich auch nicht einfach gegenüber den anderen Sicherheitsbegriffen abgrenzen. Letztlich geht es bei der Cybersicherheit aber immer um den Schutz von IT-Infrastrukturen und der mit diesen unmittelbar verbundenen Informationen und Daten. Demgegenüber beschreibt die **Cyberresilienz** die Fähigkeit einer Organisation oder eines Unternehmens, ihre wesentlichen Geschäfts- und Produktionsprozesse trotz Cyberbedrohungen und IT-Vorfällen aufrechtzuerhalten oder nach einem IT-Vorfall so schnell wie möglich weiterzuführen. Entscheidend ist dabei nicht nur die Verhinderung von IT-Vorfällen (inkl. Angriffen), sondern auch die Kenntnis welche Auswirkungen nicht akzeptierbar sind und die Fähigkeit, jederzeit handlungsfähig zu bleiben, die Schäden wirksam zu begrenzen und rasch zum Normalbetrieb zurückzukehren.

Anhang B: Sicherheitsstufen für Authentifikationsverfahren, -mittel und -dienste

Auf dem Markt sind heute viele verschiedene Verfahren, Mittel und Dienste verfügbar, die für die direkte oder indirekte Authentifikation[27] von Personen oder Prozessen eingesetzt werden können, und die sich in Bezug auf ihre Sicherheitseigenschaften zum Teil erheblich unterscheiden. Ohne auf die Unterschiede im Detail einzugehen, wird in diesem Anhang eine grobe Klassifikation mit nur drei Sicherheitsstufen («tief», «mittel» und «hoch») postuliert. Die Klassifikation orientiert sich an den Authentication Assurance Level (AAL) 1 - 3 aus [15], beschränkt sich auf wissensbasierte Ansätze,[28] ist möglichst einfach gehalten und sieht zurzeit noch keine Möglichkeit zur formalen Prüfung oder Anerkennung vor.

- **Tief:** Die Information, aufgrund derer eine (direkte oder indirekte) Authentifikation stattfinden kann, ist statisch und für jeden Authentifikationsvorgang gleich (z. B. ein Passwort oder ein kryptografischer Schlüssel). Falls diese Information z. B. im Rahmen eines «Phishing»-Angriffs oder durch Mitschneiden des Datenverkehrs in einem Netzwerk kompromittiert wird, kann sie auch für eine Identitätstäuschung missbraucht werden. Typische Beispiele sind Benutzername und Passwort, sowie kryptografisch nicht speziell geschützte «Bearer-Token» (z. B. Cookies). Die Sicherheitsstufe bleibt «tief», auch wenn die Übertragung über eine kryptografisch abgesicherte Verbindung (z. B. TLS) erfolgt. Solche Authentifikationsverfahren sollten heute aus Sicherheitsgründen nicht oder nur noch in Ausnahmefällen eingesetzt werden.
- **Mittel:** Die Information, aufgrund derer eine (direkte oder indirekte) Authentifikation stattfinden kann, ist dynamisch und wird für jeden Authentifikationsvorgang neu erzeugt. Entsprechend kann sie auch bei einer Kompromittierung nicht einfach für eine Identitätstäuschung missbraucht werden. Für die direkte Authentifikation können Username und Passwort zwar noch weiter eingesetzt werden, allerdings müssen sie über einen weiteren Sicherheitsmechanismus, wie z. B. eine Gerätebindung, abgesichert sein.[29] Besser sind hier OTP-Softwarelösungen (z. B. Google oder Microsoft Authenticator), Software-Zertifikats-basierte Authentifikationen im Rahmen von TLS und FIDO2-Implementierungen mit Synchronisations- und Schlüsselexportiermöglichkeiten (z. B. Passkeys [16]). Für die indirekte Authentifikation müssen die Bescheinigungen kryptografisch abgesichert (z. B. verschlüsselt

[27] Eine Authentifikation ist direkt, wenn sie zwischen der sich authentifizierenden Entität (z. B. Person oder Prozess) und einer anderen (authentifizierenden) Entität direkt stattfindet. Wenn die Authentifikation durch eine Drittpartei (z. B. Identity Provider) moderiert wird, ist sie indirekt. In diesem Fall stellt die Drittpartei eine Bescheinigung für einen oder mehrere Ansprüche (z. B. Identität) aus, die in diesem Zusammenhang als «Ticket» oder «Token» bezeichnet wird und idealerweise selbst kryptografisch abgesichert ist. Die Authentifikation gegenüber der Drittpartei muss den Anforderungen der entsprechenden Sicherheitsstufe genügen.

[28] Entsprechend nicht berücksichtigt sind in dieser Klassifikation andere Ansätze zur Authentifikation, wie z. B. biometrische Ansätze und Ansätze, die auf «etwas haben» basieren, sowie physische Zugangskontrollmechanismen.

[29] Grundsätzlich stellen auch SMS-Verifikationscodes eine solche Absicherung dar. Allerdings ist die Sicherheit SMS-basierter Authentifikationsverfahren in Frage gestellt, so dass solche Verfahren nur noch eingesetzt werden sollten, wenn es keine bessere Alternative gibt.

und/oder digital signiert) und auf eine dem Stand der Technik entsprechende Art und Weise an den Anwenderkontext (z.B. die «Session») gebunden sein.[30] Beispiele sind Kerberos-Tickets, SAML- und OIDC-Token,[31] sowie JSON Web Tokens (JWTs).

- **Hoch:** Die Information, aufgrund derer eine (direkte oder indirekte) Authentifikation stattfinden kann, ist nicht nur dynamisch und wird für jeden Authentifikationsvorgang neu erzeugt, sondern hängt auch von einem kryptografischen Schlüssel ab, der in einem dedizierten Hardware-Modul gespeichert ist und von dort (mit vertretbarem Aufwand) nicht ausgelesen werden kann. Zudem muss das Hardware-Modul persönlich sein und im Rahmen eines definierten und nachvollziehbaren Registrationsprozesses ausgestellt und einer Person auf eine kontrollier- und nachvollziehbare Art und Weise übergeben worden sein. Typische Beispiele sind OTP-Token (z. B. von RSA, Vasco oder einem anderen Hersteller), OTP-Lösungen auf der Basis eines TPM, Hardware-Zertifikats-basierte Authentifikationen im Rahmen von TLS, FIDO2-Implementierungen ohne Synchronisations- und Schlüsselexportiermöglichkeiten, sowie Authentifikationen auf der Basis einer Swisscom Mobile ID. Für die indirekte Authentifikation gelten die gleichen Anforderungen wie bei der Sicherheitsstufe «mittel», wobei zusätzlich noch verlangt ist, dass die Authentifikation gegenüber der Kerberos-Tickets oder andere Token ausgebenden Drittpartei auf der Basis eines Authentifikationsverfahrens der Stufe hoch stattgefunden hat.

Die erwähnten Beispiele sind nicht abschliessend zu verstehen und in Tabelle B.1 summarisch zusammengestellt.

Sicherheitsstufe	Beispiele
tief	• Benutzername und Passwort • «Bearer-Token» (z. B. Cookies)
mittel	• Benutzername und Passwort mit SMS-Verifikationscode • Benutzername und Passwort mit Gerätebindung* • OTP-Softwarelösung (z. B. Google oder Microsoft Authenticator) • Software-Zertifikats-basierte Authentifikation im Rahmen von TLS* • FIDO2-Implementierungen mit Synchronisations- und Schlüsselexportiermöglichkeiten (z. B. Passkeys*) • Kerberos-Tickets • SAML- und ID und Access Tokens im Rahmen von OIDC und

[30] Diese Anforderung impliziert unter anderem auch, dass die Gültigkeitsdauer eines solchen Tokens im Hinblick auf seinen Einsatzzweck nicht übermässig gross sein darf.

[31] Während sich SAML-Tokens auf ein älteres, seit ca. 2005 eingesetztes XML-basiertes Token-Format bezieht, bei dem die Ansprüche als «Assertions» bezeichnet und von Service Providern genutzt werden, beziehen sich OIDC-Tokens auf ein neueres Token-Format auf der Basis von OAuth 2.0 und JSON. Die Ansprüche werden hier als «Claims» bezeichnet und von Relying Parties genutzt. SAML-Tokens werden typischerweise für unternehmensweite SSO-Lösungen verwendet, während OIDC-Tokens eher für authentifikations- und autorisationsspezifische APIs benutzt werden.

	OAuth 2.0 • JWTs
hoch	• OTP-Token (z.B. RSA, Vasco, …) • OTP-Lösung auf der Basis eines TPM* • Hardware-Zertifikats-basierte Authentifikation im Rahmen von TLS* • FIDO2-Implementierungen ohne Synchronisations- und Schlüsselexportiermöglichkeiten* • Swisscom Mobile ID • Kerberos-Tickets und andere Tokens, die auf der Basis einer Authentifikation der Stufe hoch ausgestellt worden sind

Tabelle B.1: Sicherheitsstufen von Authentifikationsverfahren, -mitteln und -diensten

Grundsätzlich kann durch das Kumulieren von mehreren Authentifikationsverfahren und -mitteln einer Sicherheitsstufe die Stufe nicht erhöht werden, d. h. Passkeys bleiben z. B. in der Sicherheitsstufe «mittel», auch wenn sie mit Benutzername und Passwort mit SMS-Verifikationscode kombiniert werden.

Für (sicherheitskritische) Anwendungen, bei denen damit gerechnet werden muss, dass Angreifer versuchen, authentifizierte Sessions zu übernehmen («Session Hijacking») und/oder sich im Rahmen von «Real-time Phishing» oder als «Mallory in the middle» (MITM) in Kommunikationsbeziehungen einzubringen, sind weitergehende Authentifikationsverfahren, -mittel und/oder -dienste erforderlich. Vor Session-Hijacking-Angriffen schützt z. B. eine Gerätebindung (d. h. eine Bindung der Endgeräte an die Session), währenddem vor MITM-Angriffen eine Bindung der Authentifikationsinformation an die Session schützt. In diesem Sinne weitergehende Authentifikationsverfahren, -mittel und -dienste sind in Tabelle B.1 mit einem Stern (*) markiert. Dabei gilt es zu berücksichtigen, dass die Verfahren, Mittel und Dienste in der Regel so konfiguriert werden müssen, dass sie vor Session-Hijacking- und MITM-Angriffen schützen können. Default-mässig und ohne spezielle Vorkehrungen ist ein solcher Schutz oft nicht gegeben.

Anhang C: Basisanforderungen

Die in diesem Anhang zusammengestellten und ausgeführten Basisanforderungen sind gemäss den Funktionen des NIST CSF strukturiert. Während sich die Anforderungen der Funktion 1 (GOVERN) auf die Organisation oder das Unternehmen beziehen, die bzw. das für ein Informatikschutzobjekt zuständig und verantwortlich ist, beziehen sich alle anderen Funktionen des CSF (d. h. IDENTIFY, PROTECT, DETECT, RESPOND bzw. RECOVER) auf die eigentlichen Informatikschutzobjekte. Im Gegensatz zum CSF sind die Funktionen RESPOND und RECOVER hier der Einfachheit wegen zusammengelegt (und farblich an RESPOND ausgerichtet).

Alle Anforderungen gelten grundsätzlich auch entlang von Lieferketten, wobei die Geschäftsleitung die entsprechenden Verbindlichkeiten und Modalitäten der Überprüfung festlegen muss. Die Gesamtverantwortung für die Sicherheit obliegt in jedem Fall der Geschäftsleitung.

Wenn die CSRM eingesetzt wird, entfallen die Basisanforderungen 1.2, 2.1. Sie sind entsprechend mit einem Stern (*) markiert.

An einzelnen Stellen sind konkrete Umsetzungsmöglichkeiten genannt. Diese Möglichkeiten sind nur im Sinne von Empfehlungen zu verstehen und schliessen andere Möglichkeiten zur Umsetzung nicht aus. Die Güte der Umsetzung muss sich in jedem Fall am Schutzbedarf der Organisation oder des Unternehmens bzw. des Informatikschutzobjekts orientieren.

1	GOVERN (GV)
1.1	**Sicherheitsorganisation** Die Sicherheitsorganisation muss definiert und gegenüber den Mitarbeitenden kommuniziert sein bzw. in dieser Form auch gelebt werden. Insbesondere müssen die Kontaktpersonen mit ihren Zuständigkeiten und Verantwortlichkeiten für die strategische und operative Cybersicherheit nachvollziehbar festgelegt sein.[32] Diese Personen müssen fachlich in der Lage sein, ihre Verantwortung auch wahrzunehmen.
1.2 *	**Cyberrisikomanagement** Das Cyberrisikomanagement muss definiert und festgelegt sein, d. h. es muss geklärt sein, ob und wie mit Cyberrisiken umzugehen ist, und wie die Geschäftsleitung – entweder direkt oder indirekt über ein übergeordnetes Risikomanagement – eingebunden ist. Für die Beurteilung und Einstufung

[32] Zur strategischen Cybersicherheit gehören die Steuerung und Lenkung der Cybersicherheit. Demgegenüber gehören zur operativen Cybersicherheit das Schwachstellen-, Vorfall-, Lieferanten-, Schulungs- und Sensibilisierungs- und Berechtigungsmanagement.

	von Cyberrisiken müssen Kriterien definiert sein, und für kritische Cyberrisiken[33] müssen adäquate TOMs bestimmt und umgesetzt sein.[34]
1.3	**Überprüfung von Mitarbeitenden** Die Vertrauenswürdigkeit der Mitarbeitenden[35] muss ihren Stufen und Tätigkeiten entsprechend überprüft sein.
1.4	**Schulung und Sensibilisierung** Die Mitarbeitenden müssen im Hinblick auf Fragen der Cybersicherheit ihren Stufen und Tätigkeiten entsprechend sensibilisiert und geschult sein. Im Rahmen der Schulungen müssen soweit möglich auch tatsächliche Vorfälle und daraus resultierende Schlussfolgerungen für die Organisation oder das Unternehmen thematisiert werden.

2 IDENTIFY (ID)	
2.1 *	**Informatikschutzobjekte** Alle (wesentlichen) Hard- und Softwarekomponenten müssen mit ihren Ein- und Ausgabedaten, Konfigurationen, sowie Datenflüssen dokumentiert und im Hinblick auf ihren Schutzbedarf analysiert sein.[36] Dabei können mehrere logisch zusammengehörende Komponenten (inklusive Peripheriegeräte) zusammengefasst und zu einem Informatikschutzobjekt aggregiert sein. Die entsprechenden Schutzbedarfsanalysen und Dokumentationen müssen alle umgesetzten und noch umzusetzenden TOMs mit umfassen und stets aktuell gehalten werden.
2.2	**Lieferketten** Alle Abhängigkeiten in den Lieferketten müssen identifiziert, mit ihrer Bedeutung für die Geschäftstätigkeit (d. h. die Geschäfts- und Produktionsprozesse) beurteilt und überwacht werden.[37] Insbesondere muss sichergestellt sein, dass die Lieferanten von für die Geschäfts- und Produktionsprozesse wesentlichen Hard- und Softwarekomponenten und Leistungen (z. B. SaaS-

[33] Ein Cyberrisiko ist kritisch, wenn die möglichen Auswirkungen gravierend und in hohem Masse auch geschäftskritisch sind.

[34] Präventiv, detektiv und reaktiv wirkende TOMs dienen der Umsetzung der Funktionen PROTECT, DETECT und RESPOND. Die drei Funktionen sind wichtig und ergänzen sich gegenseitig. Für jedes relevante Risiko müssen geeignete TOMs definiert und implementiert werden, wobei detektiv und reaktive TOMs unbedingt erforderlich sind.

[35] Dabei müssen externe Mitarbeiter genauso berücksichtigt werden wie interne.

[36] Diese Anforderung gilt für alle (wesentlichen) Hard- und Softwarekomponenten der IT-Infrastruktur, unabhängig ob sie «On-Premises» betrieben oder als Dienstleistung von einem Cloud Service Provider (CSP) bezogen werden. Der Schutzbedarf bezieht sich auf die Bedeutung der Hard- und Softwarekomponenten bzw. der Informatikschutzobjekte für die damit unterstützten Geschäfts- und Produktionsprozesse, sowie auf die Akzeptanz der Auswirkungen bei einer Verletzung von Schutzzielen.

[37] Das gilt sowohl für die Information Technology (IT) als auch für die Operational Technology (OT) gemäss Anhang A.

	Dienstleistungen), sowie die Lieferanten mit privilegierten Zugriffsmöglichkeiten oder Zugang zu sensiblen Daten (z. B. bei erforderlichen Überwachungs- und Unterhaltsarbeiten) durch die Umsetzung von adäquaten TOMs selbst auch bestmöglich abgesichert und damit resilient sind.

3	**PROTECT (PR)**
3.1	**Physischer Schutz, Konfiguration und Betrieb** Jede Hard- und Softwarekomponente bzw. jedes aggregierte Informatikschutzobjekt muss so konfiguriert sein und betrieben werden, dass seine Angriffsfläche möglichst klein gehalten wird.[38] Insbesondere müssen (a) ein adäquater physischer Schutz[39] gegeben, (b) eine bestmögliche logische Abschottung und Isolierung (z. B. durch den Einsatz von Virtualisierungstechnologien) erreicht und (c) eine technische Härtung vorgenommen worden sein, wobei diese Härtung unter anderem bedeutet, dass • vordefinierte Konti entfernt[40] und • nicht benötigte Dienste deaktiviert sind, sowie • Änderungen an den Sicherheitseinstellungen physischer Geräte eine interaktive Bestätigung (z. B. das Drücken einer Taste) erforderlich machen, sowie (d) ineinandergreifende und voneinander unabhängige Komponenten die Möglichkeiten von Stör- und Unfällen bestmöglich verhindern.
3.2	**Schwachstellen- und Verwundbarkeitsmanagement** Jede Hard- und Softwarekomponente bzw. jedes aggregierte Informatikschutzobjekt muss im Rahmen des Lifecycles und im Hinblick auf bekannt gewordene Schwachstellen und Verwundbarkeiten vorzugsweise automatisiert überwacht[41] werden und gemäss Erfahrungswerten oder den Anweisungen des oder der Hersteller gewartet und auf möglichst aktuellem Stand gehalten werden (z. B. durch zeitnahes Einspielen von Patches oder

[38] Diese Anforderung folgt dem Motto: «Do not expose things on the Internet that do not need to be accessed by everyone».

[39] Auf der einen Seite hat der physische Schutz vor meteorologischen Naturgefahren, wie Hagel, Sturm, Regen, Schnee oder Blitzschlag, gravitativen Naturgefahren, wie Hochwasser, Murgang, Lawinen oder Steinschlag, sowie tektonischen und geologischen Gefahren, wie Erdbeben oder Radonemissionen, zu schützen. Auf der anderen Seite hat der physische Schutz aber auch den Zugang und die physische Zugriffsmöglichkeit für nur autorisierte Personen zu kontrollieren und z. B. auch mit Hilfe von Closed-Circuit Television (CCTV) Kameras zu überwachen und sicherzustellen.

[40] Damit existieren keine vordefinierten Zugangsdaten. Wenn solche für die Aktivierung erforderlich sind, müssen sie nach der Inbetriebnahme neu generiert und der Benutzerin oder dem Benutzer zugänglich gemacht werden.

[41] Zur Erkennung möglicher Verwundbarkeiten können Überwachungsdienste, wie z. B. der Shadowserver (https://www.shadowserver.org) verwendet werden. Für die kontinuierliche Überwachung von Schwachstellen sollen die vom Hersteller zur Verfügung gestellte Software Bill of Material (SBOM) und weitere Anweisungen mit herangezogen werden.

	Auswechseln von Komponenten). Bei vernetzten Geräten muss (wenn technisch möglich) ein automatisierter Firmware-Update-Mechanismus vorhanden und standardmässig aktiviert sein.
3.3	**Identitäts- und Zugriffskontrollmanagement** Jede Hard- und Softwarekomponente bzw. jedes aggregierte Informatikschutzobjekt muss in ein umfassendes Identitäts- und Zugriffskontrollsystem eingebunden sein, das sicherstellt, dass Zugriffe nur authentifiziert und autorisiert erfolgen können. (a) Ein Zugriff ist authentifiziert, wenn die Identität der zugreifenden Entität definiert und mit Hilfe eines dem Schutzbedarf entsprechenden Authentifikationsverfahrens, -mittels oder -dienstes verifiziert worden ist.[42] (b) Ein Zugriff ist autorisiert, wenn die Zugriffsrechte und Privilegien der zugreifenden Entität den Zugriff in dieser Form auch zulassen. Dabei muss die Vergabe von Zugriffsrechten und Privilegien möglichst minimal erfolgen («Least Privilege»-Prinzip).
3.4	**Netzwerksicherheit** Jede Hard- und Softwarekomponente bzw. jedes aggregierte Informatikschutzobjekt muss vor netzwerkbasierten Angriffen[43] adäquat geschützt sein. Ein solcher Schutz kann grundsätzlich auf zwei Arten erreicht werden: • Die Komponente oder das Informatikschutzobjekt wird in einem separaten Netzwerk(segment) betrieben,[44] das über einen geeigneten Perimeterschutz mit einer Beschränkung von Netzwerkdiensten, -protokollen und -ports verfügt (im Sinne einer Firewall). • Die Komponente oder das Informatikschutzobjekt verfügt selbst über geeignete Sicherheitsmechanismen und -vorkehrungen (im Sinne von «Zero» bzw. «Minimal Trust»[45]).

[42] Ein Zugriff kann interaktiv durch eine Benutzerin oder einen Benutzer oder nicht-interaktiv durch einen Dienst oder Prozess erfolgen. Weiter kann ein Zugriff auch über ein Verfahren zur Zurücksetzung von Authentifikationsschlüssel erfolgen. In allen Fällen sind die Anforderungen an die Authentifikation gleich. Für wissensbasierte Authentifikationsansätze, d. h. Ansätze, die darauf beruhen, dass die Benutzerinnen und Benutzer etwas wissen, mit dem sie sich authentifizieren können (z. B. ein Passwort oder ein kryptografischer Schlüssel), ist eine mögliche Klassifikation in drei Sicherheitsstufen in Anhang B vorgeschlagen. In jedem Fall muss die Authentifikation so gestaltet sein, dass sie nicht einfach neu initialisiert und damit umgangen werden kann. Alternativ zu wissensbasierten Authentifikationsansätzen kann die Anforderung auch mit anderen Authentifikationsansätzen oder mit physischen Massnahmen umgesetzt werden.

[43] Mit dieser Anforderung sollen in erster Linie «Pass-the-Hash»-Angriffe und sogenannte «Lateral Movements» verhindert werden. Letztere sind auch Gegenstand der Erweiterung von STRIDE zu STRIDE-LM.

[44] Im Rahmen der Netzwerksegmentierung sollte sichergestellt sein, dass mindestens IT- und OT-Systeme voneinander getrennt sind (d. h. in unterschiedlichen Segmenten betrieben werden).

[45] Der übliche Begriff lautet hier «Zero Trust». Weil aber immer Annahmen über Vertrauensverhältnisse gemacht werden müssen und diese minimal sein sollten, wird an dieser Stelle der Begriff «Minimal Trust» favorisiert und entsprechend verwendet.

3.5	**Malwareschutz** Jede Hard- und Softwarekomponente bzw. jedes aggregierte Informatikschutzobjekt muss Jede Hard- und Softwarekomponente bzw. jedes aggregierte Informatikschutzobjekt muss mit geeigneten Massnahmen[46] wirksam vor bösartiger Software (Malware) und datengetriebenen Angriffen[47] geschützt sein.
3.6	**Verschlüsselung und Löschung von Daten** Während ihrer Speicherung, Verarbeitung und Übertragung müssen Daten in Bezug auf ihre Vertraulichkeit und Integrität adäquat geschützt sein (z. B. mit Hilfe geeigneter kryptografischer Verfahren). Nicht mehr benötigte Daten müssen ihrem Schutzbedarf und regulatorischen Vorgaben entsprechend gelöscht werden.[48] Diese Anforderung betrifft nicht nur den Betrieb, sondern auch die Entwicklung von Systemen und Anwendungen.
3.7	**Datensicherung** Alle für die wichtigen Geschäfts- und Produktionsprozesse relevanten Daten müssen regelmässig gesichert werden. Idealerweise ist dazu ein Backupkonzept umzusetzen, das eine Online/Offline-Datenhaltung in mehreren Generationen an mehreren Standorten vorsieht. Zudem müssen zu jedem Zeitpunkt die Daten möglichst zeitnah und vollständig wieder hergestellt werden können, und die Datenwiederherstellung muss periodisch geübt werden.
3.8	**Entwicklung** Bei der Entwicklung von Hard- und Softwarekomponenten muss die Cybersicherheit von Anfang an mitberücksichtigt werden. Dazu gehören z. B. eine Bedrohungsmodellierung bei der Architekturplanung, das Einhalten von Richtlinien[49] und Erfahrungswerten bei der Umsetzung (bzw. die Vermeidung von unsicheren Praktiken), das Verwenden einer CI/CD-Plattform, die kontinuierliche Sicherheitsprüfungen miteinschliesst, die Gestaltung von

[46] Diese Anforderung muss nicht zwingend mit Hilfe von zusätzlicher Software erfüllt werden. In vielen Fällen reicht es aus, wenn die Bordmittel der eingesetzten Betriebssysteme eingesetzt werden und entsprechend konfiguriert sind. Zudem kann der Schutz auch durch die Prüfung von Daten und/oder Blockieren von nicht benötigten Daten während der Übertragung (d. h. vor dem Erreichen der Endsysteme) erfolgen.

[47] Bei einem datengetriebenen Angriff findet der Angriff über Daten statt, die in ein IT-System oder eine Anwendung eingespielt werden und dort ein Fehlverhalten auslösen.

[48] Ab einem bestimmten Schutzbedarf reicht eine logische Löschung auf der Stufe des Betriebssystems nicht aus. Stattdessen müssen die zu löschenden Daten mehrfach mit zufällig gewählten Daten überschrieben werden.

[49] Für die Softwareentwicklung bietet sich z. B. die Minimum Viable Secure Product (MVSP) Richtlinie an (https://mvsp.dev). Grundsätzlich müssen dabei die Prinzipien *Security by Design und Security by Default* bei der Entwicklung hineinfliessen. Security *by Default* bedeutet, dass die Informatikmittel so entwickelt, konfiguriert und betrieben werden, dass alle – in einem spezifischen Umfeld sinnvollen – Sicherheitsmassnahmen standardmässig aktiviert sind und ihre Wirkung entfalten können, ohne dass sich die Benutzerinnen und Benutzer darum kümmern müssen. Security *by Design* erwartet, dass bei der Entwicklung die Sicherheit von Anfang als integraler Bestandteil berücksichtigt ist.

	Schnittstellen (insbesondere der grafischen Benutzeroberflächen), die nicht zu Fehlern verleiten, sowie die sicherheitsbewusste Verwendung von integrierten Entwicklungsumgebungen und entsprechende Plugins durch die Entwickler. In jedem Fall müssen Entwicklungs- und produktive Umgebungen getrennt werden.
3.9	**Verfügbarkeit** Jede Hard- und Softwarekomponente bzw. jedes aggregierte Informatikschutzobjekt muss im Hinblick auf seine Verfügbarkeit gesichert sein. Insbesondere müssen dazu genügend Rechen-, Speicher- und Übertragungskapazitäten vorhanden und wichtige Komponenten wann immer sinnvoll auch redundant vorhanden sein.

4	**DETECT (DE)**
4.1	**Aufzeichnung und Überwachung** Für jede Hard- und Softwarekomponente bzw. jedes aggregierte Informatikschutzobjekt (und dabei insbesondere für Netzwerke) müssen sicherheitsrelevante Aktivitäten, Vorfälle und Ereignisse aufgezeichnet[50] und im Hinblick auf möglicherweise erfolgte Angriffe möglichst zeitnah und automatisiert ausgewertet werden (z. B. im Rahmen eines SOC).
4.2	**Meldestelle** Für jede Hard- und Softwarekomponente bzw. jedes aggregierte Informatikschutzobjekt muss ersichtlich sein, wie Aussenstehende Schwachstellen und sicherheitsrelevante Vorfälle melden können.[51]

5	**RESPOND (RS) und RECOVER (RC)**
5.1	**Vorfallmanagement** Vorfälle und erkannte Störungen, die die relevanten Geschäfts- und Produktionsprozesse beeinträchtigen können, müssen möglichst zeitnah triagiert und behoben werden.
5.2	**Notfallplanung** Für jede Hard- und Softwarekomponente bzw. jedes aggregierte Informatikschutzobjekt muss die Wiederherstellung der Betriebsfähigkeit

[50] Die Aufzeichnungen müssen in geeigneter Form während einer angemessenen Zeitspanne in nicht veränderbarer Form gespeichert und für die Sicherstellung der Nachvollziehbarkeit von sicherheitsrelevanten Aktivitäten wieder verfügbar gemacht werden können. Zur Erkennung einer möglichen Kompromittierung sollten hier auch «Canaries» eingesetzt werden.

[51] Dies kann im Rahmen einer über das Web verfügbaren security.txt-Datei gemäss RFC 9116 erfolgen.

	sichergestellt sein.[52] Dazu müssen Notfall- und Wiederherstellungspläne[53] definiert, priorisiert, regelmässig geübt und gegebenenfalls auch verbessert werden. Diese Pläne müssen in einen übergeordneten Notfallplan für die ganze Organisation oder das ganze Unternehmen eingebunden sein.
5.3	**Kommunikation** Für alle gemäss Anforderung 5.2 zu erstellenden Notfallpläne müssen die Verantwortlichkeiten und Zielsetzungen der Kommunikation bekannt sein.

[52] Dabei müssen auch die Abhängigkeiten in den IT-/OT-Lieferketten gemäss der Basisanforderung 2.2 und die Wiederverwendbarkeit der gesicherten Daten gemäss Basisanforderung 3.7 mitberücksichtigt sein.

[53] Die Erkenntnisse und Lehren aus früheren Sicherheitsvorfällen und allfälligen Simulationen müssen in diesen Plänen mitberücksichtigt werden.