Cybersicherheits- und Resilienzmethode (CSRM)

Am 24. November 2025 hat das Bundesamt für Cybersicherheit (BACS) die Cybersicherheits- und Resilienzmethode vorgestellt. Es ist eine strukturierte Vorgehensweise zur Stärkung der Cybersicherheit und Resilienz. In Zusammenarbeit mit ausgewählten Partnern und interessierten Kreisen wird die CSRM zurzeit ausgetestet und weiterentwickelt. Trotzdem lohnt sich schon jetzt ein Blick in das öffentlich verfügbare Dokument.

Das Bundesamt für Cybersicherheit (BACS) hat mit der Cybersicherheits- und Resilienzmethode (CSRM) einen strukturierten, aber bewusst pragmatischen Ansatz entwickelt, um die Cybersicherheit und die Cyberresilienz von Organisationen und Unternehmen zu verbessern. Die Methode ist unabhängig von der Branche und richtet sich ausdrücklich auch an kleine Organisationen, die kein komplexes Risiko-Framework erstellen wollen oder können.

Die CSRM folgt international anerkannten Standards und Best Practices, vor allem dem NIST Cybersecurity Framework (CSF) sowie den bewährten IT-Sicherheitsvorgaben der Bundesverwaltung. Sie entscheidet sich dabei bewusst gegen eine vollständige, quantitative Risikoanalyse. Stattdessen wird ein qualitativ risikobasierter Ansatz verfolgt, der sich an den tatsächlichen Auswirkungen von IT-Sicherheitsvorfällen auf die wichtigen Tätigkeiten und Prozesse einer Organisation orientiert.

Im Mittelpunkt steht der erweiterte Grundschutzansatz: Eine festgelegte Menge von Basisanforderungen gilt grundsätzlich für alle Informatikschutzobjekte und muss unabhängig vom individuellen Schutzbedarf umgesetzt werden. Wenn ein erhöhter Schutzbedarf erkannt wird, werden zusätzliche technische und organisatorische Massnahmen (TOMs) ergänzt.

In der mittelfristigen Zukunft könnte die CSRM auch als mögliche Alternative zum IKT-Minimalstandard des Bundesamts für wirtschaftliche Landesversorgung fungieren.

Übersicht über die Methode

Die CSRM vereint den Grundschutz mit einem Fünf-Schritte-Ansatz. Der Grundschutz legt über Basisanforderungen fest, was zu beachten ist, während die fünf Schritte Sicherheitsüberlegungen zu einzelnen Informatikschutzobjekten anstellen. Die Methode umfasst keine Verwundbarkeiten in spezifischen Produkten oder Implementierungen; diese sind im operativen Betrieb zu behandeln. Die fünf Schritte sind:

1 Analyse der wichtigen Tätigkeiten
2. Bestimmung der Informatikschutzobjekte
3. Schutzbedarfsanalyse
4. Sicherheitskonzipierung
5. Umsetzung

Für jedes Informatikschutzobjekt sind die Schritte 3 bis 5 einzeln auszuführen. Die organisatorische Strukturierung – wie Rollen, Verantwortlichkeiten oder Genehmigungsprozesse – bleibt absichtlich offen und sollte an die jeweilige Organisation angepasst werden.

Schritt 1: Analyse der wichtigen Aufgaben

Die CSRM setzt nicht die IT, sondern die wichtigen Tätigkeiten und damit zusammenhängenden Geschäfts- und Produktionsprozessen in den Mittelpunkt. Als Erstes ist es relevant, die wichtigen Aktivitäten der Organisation oder des Unternehmens zu bestimmen, einschliesslich der damit verbundenen Geschäfts- und Produktionsprozesse.

Durchführung

Die Analyse wird in zwei Schritten durchgeführt. Als Erstes werden die relevanten Prozesse identifiziert, die unbedingt notwendig sind, um strategische und wirtschaftliche Ziele zu erreichen. Es können bestehende Prozessdokumentationen, SOPs, Interviews oder Workshops als Grundlage dienen. In der Regel ist die Anzahl dieser Prozesse überschaubar.

Danach erfolgt eine detaillierte Analyse der Abläufe mit Fokus auf Cybersicherheit und Resilienz. Zwei Aspekte stehen dabei im Mittelpunkt:

- Prozessziele, die ein Primärziel (zum Beispiel Leistungserbringung oder Produktion) sowie mehrere Sekundärziele wie Sicherheit, Compliance, Schutz vor Stör- und Unfällen oder der Schutz geistigen Eigentums umfassen. Für jedes Ziel werden die maximal zulässigen Abweichungen festgelegt.
- Prozessdaten, die eine strukturierte Darstellung des Prozesses ermöglichen (Metadaten über einen Prozess), wie Eingaben, Ressourcen, Arbeitsschritte, Abhängigkeiten, Rahmenbedingungen und potenzielle Störungen.

Es ist keine klassische Risikoanalyse vorgesehen; stattdessen geht es um ein realistisches Verständnis des Prozesses und seiner Sensitivitäten.

Ergebnisse

Das Ergebnis ist eine dokumentierte und nachvollziehbare Be-

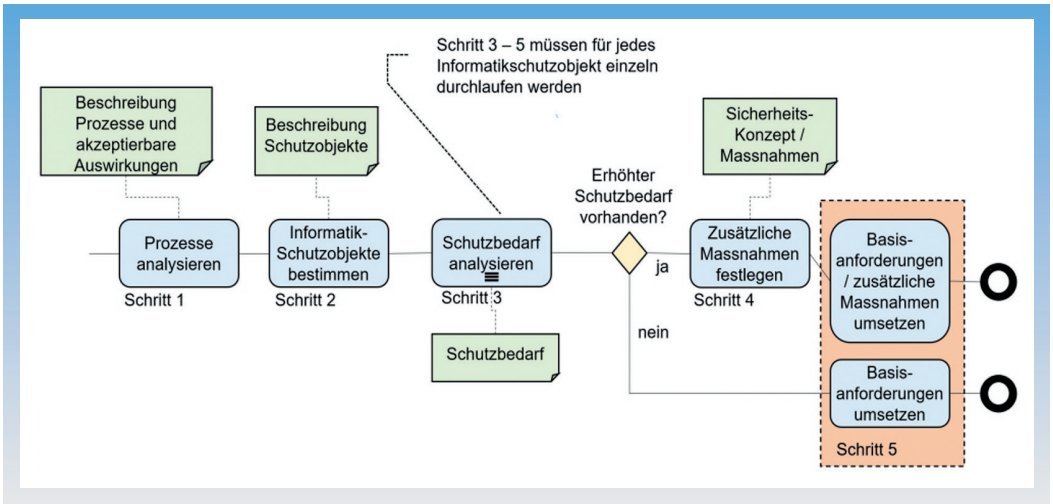

Bild: Bundesamt für Cybersicherheit BACS

BPMN-Spezifikation der SCRM.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

schreibung der relevanten Prozesse, die eine grafische Darstellung sowie eine strukturierte Beschreibung der Prozessziele und -daten umfasst. Diese Dokumentation ist die Basis für alle weiteren Aktionen.

Schritt 2: Informatikschutzobjektbestimmung

Im zweiten Schritt wird die IT-Infrastruktur entlang der zuvor analysierten Prozesse in sogenannte Informatikschutzobjekte gegliedert.

Ein Informatikschutzobjekt besteht aus einer logisch verbundenen Gruppe von Informatikmitteln – wie Anwendungen, Plattformen oder Datenbeständen –, die alle einem gemeinsamen Zweck dienen.Die CSRM unterscheidet sich hier bewusst von den traditionellen Asset-Ansätzen, indem sie Aggregation erlaubt und sogar fördert. Das Ziel ist es, die Komplexität beherrschbar zu halten und Sicherheitsmassnahmen kohärent umzusetzen.

Durchführung

Die Bestimmung erfolgt typischerweise in drei Teilschritten:

1 Ermittlung der prozessrelevanten Anwendungen
2. Zuordnung der benötigten Informatikmittel (Hard-, Software und Daten)
3. Überprüfung, Vereinfachung und sinnvolle Aggregation zu Schutzobjekten

Dabei wird akzeptiert, dass es keine «eine richtige» Lösung gibt. Überschneidungen zwischen Schutzobjekten sind möglich, sollen jedoch minimiert werden.

Ergebnisse

Jedes Informatikschutzobjekt wird dokumentiert, unter anderem mit Namen, Beschreibung, zugehörigen Prozessen, eingesetzten Komponenten (Hard- und Software), Datenflüssen, beteiligten Personen sowie relevanten physischen und organisatorischen Rahmenbedingungen.

Schritt 3: Schutzbedarfsanalyse

Für jedes Informatikschutzobjekt wird nun geprüft, ob ein erhöhter Schutzbedarf besteht. Die Analyse basiert auf den Prozesszielen und den maximal zulässigen Abweichungen aus Schritt 1.

Durchführung

Zunächst wird ein Datenverzeichnis erstellt, in dem die relevanten Datengruppen strukturiert erfasst werden. Anschliessend wird qualitativ beurteilt, welche Auswirkungen eine Verletzung der IT-Schutzziele – insbesondere Vertraulichkeit, Integrität und Verfügbarkeit – auf die Prozesse hätte. Führt eine solche Verletzung zu nicht akzeptablen Abweichungen, gilt der Schutzbedarf als erhöht. Am Schluss muss eine Schutzbedarfsanalyse im Hinblick auf Plausibilität und Konsistenz geprüft werden.

Ergebnisse

Das Ergebnis ist ein binärer Entscheid: erhöhter Schutzbedarf ja oder nein. Bei positivem Entscheid liefern die detaillierten Bewertungen eine wichtige Grundlage für die nachfolgende Sicherheitskonzipierung.

Schritt 4: Sicherheitskonzipierung

Für Informatikschutzobjekte mit erhöhtem Schutzbedarf wird ein Sicherheitskonzept erstellt. Dieses beschreibt zusätzliche TOMs, die über den Grundschutz hinausgehen sowie deren konkrete Umsetzung.

Durchführung

Die Sicherheitskonzipierung umfasst drei Teilschritte:

1. Bedrohungsmodellierung, empfohlen auf Basis von STRIDE-LM
2. Auswahl geeigneter TOMs anhand qualitativer und technologischer Überlegungen
3. Erstellung des Sicherheitskonzepts mit klaren Spezifikationen

Der Fokus liegt darauf, nicht akzeptable Auswirkungen durch präventive, detektive und reaktive Massnahmen zu vermeiden oder zu begrenzen.

Hinweis: 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. Der Name ist ein Akronym, das sich aus den Anfangsbuchstaben der ursprünglich sechs Kategorien von Sicherheitsbedrohungen zusammensetzt, die im Rahmen von STRIDE unterschieden werden: Spoofing (Identitätsverschleierung), Tampering (Manipulation), Repudiation (Ablehnung), Information disclosure (Verletzung der Privatsphäre oder Datenabfluss), Denial of service (Verfügbarkeit des Dienstes beeinträchtigen) und Elevation of privilege (Rechteausweitung). Das Modell wurde im Hinblick auf aktuelle Bedrohungen in Netzwerken um die Kategorie «Lateral Movement» (LM) ergänzt worden.

Ergebnisse

Resultat ist ein dokumentiertes Sicherheitskonzept, das als verbindliche Grundlage für die Umsetzung und den Betrieb dient.

Schritt 5: Umsetzung

Im letzten Schritt werden die definierten TOMs umgesetzt und in den operativen Betrieb überführt. Dabei sind Zuständigkeiten klar zu regeln, auch im Zusammenspiel mit Lieferanten oder Dienstleistern. Der Betrieb wird als kontinuierlicher, zirkulärer Prozess verstanden, der Überwachung, Verbesserung und gegebenenfalls Rückbau unwirksamer Massnahmen einschliesst.

Beurteilung und Leistungsvergleich

Die CSRM versteht Cyberresilienz als besser überprüfbare Zielgrösse als klassische IT-Sicherheit. Entsprechend definiert sie sechs Prüfziele, die von der Kenntnis der Prozesse über umgesetzte TOMs bis hin zum Umgang mit Vorfällen und Drittparteien reichen. Diese Prüfziele ermöglichen Benchmarking und gezielte Weiterentwicklung.

Anhänge

Die Anhänge liefern ergänzende Definitionen zentraler Begriffe, eine Einteilung von Authentifikationsverfahren in Sicherheitsstufen sowie eine Sammlung von Basisanforderungen, die sich am NIST CSF orientieren. Sie dienen als Referenz und unterstützen die praktische Anwendung der Methode, ohne den methodischen Kern zu verändern.

Einordnung der CSRM im Verhältnis zur ISO/IEC 27001

Die CSRM ist kein Ersatz für ein ISMS nach ISO/IEC 27001. Wer das Dokument mit dieser Erwartung liest, wird zwangsläufig enttäuscht sein – und übersieht gleichzeitig seinen Wert. Die CSRM versteht sich nicht als Norm, nicht als Zertifizierungsrahmen und nicht als vollständiges Managementsystem im formalen Sinn. Sie ist eine Methode, kein Standard.

Fazit

Die Cybersicherheits- und Resilienzmethode (CSRM) des BACS verfolgt einen bewusst pragmatischen Ansatz, um die Cybersicherheit und Resilienz zu stärken, ohne dass eine formale Risikoanalyse erstellt werden muss. Begonnen wird nicht mit IT-Systemen, sondern mit den wesentlichen Tätigkeiten sowie den Geschäfts- oder Produktionsprozessen einer Organisation. Informatikschutzobjekte werden über einen verbindlichen Grundschutz und ein klar strukturiertes Fünf-Schritte-Verfahren identifiziert: Ihr Schutzbedarf wird bestimmt und es werden gezielt zusätzliche Massnahmen definiert, wenn dies erforderlich ist. Download mittels QR-Code.