Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS
Analyse und Prävention

14. Januar 2025

Technologiebetrachtung

Cybersicherheitsmanagement

1 Einführung

In der Informationsgesellschaft spielen Informationen für Organisationen und Unternehmen eine wichtige Rolle. Dabei werden Informationen meist als Daten codiert und elektronisch gespeichert, verarbeitet und übertragen. Aufgrund ihrer grossen Bedeutung müssen solche Daten im Hinblick auf bestimmte Schutzziele abgesichert sein, wie z. B. Vertraulichkeit, Integrität (bzw. Authentizität) und Verfügbarkeit. Diese Absicherung stellt eine herausfordernde (Management-)Aufgabe dar, die auch etwa als *Informations-* oder *Cybersicherheitsmanagement* bezeichnet wird und sinnvollerweise durch ein entsprechendes Managementsystem – ein sogenanntes Informationssicherheitsmanagementsystem (ISMS) – unterstützt wird.

Im Rahmen dieser Technologiebetrachtung wird untersucht, was ein ISMS genau ist, was es zu leisten imstande ist und wie es die mit der Gewährleistung der Cybersicherheit einer Organisation oder eines Unternehmens betraute Person oder Personengruppe bestmöglich unterstützen kann. Dabei werden insbesondere auch die Fragen untersucht, was (Cyber-)Risiken sind und wie mit ihnen im Rahmen eines Cybersicherheitsmanagements bzw. ISMS sinnvollerweise umzugehen ist. Zu beachten ist, dass viele Überlegungen auch auf andere Managementsysteme zutreffen und dass ein Managementsystem jeweils im Kontext eines (Management-)Modells zu betrachten ist, in dem z. B. politische, strategische, taktische und operative Ebenen unterschieden werden können. Auf die Einbettung eines ISMS (oder eines anderen Managementsystems) in ein solches Modell wird im Folgenden nicht weiter eingegangen.

2 Begriffsdefinition

Aufgrund seiner breit ausgelegten Funktion gibt es in der Literatur viele Definitionen für den Begriff eines ISMS. Gemäss DIN EN ISO/IEC 27000[1] umfasst es z. B. «Politik, Verfahren, Richtlinien und damit verbundene Ressourcen und Tätigkeiten, die alle von einer Organisation gesteuert werden, um ihre Informationswerte zu schützen», und ist damit «ein systematisches Modell für die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Pflege und die Verbesserung der Informationssicherheit einer Organisation, um Geschäftsziele zu erreichen». Eine etwas weniger umfassende und dadurch spezifischere

[1] Deutsche Fassung von ISO/IEC 27000:2016 Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie.

Definition findet sich auf Wikipedia, wonach ein ISMS «die Aufstellung von Verfahren und Regeln innerhalb einer Organisation» ist, «die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern»[2]. Auf dieser Definition aufbauend, verwendet das Bundesamt für Cybersicherheit (BACS) folgende praxisorientierte Definition als Grundlage für diesbezügliche Arbeiten:

«Ein ISMS ist ein aus Verfahren und Regeln bestehendes System, das in einer Organisation oder einem Unternehmen eingesetzt werden kann, um die Cybersicherheit zu gewährleisten, d. h. konkrete Sicherheitsziele zu definieren und deren Erreichung zu planen, steuern und sicherzustellen.»

Obwohl diese Definition besagt, dass ein ISMS ein aus Verfahren und Regeln bestehendes System ist, das der Erreichung von definierten Cybersicherheitszielen dient, bleibt der darunterliegende Systembegriff undefiniert. Im einfachsten Fall kann ein ISMS einfach aus Vorgaben bestehen, die als Verfahren und Regeln oder auch nur aus einer Liste von regelmässig durchzuführenden Aktivitäten formuliert sind. Darüber hinaus kann ein ISMS aber auch Hilfsmittel und Werkzeuge umfassen, welche die mit dem Informationssicherheitsmanagement betraute Person oder Personengruppe in ihrer Arbeit unterstützen. Solche Werkzeuge können unterschiedlich komplex sein. Leider wird die Bedeutung von Werkzeugen oft überschätzt oder der Begriff eines ISMS wird sogar mit einem oder mehreren Werkzeugen gleichgesetzt. Getreu dem Sprichwort[3] «a fool with a tool is still a fool» kann man auch die gegenteilige Meinung vertreten, dass der Begriff ISMS unabhängig von Werkzeugen zu definieren ist und a priori nichts mit Werkzeugen zu tun hat. Allenfalls stellt sich nach einer Ausformulierung eines adäquaten ISMS die Frage, mit welchem Werkzeug oder mit welchen Werkzeugen sich dieses ISMS bestmöglich umsetzen oder unterstützen lässt. Diese Frage darf aber die Spezifikation eines ISMS weder steuern noch inhaltlich beeinflussen. Somit bestimmt das ISMS die Anforderungen, denen das Werkzeug zu folgen hat, nicht umgekehrt.

Neben der Unabhängigkeit von bestimmten Werkzeugen ist aus Sicht des BACS ein zweiter Punkt für den praktischen Einsatz eines ISMS entscheidend: Das Verständnis von Risiken und wie mit ihnen umgegangen wird. Üblicherweise werden hier von externen und internen Bedrohungen ausgehende (d. h. bedrohungsbedingte) Risiken betrachtet. Alternativ dazu können aber auch Risiken betrachtet werden, die sich auf Auswirkungen beschränken. So ist beim Risiko eines Datenverlusts z. B. primär der Datenverlust relevant. Ob dieser Verlust durch menschliches Fehlverhalten, technisches Versagen oder Malware verursacht worden ist, spielt bei der Einschätzung des von einem Datenverlust ausgehenden Risikos keine entscheidende Rolle. Es handelt sich in jedem Fall um ein Risiko, das es unter allen Umständen zu mitigieren (verringern) gilt – unabhängig von der ursächlichen Bedrohung. Entsprechend kann man versuchen, ein Informationssicherheitsmanagement nur auf der Basis von solchen (d. h. auswirkungsbedingten) Risiken aufzubauen. Dazu ist es aber sinnvoll, vorgängig noch der Umgang mit Risiken etwas zu vertiefen.

---

[2] https://de.wikipedia.org/wiki/Information_Security_Management_System

[3] Obwohl der Ursprung des Sprichwortes nicht restlos geklärt ist, wird es meist dem US- amerikanischen Informatiker Grady Booch zugeschrieben. Um die Kernaussage des Sprichwortes noch zu verschärfen oder zuzuspitzen, könnte man auch sagen: «A fool with a tool is a more foolish fool». Alternativ dazu könnte man Abraham Maslow zitieren, dem das folgende Sprichwort zugeschrieben wird: «If all you have is a hammer, everything looks like a nail». Damit hat er suggeriert, dass ein bestimmtes Werkzeug eben nicht zur Lösung aller Probleme eingesetzt werden kann.

3 Umgang mit Risiken

Im Volksmund bezeichnet ein Risiko einfach eine Bedrohung oder eine Gefahr, deren Überwindung mit einem Wagnis verbunden sein kann. Entsprechend breit ist der Risikobegriff definiert und ein bestimmtes Risiko kann subjektiv sehr unterschiedlich empfunden werden. Das gilt sogar für Risiken, die objektiv gesehen zwar quantifizierbar sind, wie z. B. das Risiko eines Flugzeugabsturzes[4]. Diese Risiken sind aber für die Betrachterin oder den Betrachter abstrakt und werden individuell unterschiedlich wahrgenommen und eingeschätzt. Entsprechend gibt es Menschen, die weitgehend sorglos in ein Flugzeug einsteigen, während andere Menschen unter den gleichen Voraussetzungen eine eigentliche Aviophobie entwickeln. Für beide ist das Risiko zwar das gleiche, es wird aber individuell unterschiedlich wahrgenommen und eingeschätzt.

Trotz unterschiedlicher Risikowahrnehmung und -einschätzung ist in der Cybersicherheit im Allgemeinen und im Informationssicherheitsmanagement im Speziellen die Meinung verbreitet, dass man Risiken quantifizieren und alle Informationssicherheitsmanagemententscheide entlang von quantifizierten Risiken fällen kann. Man spricht in diesem Zusammenhang auch etwa von einem «risikobasierten» Ansatz. Damit ist meist ein Ansatz gemeint, bei dem für jede Bedrohung – ausgehend von einer definierten Menge von Bedrohungen – ein Einzelrisiko und ein Gesamtrisiko als Summe aus allen Einzelrisiken berechnet werden kann. Dabei wird ein Einzelrisiko als Produkt einer Eintrittswahrscheinlichkeit und einer Schadenshöhe abgeschätzt.

Diese einfache Risikoformel hat über lange Zeit die Diskussionen im Informationssicherheitsmanagement (auch im Zusammenhang mit ISMS) beherrscht und dominiert diese nach wie vor. Als Begründung für einen risikobasierten Ansatz wird dabei oft auf die Versicherungswirtschaft verwiesen, die seit jeher Risiken quantifiziert und damit ein erfolgreiches Geschäftsmodell betreibt. Das funktioniert für Risiken, die wir aus dem täglichen Leben kennen und für die insbesondere statistisch relevante Aufzeichnungen von Eintrittswahrscheinlichkeit und zugehörigem Schadensausmass existieren. Das ist z. B. bei Diebstahl- oder Unfallversicherungen gegeben. Fehlen solche statistisch relevanten Aufzeichnungen für Risiken, ist die versicherungstechnische Situation komplizierter. Hier werden manchmal Versicherungslösungen versuchsweise auf dem Markt angeboten und dann laufend an die zwischenzeitlich gemachten Erfahrungswerte angepasst. So können über die Zeit Versicherungsangebote entstehen, obwohl im vornherein nicht klar war, wie Risiken berechnet werden sollten und ein sinnvolles Versicherungsangebot aussehen könnte. Genau das passiert im Moment auch im Bereich der Cybersicherheit, so dass potenzielle Kunden die ihnen vorgelegten Versicherungsangebote im konkreten Einzelfall prüfen müssen. Diese können sich in Bezug auf den Abdeckungsgrad bei Schadensfällen und den Umfang von Unterstützungsleistungen erheblich unterscheiden. Auf keinen Fall kann aber aus der Existenz einer Versicherung geschlossen werden, dass man alle in diesem Bereich möglicherweise auftretenden Risiken versteht und sinnvoll berechnen und quantifizieren kann. Dort, wo belastbare Daten fehlen, werden Annahmen getroffen und die Datenbasis erst im Laufe der Zeit aufgebaut.

Aus Sicht des BACS ist ein auf Risiken fokussierender Ansatz zwar grundsätzlich richtig. Allerdings muss die Art und Weise, wie Cyberrisiken – d. h. Risiken im Cyberraum – betrachtet werden und wie mit ihnen umgegangen wird, überdacht und angepasst werden. Zunächst einmal gibt es im Cyberraum keine «definierte Menge von Bedrohungen». Selbst wenn es eine solche Menge gäbe, wären die einzelnen Elemente, welche eine Bedrohung darstellen,

[4] Dieses Risiko lässt sich z. B. mit einer Division der Anzahl Flugzeugabstürze durch die Anzahl Flugbewegungen (pro Zeiteinheit und Fluggesellschaft) quantifizieren.

nicht elementar und könnten auch nicht abschliessend aufgezählt werden. Damit kann kein sinnvoller Wahrscheinlichkeitsraum definiert werden,[5] so dass die Wahrscheinlichkeitstheorie eigentlich nicht eingesetzt werden kann und das Rechnen mit Eintrittswahrscheinlichkeiten nicht definiert und beliebig willkürlich ist [1].[6]

Selbst abgesehen von dieser formalen Schwierigkeit ist das Abschätzen von Wahrscheinlichkeiten für Bedrohungen im Cyberraum aufgrund der fehlenden statistischen Aufzeichnungen und der hohen Dynamik und Komplexität kaum möglich. Wie wäre z. B. die Wahrscheinlichkeit der Bedrohung eines Datenabflusses sinnvoll abzuschätzen? Hier lässt sich fast jeder Wert einsetzen und begründen. Das gilt auch für die Schadenshöhe; auch hier lässt sich fast jeder Betrag begründen, insbesondere wenn man auch Folgeschäden mitberücksichtigt. So kann z. B. ein fehlerhaftes Update unter bestimmten Umständen zu einem kaum bemerkbaren und in der Höhe vernachlässigbaren Schaden führen, während es in anderen Fällen, wie z. B. beim Crowdstrike-Vorfall aus dem Jahre 2024, zu einem Schaden in Milliardenhöhe führen kann (und selbst hier weichen die geschätzten Beträge um mehrere Milliarden voneinander ab). Mit dieser Schwierigkeit der Abschätzung von Eintrittswahrscheinlichkeiten und Schadenshöhen ist die oben erwähnte einfache Risikoformel nicht sinnvoll anwendbar oder muss wenigstens angepasst oder ergänzt werden. Leider ist eine solche Anpassung oder Erweiterung bis heute nicht erfolgt, so dass die Risikoformel nicht praktikabel und bis zu einem gewissen Grad sogar illusorisch ist.

Anstelle eines formalen Umgangs mit Risiken wird in der Realität in vielen Fällen heuristisch mit Risiken umgegangen [2, 3]. Als Beispiel kann die Arbeitsweise einer allgemein praktizierenden Ärztin oder eines allgemein praktizierenden Arztes herangezogen werden. Um die Gesundheit einer Patientin oder eines Patienten sicherzustellen, wird weder eine definierte Menge von Krankheiten abgearbeitet noch mit Eintrittswahrscheinlichkeiten und Schadenshöhen argumentiert. Stattdessen wird versucht, mit Hilfe von Hintergrundwissen und punktuellen Messungen den Gesundheitszustand der Patientin oder des Patienten möglichst gut zu erfassen, um dann zielgerichtet und auf der Basis von Heuristiken eine passende Medikation vorzuschlagen. Darüber hinaus werden unabhängig vom Gesundheitszustand der Patientin oder des Patienten grundsätzliche Ratschläge erteilt, die immer gültig sind, wie z. B. eine gesunde Ernährung sowie regelmässige körperliche Betätigung. Einen ähnlichen Ansatz, der einen Grundschutzansatz mit punktuellen und zielorientierten Erweiterungen kombiniert, bietet sich auch in der Cybersicherheit bzw. im Informationssicherheitsmanagement und im Aufbau und Betrieb eines ISMS an.

4 Schlussfolgerungen und Ausblick

Ein ISMS hat die mit dem Cybersicherheitsmanagement betraute Person oder Personengruppe bestmöglich zu unterstützen. Obwohl die so avisierte Unterstützungsfunktion suggeriert, dass es sich bei einem ISMS um ein Werkzeug handelt, ist diese Eigenschaft nur sekundär. Primär besteht ein ISMS aus Verfahren und Regeln, die zwar im Rahmen eines Werkzeuges implementiert sein können, was aber nicht zwingend ist. Neben dem Fokus auf Verfahren und Regeln (statt Werkzeugen) ist es auch sinnvoll, sich im Cybersicherheitsmanagement und im Umgang mit Cyberrisiken von Risikoberechnungen zu verabschieden und

[5] Formal gesehen besteht ein Wahrscheinlichkeitsraum aus einem Ereignisraum und einem Wahrscheinlichkeitsmass, das jedem Ereignis eine Wahrscheinlichkeit (d. h. eine reelle Zahl zwischen 0 und 1) zuordnet, wobei drei Axiome von Kolmogorow erfüllt sein müssen.

[6] Allenfalls könnte man die Wahrscheinlichkeitstheorie nutzen, wenn man für jede Bedrohung einen eigenen (einelementigen) Wahrscheinlichkeitsraum definieren würde. Allerdings müsste dann jeder Bedrohung in einem solchen Wahrscheinlichkeitsraum auch die Wahrscheinlichkeit 1 zugeordnet sein (um die Axiome von Kolmogorow zu erfüllen), was die Nützlichkeit dieses Ansatzes insgesamt in Frage stellt.

stattdessen heuristische Ansätze zu nutzen. Wie die Gesundheit in der Medizin ist auch die Sicherheit im Cyberraum zu komplex, als dass sie auf einfache Formeln reduziert werden könnte. Heuristiken sind eher geeignet, der Komplexität der Cybersicherheit gerecht zu werden.

Auf der Grundlage dieser Erkenntnisse erarbeitet das BACS zurzeit eine strukturierte Vorgehensweise bzw. Methode zur Stärkung der Cybersicherheit und Resilienz. Die Methode wird öffentlich zugänglich gemacht und kann von allen Organisationen und Unternehmen unabhängig von Grösse und Branchenzugehörigkeit eingesetzt werden, um sich zielgerichtet auf die für sie relevanten Bedrohungen vorzubereiten und ein den Ausführungen dieses Dokumentes entsprechendes ISMS aufzubauen und zu betreiben. Natürlich kann ein solches ISMS dann schrittweise erweitert und in vielerlei Hinsicht auch weiter ausgebaut werden.

Referenzen

[1] 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

[2] 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

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