Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS
Analyse und Prävention

10. Juni 2025

Mess- und Prüfbarkeit der IT-Sicherheit

1. Einleitung

«Alles messen, was messbar ist, und messbar machen, was noch nicht messbar ist» ist ein Zitat, das dem italienischen Universalgelehrten, Mathematiker und Physiker Galileo Galilei zugeschrieben wird.[1] Spezialisten der Informatiksicherheit sehen sich heute vor vergleichbare Herausforderungen gestellt. Das Management von Unternehmen und Organisationen verlangt Auskunft über den Stand der eigenen IT-Sicherheit oder über diejenige ihrer Lieferanten. Ähnliche Fragestellungen sind Gegenstand öffentlicher Diskussionen. Immer wieder wird gefordert, dass die IT-Sicherheit von Produkten, Dienstleistungen und Organisationen geprüft wird, bevor man sie einsetzt, nutzt oder mit den entsprechenden Dienstleistern zusammenarbeitet.

Bis heute sind zahlreiche Versuche unternommen worden, um die IT-Sicherheit zu messen. Sich die Messergebnisse, respektive die Erreichung einer definierten «IT-Zielsicherheit» bestätigen zu lassen (insbesondere in Form von Zertifikaten) ist heute verbreitet und wird im Zusammenhang mit der Erfüllung von Compliance-Anforderungen oder der Vergabe von Aufträgen häufig verlangt. Dienstleistungen rund um die Zertifizierung der IT-Sicherheit haben sich inzwischen zu einem lukrativen Geschäftsmodell entwickelt.

Trotzdem bleibt die Frage, wie sich IT-Sicherheit nachhaltig verbessern lässt, und ob dazu deren Messung, Prüfung und allenfalls sogar Zertifizierung notwendige Voraussetzungen sind. Es mag mehr als eine Antwort auf diese Frage geben und «Wunderwaffen» zur Verbesserung der IT-Sicherheit gibt es keine. Dennoch ist das Bundesamt für Cybersicherheit (BACS) überzeugt, dass es komplementäre oder alternative Ansätze zu den heute weit verbreiteten Methoden zur Mess- und Prüfbarkeit der IT-Sicherheit braucht.

Bevor in vier Thesen auf diese Thematik eingegangen wird, soll zunächst die aktuelle Situation und die zugrunde liegende Problemstellung näher betrachtet werden [1].[2]

2. Problemstellung

Um sinnvoll messen zu können, muss zunächst definiert werden, was man genau unter der zu messenden «Grösse» versteht. Die Aussage ist trivial, aber passende Definitionen der «Sicherheit» als Messgrösse im Allgemeinen und der «IT-Sicherheit» im Besonderen sind

[1] Es gibt allerdings keine historischen Belege dafür, dass Galilei diesen Satz tatsächlich gesagt hat. Dennoch gilt das Zitat als sinnbildlich für Galileis Haltung, welche die (naturwissenschaftliche) Forschung bis heute zutiefst prägt.

[2] Die im nächsten Abschnitt folgende Darstellung ist eine Zusammenfassung aus [1]. Dort finden sich weitere für das Verständnis nützliche Erklärungen und Ausführungen.

nicht leicht zu finden. Nachdem diese Schwierigkeit beleuchtet ist, werden zwei Ansätze zur Messung der IT-Sicherheit vorgestellt, die allerdings beide mit erheblichen Nachteilen verbunden sind.

a. Definition

Eine Definition für «Sicherheit» ist schwierig, weil sie je nach Kontext und Anwendungsgebiet unterschiedlich ausfallen kann. Bei allen Definitionen geht es aber im Kern darum, dass es in einer bestimmten Situation keine ernstzunehmenden Gefahren, Bedrohungen und Risiken gibt. Sicher ist dann, wer sich auf alle möglichen Eventualitäten hinreichend gut vorbereitet hat und stets geeignet reagieren kann. Was aber «ernstzunehmende» Gefahren, Bedrohungen und Risiken sind, wie eine «hinreichend gute» Vorbereitung aussieht und was «geeignete» Reaktionen sind, hängt nicht nur von der Situation, sondern auch vom Betrachter ab. Damit ist der Begriff der Sicherheit subjektiv geprägt und unter anderem vom Empfinden und der Risikobereitschaft des Betrachters abhängig, sodass es keine präzise und für alle stimmige Definition geben kann. Ist ein Begriff wie die «Sicherheit» aber subjektiv geprägt, sowie nicht präzis und für alle stimmig definierbar, ist eine Messung oder Prüfung – gemäss der Maxime «if you can't define it, you can't measure it» [2] – ebenfalls nicht oder nur mit Einschränkungen möglich. Die Schwierigkeit ergibt sich insbesondere daraus, dass zwar eine Metrik oder Prüfkriterien erforderlich wären, die klar und eindeutig sind, dass sich solche aber aufgrund der unpräzisen Definition nicht finden lassen.

b. Messbarkeit – verifizierende und falsifizierende Ansätze

Oft behilft man sich damit, wenigstens Eigenschaften und Merkmale zu finden, die für den Begriff charakteristisch und bis zu einem gewissen Grad auch mess- oder prüf-, respektive verifizierbar sind. Bei so einem, sogenannten *verifizierenden Ansatz,* muss für den Begriff eine einfachere Definition konstruiert werden, damit eine Verifikation möglich wird [1]. Eine naheliegende Möglichkeit besteht darin, die IT-Sicherheit durch eine oder mehrere Eigenschaften oder Merkmale zu ersetzen, die gemessen und damit verifiziert werden können. Man denke hier etwa an die klassische CIA-Triade, in der die IT-Sicherheit durch die drei Eigenschaften Vertraulichkeit (Confidentiality), Integrität (Integrity) and Verfügbarkeit (Availability) ersetzt wird. Ein IT-System wird dann als sicher bezeichnet, wenn es in der Lage ist, die Vertraulichkeit, Integrität und Verfügbarkeit der gespeicherten, verarbeiteten und übertragenen Daten zu schützen. Das Zerlegen einer komplexen, schwer handhabbaren Systemeigenschaft wie der IT-Sicherheit in Teilaspekte, soll deren Mess- und Prüfbarkeit erhöhen, was aufgrund inhärenter Komplexität dennoch nur begrenzt möglich ist.[3]

Ein weitergehender Versuch, die IT-Sicherheit zu definieren und zu messen, ist die Entwicklung der Common Criteria for Information Technology Security Evaluation (vereinfachend als «Common Criteria» bezeichnet und als CC abgekürzt). CCs werden seit der Jahrtausendwende eingesetzt, um die Sicherheit von IT-Produkten bzw. deren Komponenten zu evaluieren und auf dieser Basis für den internationalen Markt zu zertifizieren [3]. Auch hier wird die Sicherheit über verifizierbare Eigenschaften und Merkmale zu definieren versucht, wie Funktionalitätsklassen und Vertrauenswürdigkeit (in Bezug auf Korrektheit der Implementierung

[3] Das beschriebene Vorgehen ist ein grundlegendes Konzept in der Informatik und wird als *Divide-and-Conquer* bezeichnet. Es geht darum, ein Problem in Teilprobleme zu zerlegen (*divide*), die einzeln gelöst (*conquer*) und anschliessend zur Gesamtlösung kombiniert werden. Dieser Ansatz scheitert im Fall der IT-Sicherheit daran, dass diese nicht auf die Eigenschaften Vertraulichkeit, Integrität und Verfügbarkeit reduzierbar ist. Vielmehr umfasst die IT-Sicherheit weitere Aspekte wie Verbindlichkeit, Anonymität, Effizienz, Nutzerfreundlichkeit, usw., die nicht nur eine isolierte Betrachtung oder Zerlegung unmöglich machen, sondern zum Teil auch in einem Zielkonflikt zueinander stehen, wie z. B. Authentizität und Verbindlichkeit auf der einen Seite sowie Anonymität auf der anderen Seite (beispielsweise im Falle von E-Voting).

und Prüftiefe). Allerdings haben sich die CC im Bereich der Evaluation und Zertifizierung bis heute nicht durchgesetzt und die Zahl der zertifizierten IT-Produkte ist immer noch vergleichsweise klein. Zudem sind zertifizierbare Produkte bzw. Komponenten eher für einzelne Funktionen ausgelegt und in diesem Sinne auch nicht besonders komplex, wie z. B. Smartcards und Smartcard-Lesegeräte oder Sensoren. Sobald ein Produkt eine gewisse Komplexität erreicht, ist eine Evaluation und Zertifizierung kaum mehr möglich und müsste im Prinzip für jeden neuen Release in wenigstens vereinfachter Form wiederholt werden.

Auch im Bereich der Sicherheit von Organisationen und IT-bezogenen Geschäftsprozessen gibt es verifizierende Ansätze: Wenn sich eine Organisation als sicher und gemäss den Best Practices im IT-Sicherheitsbereich agierend präsentieren will, bietet sich die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems (Information Security Management System, ISMS) gemäss ISO/IEC 27001 [4] an. Um eine höhere Visibilität zu erreichen, kann ein solches ISMS zertifiziert werden. Dabei wird die Sicherheit auf die Existenz eines ISMS mit entsprechenden Sicherheitskontrollmassnahmen reduziert, d. h. es wird angenommen, dass eine Organisation sicher agiert, wenn sie sich auf ein ISMS abstützen kann. Die Frage, ob die Sicherheitskontrollmassnahmen im Einzelnen auch geeignet sind, die Sicherheitsanforderungen der Organisation zu erfüllen, bleibt unbeantwortet bzw. im Ermessen des Auditors. Damit ist a priori unklar, inwiefern diese Annahme gerechtfertigt ist und die Sicherheit mit der Existenz eines ISMS gemäss ISO/IEC 27001 korreliert. Aufgrund dieser Unschärfen gestalten sich Versuche, Sicherheitsmetriken aus der ISMS-Implementierung abzuleiten, oft als schwierig oder unzureichend.

Neben den eben beschriebenen verifizierenden Ansätzen gibt es auch *falsifizierende Ansätze*. Bei einem falsifizierenden Ansatz wird nicht versucht, die IT-Sicherheit über verifizierbare Eigenschaften und Merkmale zu definieren. Stattdessen wird versucht aufzuzeigen, dass ein zur Diskussion stehendes und zu prüfendes IT-System auf eine bestimmte Art und Weise kompromittiert werden kann. Damit wird eigentlich Unsicherheit nachgewiesen und Sicherheit widerlegt. Ein falsifizierender Ansatz ist also grundsätzlich auf eine Prüfung ausgelegt, wobei diese darin besteht, dass das IT-System nicht kompromittiert werden kann. Allenfalls könnte man aus der Schwierigkeit einer Kompromittierung eine Metrik ableiten, aber auch eine solche wäre bis zu einem gewissen Grad willkürlich.

In der IT-Sicherheit muss im Rahmen eines falsifizierenden Ansatzes das zu prüfende IT-System kompromittiert werden. Dazu müssen passende Angriffsvektoren gefunden und so zusammengesetzt werden, dass eine Kompromittierung resultiert. Das ist eine heuristische und kreative Tätigkeit, die massgeblich vom Expertenwissen und den Fähigkeiten der Prüfenden abhängt. Anstelle einer vordefinierten Liste von Eigenschaften und Merkmalen, die einzeln geprüft werden können, wird eine solche Liste ad-hoc (d. h. während der Prüfung) erstellt. Das hat zwar den Vorteil, dass eine Prüfung nicht vorhersehbar ist; dafür ist aber das Ergebnis von den Prüfenden abhängig und bis zu einem gewissen Grad beliebig. Das ist zwar nicht gut, aber in vielen Bereichen das Bestmögliche. Entsprechend viele Angebote für solche Sicherheits(über)prüfungen sind denn auch auf dem Markt verfügbar. Man denke hier etwa an ethische Hacker, Penetrationstester, Bug Bounty Hunter und Red Teams. Sie alle bieten Prüfungen an, die sich sowohl methodisch als auch in Bezug auf Aufwand und Intensität stark unterscheiden können.

Obige Ausführungen zeigen, dass die Sicherheit ein Begriff ist, der nicht präzis definiert und entsprechend geprüft, sondern streng genommen nur falsifiziert werden kann. Zudem lässt auch eine fehlende Falsifizierung immer noch keine absolute Aussage über die Sicherheit zu. Auch ein als nicht unsicher nachgewiesenes IT-System muss nicht notwendigerweise sicher sein, beispielsweise dann, wenn das (Mess)Ergebnis den mangelnden Fähigkeiten oder Ressourcen der Experten zuzuschreiben ist.

Zusammenfassend lässt sich sagen, dass verifizierende Ansätze gewünschte Ergebnisse in Bezug auf Objektivität und Nachvollziehbarkeit liefern und in diesem Sinne auch das erklärte Ziel von wissenschaftlichen Bestrebungen sind (auch im Bereich der IT-Sicherheit). Allerdings sind solche Ansätze (wie bei den CC-Zertifikaten beschrieben) nur für kleine und einfache Produkte bzw. Komponenten möglich, für die eine umfassende und in der Summe aussagekräftige Menge von verifizierbaren Eigenschaften und Merkmalen festgelegt werden kann. Ab einer gewissen Grösse und Komplexität ist das nicht mehr möglich, sodass man auf falsifizierende Sicherheitsprüfungen angewiesen ist bzw. ausweichen muss.[4] Auf die Zertifizierung wird im Folgenden noch genauer eingegangen.

c. Zertifizierung

Vorwiegend im Bereich der verifizierenden Ansätze gibt es heute verschiedene Zertifizierungen, die alle eine Messung oder Prüfung der IT-Sicherheit voraussetzen und als Nachweis der Qualitätssicherung von Standards dienen. Sie werden sowohl für Produktestandards (CC-Zertifikate) als auch für Standards im Bereich der Dienstleistungen und Organisationen (ISO/IEC 27001-Zertifikate) angeboten.

Dazu ist festzuhalten, dass sich bis heute keine Zertifizierung breit durchgesetzt hat. Dort wo Zertifikate eingesetzt werden, gibt es meistens auch entsprechende regulatorische Vorgaben, die alle zum Ziel haben, das vertrauenswürdige Verhalten einer Organisation zu beeinflussen und damit entweder die Kunden zu unterstützen oder die Verfügbarkeit von gewissen für das Funktionieren eines Landes relevanten Gütern oder Dienstleistungen sicherzustellen. Neben der Schwierigkeit, vereinfachende Definitionen mit für die IT-Sicherheit charakteristischen Eigenschaften und Merkmalen zu finden, bestehen die hauptsächlichen Probleme dieser Ansätze darin, dass Zertifizierungen aufwändig und teuer sind und dass der Markt für Zertifikate selbst Anzeichen eines «Lemon Markets»[5] aufweist [5]. Entsprechend besteht die Möglichkeit, dass die Güte von Zertifikaten unter einem konstanten Preisdruck erodiert. Die einzigen Instrumente, die man hat, um eine solche Erosion zu beeinflussen und bestenfalls zu verhindern, sind auf der einen Seite die staatliche Akkreditierung der zugelassenen Zertifizierungsstellen und auf der anderen Seite die Regelung der Haftung dieser Zertifizierungsstellen. Solange ein Zertifikat ohne gleichzeitige Übernahme von Haftungsansprüchen ausgestellt werden kann, erscheint die Aufrechterhaltung einer hohen Güte und Aussagekraft der Zertifikate schwierig. Zudem ist der Zertifikatmarkt international organisiert, so dass die Steuerungsmöglichkeiten einzelner Staaten grundsätzlich begrenzt sind.

Zusammenfassend ist festzuhalten, dass der Nutzen von Zertifikaten beschränkt ist. Im Fall von IT-Produkten sind Zertifikate häufig auf wenige Funktionalitäten limitiert und müssten prinzipiell für jeden Release wieder neu geprüft und ausgestellt werden, womit Aufwand und Ertrag in einem unvernünftigen Verhältnis zueinanderstehen. Künftige Erfahrungen mit dem Cyber Resilience Act (CRA) in der EU werden zeigen, ob sich dieser Eindruck erneut bestätigen

[4] Gemäss dem österreichisch-britischen Philosophen Karl R. Popper (1902 – 1994) gilt dies generell für wissenschaftliche Theorien (als ein Beispiel für ein komplexes System). Diese lassen sich nie endgültig beweisen (verifizieren), wohl aber widerlegen (falsifizieren). Popper betonte, dass eine Theorie überhaupt nur dann als wissenschaftlich gilt, wenn sie falsifizierbar ist, das heisst, wenn sie so formuliert ist, dass prinzipiell ein Gegenbeispiel gefunden werden kann, das sie widerlegt.

[5] Unter einer «Lemon» wird in einem Aufsatz des Wirtschaftsnobelpreisträgers (2001) George A. Akerlof ein «Montagsauto» bzw. ein schlechter Gebrauchtwagen verstanden. Der Markt für Gebrauchtwagen zeichnet sich durch eine Wissensasymmetrie aus. Während der Verkäufer den wahren Zustand des Wagens kennt, ist dieser für den Käufer schwer einzuschätzen. Akerlof hat gezeigt, dass in solchen Märkten die Preise erodieren, d. h. sowohl für «Lemons» als auch für qualitativ gute Gebrauchtwagen niedrige Verkaufserlöse erzielt werden.

wird.[6] Zertifikate komplexerer Prüfgegenstände, deren Sicherheit nicht präzis definiert und entsprechend auch nicht aussagekräftig gemessen oder geprüft werden kann (z. B. im Rahmen von ISO/IEC 27001-Zertifikaten) bescheinigen (bestenfalls), dass zum Zeitpunkt der Prüfung gewisse Abläufe, Prozeduren, Massnahmen und Dokumentationen eingehalten werden, respektive vorhanden sind.[7] Ob und inwieweit diese zur Unternehmung passen, respektive zu deren Sicherheit beitragen, ist a priori nicht klar.

3. Alternative Ansätze

Wie ausgeführt, sind die Definition der IT-Sicherheit, deren Messung, ihre Prüfung und die darauf aufsetzenden Zertifizierungen schwierig. Die jeweiligen Ansätze haben sich oft nur in Nischen durchgesetzt und Zertifikate kommen dann breit(er) zur Anwendung, wenn Regulierungen dies vorsehen. Untersuchungen über deren Nutzen liegen nach unserem Kenntnisstand bis heute keine vor. Dennoch ist feststellbar, dass Staaten (tendenziell) auf zunehmend komplexe Regulierungen setzen. Der bereits erwähnte Cyber Resilience Act (CRA) der EU im Bereich der Produktesicherheit [6] und die Richtline für ein hohes Cybersicherheitsniveau in der Union (NIS-2-Richtline) [7] sind zwei Beispiele, welche alle Staaten der Europäischen Union betreffen.

Nachfolgend werden alternative Ansätze beleuchtet, welche (i) die Mess- und Prüfbarkeit der IT-Sicherheit erhöhen und (ii) Aspekte der IT-Sicherheit entlang den Lieferketten (Lieferanten, Zulieferer und Provider) einbeziehen. Die Ansätze sind in Form von vier Thesen formuliert.

a. These 1: Komplexität reduzieren

Ein weit verbreiteter Standard zur Verbesserung der Cybersicherheit in Unternehmen und Organisationen ist das vom U.S. National Institute of Standards and Technology (NIST) publizierte Cybersecurity Framework (CSF) [8]. Auf dem NIST CSF basiert unter anderem der IKT-Minimalstandard, welcher vom Bund erarbeitet [9] und beispielsweise für die Strombranche per 1. Juli 2024 für verbindlich erklärt wurde [10]. Das dem Minimalstandard zugrunde liegende CSF 1.1 aus dem Jahr 2018 basierte auf fünf Kernfunktionen (Identify, Protect, Detect, Respond und Recover) mit 23 Kategorien und total 108 Unterkategorien oder Massnahmen (sogenannten «Controls»). Mit der Veröffentlichung des NIST CSF 2.0 im Februar 2024 kam eine sechste Kernfunktion «Govern» dazu. Die Kernfunktionen sind seither in 22 Kategorien und total 106 Unterkategorien (Massnahmen) gegliedert. Ebenfalls weit verbreitet ist der ISO/IEC 27001 Standard [4]. In seiner aktuellen Version 2022 enthält er 93 Controls, aufgeteilt in vier Hauptkategorien (Organisational Controls, People Controls, Physical Controls, Technological Controls). Gegenüber ISO 27001:2013 in der noch 114 Controls verteilt auf 14 Kategorien aufgeführt waren, stellt diese Reduktion eine Vereinfachung dar, welche grundsätzlich zu begrüssen ist. Dennoch ist festzustellen, dass die Anzahl Massnahmen bei beiden gängigen Standards hoch ist.

Zwar sehen sowohl NIST CSF als auch ISO 27001 eine flexible und risikobasierte Umsetzung der Massnahmen vor. Wird jedoch auf die Umsetzung bestimmter Controls verzichtet, so

[6] Im Rahmen des CRA wird die Konformität eines Produkts mit den Cybersicherheitsanforderungen durch die Vergabe des CE-Zeichens (Conformité Européenne) im Sinne eines «Zertifikats» bestätigt. Für Produkte mit geringem Risiko genügt hierfür eine Selbstdeklaration des Herstellers. Bei Produkten mit hohem Risikopotenzial – etwa solchen, die in kritischen Infrastrukturen eingesetzt werden – ist hingegen eine Prüfung durch eine zugelassene unabhängige und notifizierte Stelle verpflichtend, um die CE-Kennzeichnung zu erhalten.

[7] Im weiteren Text (These 4) gehen wir detaillierter darauf ein, dass mangels Alternativen, zur Zertifizierung oft Kriterien wie der Reifegrad (Maturität) herangezogen werden, die weniger mit der IT-Sicherheit selbst als vielmehr mit der methodischen Korrektheit der Implementierung zu tun haben.

muss dies begründet werden. Häufig wird mit einem geringen Restrisiko argumentiert. Auf die Problematik von Risikobetrachtungen wird nachfolgend detaillierter eingegangen. An dieser Stelle ist bereits festzuhalten, dass wahrscheinlichkeitsbasierte (d. h. quantitative) Risikobetrachtungen grundsätzlich schwierig und nicht optimal für die Beurteilung sind, ob bestimmte Massnahmen umgesetzt werden sollen [11]. Der risikobasierte Verzicht auf Massnahmen ist ebenfalls wenig geeignet, wenn es um die Herstellung von Transparenz geht, da vergleichbare Unternehmen – trotz Einhaltung desselben Standards – zu unterschiedlichen Risikoeinschätzungen und damit zu abweichenden Massnahmenkatalogen gelangen können.

Um diese Nachteile zu überwinden, kann eine grundlegende Reduktion der Komplexität vorgeschlagen werden. Anstelle zahlreicher Einzelmassnahmen, die jeweils auf Basis einer wahrscheinlichkeitsbasierten Risikoanalyse bewertet und umgesetzt oder verworfen werden, setzt das BACS auf einen erweiterten Grundschutzansatz. Dieser Ansatz definiert eine möglichst kleine Menge verbindlicher Basisanforderungen, die zwingend umzusetzen sind. Erst bei erhöhtem IT-Schutzbedarf sollen gezielt zusätzliche technische und organisatorische Massnahmen (TOMs) implementiert werden. Im Gegensatz zu den in [12,13] postulierten Ansätzen wird auf eine wahrscheinlichkeitsbasierte Risikoanalyse verzichtet.[8]

Weniger, dafür generelle Massnahmen, welche (unabhängig von Risikobetrachtungen) umzusetzen sind, verringern die Komplexität und erhöhen die Transparenz, da zu jeder Zeit klar ist, was mindestens umgesetzt werden muss. Dieses Vorgehen stützt sich unter anderem auf die Erkenntnisse des Government CERTs (GovCERT.ch) aus zahlreichen analysierten IT-Sicherheitsvorfällen, die oft durch einfache Massnahmen wie die Einführung einer Zwei-Faktor-Authentifizierung hätten verhindert werden können. Zusätzliche TOMs können auf der Basis einer Bedrohungsmodellierung (siehe unten) ausgewählt und umgesetzt werden. Damit lässt sich der Sinn und Zweck jeder Massnahme erklären und transparent nachvollziehen.

b. These 2: Massnahmen auf Fakten basieren

Menschen sind darin geübt, Fakten zu analysieren und daraus Schlussfolgerungen zu ziehen. Deutlich schwieriger ist hingegen das Entwickeln und Bewerten fiktiver Szenarien und Ereignisse. Insbesondere die Einschätzung der Eintrittswahrscheinlichkeit und des Schadensausmasses eines bestimmten Ereignisses gestaltet sich in solchen Fällen als äusserst schwierig – wenn nicht gar unmöglich. Dies liegt nicht nur daran, dass Menschen unbewusst dazu neigen, ideologische Vorurteile und persönliche Erfahrungen in die Bewertung von fiktiven Szenarien einfliessen zu lassen, sondern auch daran, dass statistische Analysen eine ausreichend grosse Anzahl vergleichbarer Ereignisse erfordern, welche oft fehlen.[9] Die Resultate von wahrscheinlichkeitsbasierten Risikoanalysen sind damit häufig willkürlich, haben wenig Aussagekraft [2,11,14] und sind folglich nur bedingt geeignet, sinnvolle IT-Sicherheitsmassnahmen abzuleiten. Da IT-Sicherheitsspezialisten oft intuitiv wissen, welche Massnahmen sinnvoll sind, behelfen sich diese gemäss Erfahrungen des BACS oft damit, Risiken «rückwärts» zu berechnen und passend (in allfällige Hilfsmittel) einzusetzen, sodass diejenigen Massnahmen resultieren, die sie (basierend auf ihrem Erfahrungsschatz) umsetzen möchten. Diese Rekonstruktion der Risiken aus den Massnahmen führt die Idee der Risikoanalyse jedoch ad absurdum.

[8] Wie weiter unten erläutert, wird der erhöhte Schutzbedarf nicht durch eine wahrscheinlichkeitsbasierte Risikoanalyse, sondern durch die Bewertung der Auswirkungen von definierten IT-Sicherheitsbedrohungen auf Geschäfts- und Produktionsprozesse bestimmt (vgl. Abschnitt 4.a Informationssicherheits-Managementsysteme (ISMS)).

[9] Bei Zero-Day-Exploits und anderen bisher unbekannten Angriffsvektoren ist das zum Beispiel nicht anders möglich.

Das BACS empfiehlt daher, Massnahmen nicht basierend auf fiktiven Ereignissen und Szenarien auszuwählen. Sie sollten entweder universell gelten – wie im erwähnten Grundschutzansatz – oder bei erhöhtem Schutzbedarf faktenbasiert hergeleitet werden. Die erforderlichen Grundlagen zur Bestimmung des Schutzbedarfs, wie Geschäftsprozesse, Prozessziele mit maximal zulässigen Abweichungen sowie beteiligte Hard- und Softwarekomponenten lassen sich objektiv bestimmen, können von Dritten verifiziert werden und erfordern keine willkürlichen Annahmen. Wird erhöhter Schutzbedarf festgestellt, eignet sich zur strukturierten Ableitung von Massnahmen die Bedrohungsmodellierung nach STRIDE [15], respektive STRIDE-LM[10]. Die sechs Bedrohungskategorien dieser Methode sind universell (Fussnote 10). Dasselbe gilt für die typischen dazugehörenden Gegenmassnahmen.[11,12] Mit grossen Unsicherheiten behaftete Szenarien sind nicht notwendig.

Wenn Massnahmen der IT-Sicherheitskonzeption auf Fakten, die auch von Dritten nachvollzogen werden können (siehe auch These 4) statt auf zufälligen oder fiktiven Szenarien beruhen, profitieren nicht nur die IT-Sicherheit, sondern auch die Transparenz bezüglich der Notwendigkeit bestimmter Massnahmen, was zugleich die Prüfbarkeit erhöht oder überhaupt erst ermöglicht.

c. These 3: Verifizierende und falsifizierende Ansätze kombinieren

Weiter oben sind zwei Ansätze beschrieben, um die IT-Sicherheit einer Organisation oder einer Unternehmung festzustellen. Der eine Ansatz wurde verifizierend, der andere falsifizierend genannt. Im ersten Fall wird die «Anwesenheit von Sicherheit» bestätigt, indem verifiziert wird, ob ein definiertes Verfahren (z. B. ein Schwachstellenmanagement) korrekt implementiert wurde. Im zweiten Fall wird die «Abwesenheit von Unsicherheit» bestätigt, beispielsweise weil es ethischen Hackern nicht gelingt, die IT-Sicherheit zu kompromittieren. Beide Ansätze haben Vor- aber auch Nachteile, wobei sich letztere im Idealfall durch eine Kombination beider Ansätze kompensieren lassen.

Wenn die IT-Sicherheit einer Unternehmung oder Organisation mit beiden Ansätzen angeschaut wird, verändert sich der Blickwinkel. Der verifizierende Ansatz fokussiert auf die einzelnen (technischen und organisatorischen) Massnahmen und deren Implementierung. Beim falsifizierenden Ansatz (ethisches Hacking, Penetrationstests, usw.) wird ein Angriff auf die IT-Sicherheit durchgeführt, respektive simuliert. Dieser kann dann erfolgreich abgewehrt werden, wenn das Kollektiv der Massnahmen dem Angriff Stand hält bzw. diesen abwehren kann.

---

[10] 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 (Form der Abkürzung), das sich aus den Anfangsbuchstaben der ursprünglich sechs 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 Gefährdungen in Netzwerken um die Kategorie LM «Lateral Movement» (laterale Bewegung, d. h. die Fähigkeit in einem Netzwerk weitere Systeme zu kompromittieren) ergänzt worden.

[11] Beispiele sind die Authentifizierung als Massnahme gegen die Spoofing-Bedrohung oder die Verschlüsselung als Massnahme gegen die Bedrohung durch einen Datenabfluss (Information Disclosure). Diese Massnahmen sind allgemeingültig und können flexibel und kohärent auf unterschiedliche Systeme zugeschnitten werden.

[12] STRIDE bietet im Vergleich zur direkten Ableitung von Massnahmen ohne Bedrohungsmodell, wie etwa aus der CIA-Triade, die lediglich IT-Schutzziele wie Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) definiert, einen klaren, systematischen und nachvollziehbaren Rahmen zur Identifikation von Bedrohungen und zur Ableitung passender Massnahmen. Dadurch wird ermöglicht, Sicherheitsmassnahmen gezielt auf konkret analysierte Bedrohungen abzustimmen – ein entscheidender Vorteil gegenüber weniger strukturierten Ansätzen wie der CIA-Triade.

Im Fokus steht damit insbesondere auch die Prüfung des Zusammenspiels, respektive der Wechselwirkungen zwischen den TOMs zur Verhinderung von Angriffen.[13]

Durch die Kombination beider Prüfansätze (verifizierend und falsifizierend) lässt sich die IT-Sicherheit einer Organisation umfassender bewerten, als es die isolierte Anwendung nur eines Ansatzes ermöglicht. Dies liegt daran, dass sich die Stärken des einen Ansatzes dort zeigen, wo der jeweils andere Erkenntnislücken («blinde Flecken») aufweist.

Der hier vorgestellte Vorschlag sieht nicht vor, jeden Prozess oder jede Hard- und Softwarekomponente mit beiden Ansätzen zu testen. Vielmehr geht es darum, die vorhandenen Ressourcen gezielt und strategisch einzusetzen, um die Cybersicherheit der Unternehmung oder Organisation bestmöglich zu stärken. Je nach Anwendungsfall kann mal der eine, mal der andere Ansatz geeigneter sein. Insbesondere beim Schutz zentraler Geschäfts- und Produktionsprozesse mag es jedoch sinnvoll sein, beide Ansätze parallel einzusetzen, um einen umfassenderen Schutz zu erreichen.

d. These 4: IT-Sicherheit schaffen durch Vertrauen und Transparenz

In dieser These wird erneut die Frage nach dem Nutzen von Zertifikaten und deren Bedeutung für die IT-Sicherheit beleuchtet. Für Unternehmungen und Organisationen gibt es (im Wesentlichen) drei Gründe, die Umsetzung eines Sicherheitsstandards zertifizieren zu lassen: Erstens, weil dies von Gesetzes wegen verlangt wird. Zweitens, weil sich das Unternehmen einen Marktvorteil verspricht (d. h. seine Kunden eine Zertifizierung nachfragen). Der dritte Grund, nämlich die (externe) Überprüfung und allfällige Optimierung der eigenen IT-Sicherheit und Resilienz spielt mutmasslich oft nur eine untergeordnete Rolle. Das ist überraschend, sollte doch gerade der dritte Punkt aus der Sicht der Unternehmung oder Organisation die eigentliche Kernmotivation für seine Zertifizierung sein. Die beiden ersten Punkte lassen den Schluss zu, dass sowohl Behörden als auch Kunden erwarten, dass zertifizierte Unternehmungen und Organisationen gegenüber IT-Sicherheitsausfällen und -störungen umfassender und besser geschützt sind als solche ohne Zertifikate. Diese Erwartung ist aber oft unrealistisch.

Die IT-Sicherheit – insbesondere bei hoher Komplexität des zu prüfenden Systems – lässt sich weder exakt definieren noch objektiv messen. Dennoch sollen genau diese unmöglichen «Messungen» die Grundlage für Zertifizierungen bilden. Mangels praktikabler Alternativen wird oft der Reifegrad (Maturität) eines Systems – etwa eines Sicherheitsverfahrens – zur Zertifizierung herangezogen. Diese Metrik zeigt jedoch primär, wie methodisch vollständig eine Lösung implementiert wurde, nicht aber ihre tatsächliche Sicherheitseffektivität.[14] Reifegradmodelle erlauben nur eingeschränkte Rückschlüsse auf die reale IT-Sicherheit.

Problematisch ist zudem die mangelnde Transparenz des Zertifizierungsprozesses, der ausschliesslich zwischen der zu prüfenden Unternehmung oder Organisation und der Zertifizierungsstelle abläuft. Behörden und Kunden haben dadurch keine Möglichkeit, nachzuvollziehen, ob und wie ihre wichtigen Anliegen berücksichtigt werden – sie kennen weder die

---

[13] Dem griechischen Universalgelehrten Aristoteles folgend könnte man formulieren: Das Ganze (geprüft beispielsweise beim ethischen Hacking) ist etwas *anderes* als die Summe seiner Teile (geprüft durch Verifikation der einzelnen Massnahmen). Entsprechend unterscheidet und ergänzt sich der Erkenntnisgewinn.

[14] Zertifizierungen bestätigen häufig einen bestimmten Reifegrad (Maturität). Dieser bezieht sich stets auf ein konkretes System – wie ein bestimmtes Informationssicherheits-Managementsystem (ISMS) oder ein Business Continuity Management System (BCMS) – und spiegelt wider, wie *methodisch vollständig* die Organisation dieses umgesetzt hat. Ein hoher Reifegrad steht damit – ganz besonders bei komplexen Systemen – nicht automatisch für ein hohes IT-Sicherheitsniveau. Dies gilt insbesondere, wenn das betreffende System für die spezifischen Anforderungen der Organisation ungeeignet ist oder auf fehlerhaften Annahmen – wie etwa unzutreffenden Risikobewertungen – basiert. Die Aussagekraft des Reifegrads hängt somit massgeblich davon ab, wie passgenau das System gewählt und wie qualitativ hochwertig es implementiert wurde.

zugrunde liegenden Risikoüberlegungen noch können sie Einfluss auf die Umsetzung der IT-Sicherheitsmassnahmen nehmen.

Behörden und Kunden sollten verinnerlichen, dass Zertifikate lediglich begrenzte Aussagekraft zur IT-Sicherheit besitzen und eine Zertifizierung kein Garant dafür ist, dass eine Unternehmung oder Organisation den erwartet hohen IT-Sicherheitsstandard gewährleistet. Es stellt sich damit die grundsätzliche Frage, was von Unternehmungen oder Organisationen betreffend ihrer IT-Sicherheit erwartet werden kann und wie sich diese Erwartungen prüfen lassen.

Eine realistische Erwartung ist, dass sich eine Unternehmung oder Organisation seiner Verantwortung für das Funktionieren eines Landes (gilt insbesondere für die Betreiber kritischer Infrastrukturen, siehe unten) und für die wirtschaftliche Prosperität seiner Kunden bewusst ist und «verspricht», seine IT-Sicherheit gemäss dem Stand der Technik umzusetzen, wozu auch die Umsetzung geeigneter Standards zählen kann. Behörden und Kunden sollten statt Zertifikate nachweisbare Transparenz fordern, um die Einhaltung dieser Zusage überhaupt sinnvoll prüfen zu können. Das Konzept «Sicherheit durch Vertrauen und Transparenz» stellt – trotz offensichtlicher Herausforderungen bei der Skalierung[15] – eine vielversprechende und prüfenswerte Alternative zu herkömmlichen Zertifizierungen dar.

Wie angedeutet, stellt die Skalierbarkeit die grösste Herausforderung bei der Umsetzung des Konzepts «Sicherheit durch Vertrauen und Transparenz» dar. Ein möglicher Lösungsansatz könnte die Idee hinter RFC 9116 [16] bieten: Im April 2022 veröffentlichte die Internet Engineering Task Force (IETF) dieses Dokument, das sich mittlerweile bei vielen Website-Betreibern etabliert hat. RFC 9116 definiert Format und Nutzung der Datei «security.txt», mit welcher Organisationen ihre Prozesse zur Offenlegung von Sicherheitslücken (Vulnerability Disclosure) bekannt machen können. Diese Datei wird auf dem Webserver abgelegt und bietet eine effektive Möglichkeit, Sicherheitsforscher und Administratoren miteinander in Kontakt zu bringen. Dadurch wird das Melden von Schwachstellen erleichtert, was zur Verbesserung der Sicherheit einer Website beitragen kann.

In Anlehnung an das Konzept von «security.txt» wird vorgeschlagen, eine Datei mit dem Namen «cybersecurity-transparency.txt» einzuführen. Diese soll dazu dienen, die von einer Organisation oder einem Unternehmen implementierten IT-Sicherheitsmassnahmen und -mechanismen transparent zu dokumentieren und gegenüber Dritten, wie etwa Behörden oder Kunden, offenzulegen. Die Dokumentation erfolgt pro Geschäfts- bzw. Produktionsprozess und Produkt und umfasst unter anderem folgende Angaben: Prozessziele, IT-Schutzziele, umgesetzte IT-Sicherheitsbasisanforderungen, Verantwortlichkeiten, Kontaktinformationen sowie das Datum der letzten Aktualisierung.

Da die Offenlegung detaillierter technischer Massnahmen, Konfigurationen oder bekannter Schwachstellen potenziellen Angreifern gezielte Informationen liefern könnten, sollte die Transparenz auf einer übergeordneten Ebene erfolgen. Es empfiehlt sich daher, die Angaben auf Prinzipien, Prozesse und Verantwortlichkeiten zu beschränken und auf operative Details zu verzichten, die Rückschlüsse auf konkrete Angriffsvektoren ermöglichen könnten. Hinweise auf diese Offenlegungsgrenzen sind in «cybersecurity-transparency.txt» ebenfalls zu vermerken.

Ob und in welchem Umfang eine Unternehmung oder Organisation die Datei «cybersecurity-transparency.txt» erstellt und veröffentlicht, sollte ihr selbst überlassen bleiben. Denkbar ist

[15] Dass Zertifikate trotz ihrer Mängel überhaupt benutzt werden, erklärt sich u. a. mit deren Skalierbarkeit und Praktikabilität. Unternehmen müssen jedoch erkennen, dass sie Mitverantwortung für Schäden tragen, welche sie durch mangelnde IT-Sicherheit ihrer Zulieferer erfahren. Eine reduktionistische Haltung, die sich auf das Einfordern von Zertifikaten beschränkt, ist riskant bis fahrlässig.

beispielsweise eine gezielte und exklusive Bereitstellung der Datei für potenzielle Kunden im Rahmen der Offertenerstellung oder eine allgemeine Veröffentlichung auf der eigenen Website. In beiden Fällen schafft die Unternehmung oder Organisation damit eine vertrauensvolle Basis für die Zusammenarbeit und zeigt einen offenen und verantwortungsvollen Umgang mit dem Thema IT-Sicherheit gegenüber von Kunden und Partnern. Das Vorweisen der Datei «cybersecurity-transparency.txt» könnte künftig als zeitgemässe Alternative zu herkömmlichen Zertifikaten dienen, bei der – im Gegensatz zu Zertifikaten – jeder Geschäftspartner die Möglichkeit hat, die IT-Sicherheit des Lieferanten hinsichtlich seiner Prioritäten selbst zu überprüfen, respektive das Dokument als Ausgangspunkt für weiterführende Gespräche zu nutzen (siehe dazu auch Abschnitt «Cybersicherheit entlang der Lieferkette» weiter unten).

4. Anwendungen der Thesen

Im Folgenden wird anhand ausgewählter Beispiele gezeigt, wie sich die Thesen in die Praxis umsetzen lassen. Die Beispiele stammen aus aktuellen Projekten, die im Bereich der präventiven Cybersicherheit beim BACS geplant, entwickelt und teilweise bereits realisiert worden sind.

a. Informationssicherheits-Managementsysteme (ISMS)

Ein besonders relevantes Gebiet für die Prüf- und Messbarkeit der IT-Sicherheit sind die Informationssicherheits-Managementsysteme (ISMS). Ein ISMS lässt sich wie folgt definieren:

Ein ISMS ist ein aus Verfahren und Regeln bestehendes System, 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.

Das BACS entwickelt zurzeit eine Methode, welche die Grundlage für den Aufbau eines ISMS nach obiger Definition bilden soll. Die Methode berücksichtigt die Reduktion der Komplexität (These 1) ebenso wie das Abstützen der Massnahmen auf Fakten (These 2). Dazu setzt sie einerseits auf universell geltende Basisanforderungen bestehend aus rund 20 Massnahmen, welche in jedem Fall umzusetzen sind. Zusätzliche (technische und organisatorische) Massnahmen werden bei erhöhtem Schutzbedarf gezielt erarbeitet. Dazu werden Parameter wie Geschäftsprozesse, Prozessziele, deren jeweils maximal zulässige Abweichungen sowie die an den Geschäftsprozessen beteiligten Hard- und Softwarekomponenten herangezogen. Diese Faktoren sind objektiv feststellbar und können bei Bedarf von Dritten überprüft werden. Die Massnahmen ergeben sich aus einer Bedrohungsanalyse nach STRIDE, respektive STRIDE-LM. Dabei sind die sechs Bedrohungskategorien ebenso universell gültig, wie die jeweils dazugehörenden Gegenmassnahmen (siehe Fussnote 11). Auf mit grossen Unsicherheiten behaftete Risikoszenarien sowie die Einschätzung ihrer Eintretenswahrscheinlichkeit wird verzichtet.

b. Cybersicherheit in der Lieferkette

Ein konkretes Beispiel dafür, wie IT-Sicherheit durch Vertrauen und Transparenz gestärkt werden kann (These 4), ist der Ansatz des BACS zum Umgang mit IT-Sicherheit in der Lieferkette. Im Jahr 2024 wurde hierzu ein Pilotprojekt in Zusammenarbeit mit der Wirtschaft gestartet. Ziel ist es, Unternehmen und Organisationen dafür zu sensibilisieren, bei der Auswahl von Lieferanten nicht nur auf die Qualität von Produkten und Dienstleistungen zu achten, sondern von Anfang an auch Aspekte der IT-Sicherheit einzubeziehen und gemeinsam mit den Lieferanten abzustimmen.

Das BACS empfiehlt, IT-Sicherheitsanforderungen systematisch in den Auswahl- und Prüfprozess von Lieferanten zu integrieren. Hierzu wurde ein Regelkreis mit sieben Schritten

entwickelt, der von der Identifikation und Bewertung der Lieferkette über die Lieferantenprüfung bis hin zur vertraglichen Festlegung von Massnahmen reicht. Konkrete Leitfragen an Lieferanten, empfohlene Massnahmen und Hinweise zur vertraglichen Absicherung sind in den entsprechenden Hilfsmitteln des BACS aufgeführt [17].

Im Unterschied zum blossen Einfordern von Zertifikaten, das wenig Einblick in die tatsächliche IT-Sicherheitslage von Lieferanten bietet, ermöglicht dieser Ansatz eine gezielte Abstimmung der Anforderungen und Erwartungen auf die individuellen Bedürfnisse der Partner. Zwar ist dieses Vorgehen aufwändiger als das Einholen eines Zertifikats, doch stellt es eine unverzichtbare Aufgabe für jedes verantwortungsbewusste Unternehmen dar, die nicht delegiert werden sollte (Fussnote 15).

Das Bereitstellen einer «cybersecurity-transparency.txt»-Datei könnte hier einen niederschwelligen und effizienten Einstieg in den Dialog mit Lieferanten bieten. Idealerweise führt dieser Austausch zu einem gestärkten Vertrauensverhältnis und einer Kooperation, die die Cybersicherheit entlang der gesamten Lieferkette nachhaltig verbessern kann.

c. Cybersicherheit und Schutz kritischer Infrastrukturen

Auch aus staatlicher Sicht ist die Gewährleistung der IT-Sicherheit in bestimmten Unternehmen von zentraler Bedeutung – insbesondere bei den Betreibern kritischer Infrastrukturen. Da deren Funktionsfähigkeit massgeblich von der IT-Sicherheit abhängt, hat der Staat sogar den verfassungsmässigen Auftrag, zu deren Schutz beizutragen. In diesem Zusammenhang nehmen Staaten häufig eine regulierende Rolle ein und verpflichten die betroffenen Marktteilnehmer zur Einhaltung bestimmter Standards. Dies ist vor allem dort sinnvoll, wo unterschiedliche Interessenlagen (von Staat und Unternehmen) bestehen.[16]

Allerdings bleibt dabei unberücksichtigt, dass viele Unternehmen ein eigenes, erhebliches Interesse am Schutz vor IT-Sicherheitsvorfällen haben – nicht zuletzt, weil solche Vorfälle auch ihre eigenen Geschäftsinteressen gefährden. In manchen Fällen mangelt es den Unternehmen weniger am Willen als am notwendigen Fachwissen, um angemessene Schutzmassnahmen umzusetzen. In solchen Situationen kann die Vermittlung von Wissen und praxisnahen Hilfestellungen – im Sinne einer «Hilfe zur Selbsthilfe» und in Berücksichtigung der Thesen 1,2 und 4 – eine sinnvolle und wirkungsvolle Alternative oder Ergänzung zur reinen Regulierung darstellen.

Im Rahmen der Umsetzung der Nationalen Cyberstrategie (NCS) bietet das BACS vielfältige Hilfestellungen an. Die Technologiebetrachtungen des BACS greifen aktuelle und relevante Themen auf, darunter Cloud Computing [18], Quantencomputer und Post-Quanten-Kryptographie [19], sowie Herausforderungen der heutigen Internetarchitektur im Zusammenhang mit netzwerkbasierten Angriffen und möglichen Lösungsansätzen wie SCION [20].

Die Publikationen des BACS werden aus einer neutralen Perspektive verfasst, häufig in Abstimmung mit Expertinnen und Experten aus Wirtschaft und Wissenschaft. Sie unterstützen Unternehmen dabei, fundierte und faktenbasierte Entscheidungen im Bereich der IT-Sicherheit zu treffen.

Eine weitere Möglichkeit, Transparenz zu fördern (These 4), besteht darin, den Cyber Security Hub (CSH) des BACS als zentrale Plattform für den Informationsaustausch zwischen Behörden und Betreibern kritischer Infrastrukturen zu nutzen. Der CSH ermöglicht bereits heute

[16] Unterschiedliche Interessenlagen entstehen beispielsweise dann, wenn Unternehmen im Interesse des Staates – etwa zum Schutz von Wirtschaft und Bevölkerung – verpflichtet werden sollen, sich auf bestimmte Ereignisse vorzubereiten, der dafür erforderliche Aufwand jedoch den potenziellen Nutzen einer fortgesetzten Dienstleistung oder Güterproduktion im Ereignisfall deutlich übersteigt. Ein Beispiel hierfür ist die Aufrechterhaltung von Telekommunikationsdienstleistungen im Falle eines langanhaltenden Stromausfalls.

einen strukturierten Austausch zu Cyberbedrohungen, Vorfällen und Best Practices und unterstützt so die operative Cybersicherheit. Künftig soll der CSH verstärkt für präventive Zwecke eingesetzt werden, etwa indem er Werkzeuge bereitstellt, mit denen Betreiber kritischer Infrastrukturen den Stand ihrer IT-Sicherheit selbst bewerten, respektive (anonymisiert) mit weiteren Unternehmen ihrer Branche vergleichen können (sogenanntes «Benchmarking»). Solche Selbstbewertungen liefern Unternehmen wertvolle Hinweise zur Weiterentwicklung ihrer Cybersicherheit und ermöglichen es gleichzeitig dem Staat, aggregierte Erkenntnisse zum Sicherheitsniveau im Sektor zu gewinnen, um bei Bedarf gemeinsam mit der Branche gezielte Verbesserungsmassnahmen zu erarbeiten.

Dieses Vorgehen setzt Transparenz und gegenseitiges Vertrauen voraus: Nur wenn der Austausch freiwillig und vertraulich erfolgt, entsteht ein offener Dialog, der die kontinuierliche Verbesserung der Cybersicherheit fördert.[17]

5. Fazit

Aufgrund des Gesagten scheint die Mess- und Prüfbarkeit der IT-Sicherheit grundsätzlich nicht gegeben und nur in (trivialen) Einzelfällen überhaupt möglich zu sein. Entsprechende Zertifikate sind zum Teil trügerisch und täuschen in der Realität oft Eigenschaften vor, die einer kritischen Betrachtung nicht standzuhalten vermögen. Die IT-Sicherheit ist keine Eigenschaft, die sich oberflächlich beurteilen lässt. Will man die IT-Sicherheit eines Systems beurteilen, muss man in den Kern des Systems vordringen und diesen sehr genau untersuchen. In der Realität bedeutet das, dass man im Beispiel von Organisationen und Unternehmen bei den Geschäfts- und Produktionsprozessen beginnen muss, die auf eine funktionierende IT-Infrastruktur angewiesen sind. Auch bei Produkten und Dienstleistungen geht es immer darum, den eigentlichen «Use Case» zu betrachten. Keine Sicherheitstechnologie hat Selbstzweck; stattdessen hat sie einem Geschäfts- oder Produktionsprozess bzw. einem «Use Case» zu dienen und muss ein sozio-technisches Gesamtsystem absichern.

Will man vor diesem Hintergrund die IT-Sicherheit mess- und/oder prüfbar machen, müssen auch alternative Ansätze (zu Zertifikaten) betrachtet werden. Exemplarisch wurde in vorliegender Arbeit die Reduktion der Komplexität (These 1), das Abstützen von Massnahmen auf Fakten (These 2), die Kombination von verifizierenden und falsifizierenden Ansätzen (These 3) und das Schaffen von Sicherheit durch Vertrauen und Transparenz (These 4) formuliert. Natürlich können auch weitere Thesen gefunden und mit den bereits formulierten Thesen kombiniert werden, um eine sinnvolle und praktikable Form der Mess- und Prüfbarkeit der IT-Sicherheit zu erreichen.

Abkürzungen

BACS	Bundesamt für Cybersicherheit
BCMS	Business Continuity Management System (Kontinuitätsmanagement-System)
CC	Common Criteria
CE	Conformité Européenne
CERT	Computer Emergency Response Team

[17] In diesem Bereich sind zahlreiche weitere Kooperationsmöglichkeiten denkbar, die auf gegenseitigem Vertrauen und Transparenz basieren. Solche Modelle können sich in Bezug auf die Verbesserung der Cybersicherheit als nachhaltiger und effizienter erweisen als Ansätze, die auf strikte Vorgaben, Misstrauen und Kontrollen setzen.

CIA	Confidentiality, Integrity, Availability
CRA	Cyber Resilience Act der Europäischen Union
CSH	Cyber Security Hub (Informationssystem des BACS)
EU	Europäische Union
GovCERT.ch	Government CERT (Teil des BACS)
IETF	Internet Engineering Task Force
ISMS	Informationssicherheits-Managementsystem
ISO / IEC	International Organization for Standardization / International Electrotechnical Commission
NCS	Nationale Cyberstrategie
NIS-2	Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Europäischen Union
NIST	National Institute of Standards and Technology
NIST CSF	NIST Cybersecurity Framework
RFC	Request for Comments
SaaS	Software as a Service
SCION	Scalability, Control and Isolation on Next-Generation Networks (Skalierbarkeit, Kontrolle und Isolation in Netzwerken der nächsten Generation)
STRIDE-LM	Akronym für Spoofing (Identitätsverschleierung), Tampering (Manipulation), Repudiation (Verleugnung), Information Disclosure (Verletzung der Privatsphäre oder Datenabfluss), Denial of Service (Verweigerung des Dienstes), Elevation of Privilege (Rechteausweitung), Lateral Movement (laterale Ausbreitung).
TOM	Technische und organisatorische Massnahme

Referenzen

[1] A. Grünert, J. B. Michael, R. Oppliger and R. Rytz, "On the Measurability and Testability of IT Security" in IEEE Computer, vol. 58, no. 3, pp. 120-126, März 2025

[2] Rolf Oppliger und Andreas Grünert, “How to Measure Cybersecurity and Why Heuristics Matter” in IEEE Computer, vol. 57, no. 2, pp 111-115, Februar 2024

[3] ISO/IEC 15408-1, Information security, cybersecurity and privacy protection – Evaluation criteria for IT security, Part 1: Introduction and general model, 2022

[4] ISO/IEC 27001, Information security, cybersecurity and privacy protection – Information security management systems – Requirements, 2022

[5] George A. Akerlof, The Market for Lemons: Quality Uncertainty and the Market Mechanism, The Quarterly Journal of Economics, Vol. 84, No. 3, August 1970, Seiten 488 – 500

[6] Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 14. November 2024 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau von Produkten mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020" (Cyber Resilience Act)

[7] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

[8] National Institute of Standards and Technology (NIST), 2024. NIST-Cybersicherheits-Framework (CSF) 2.0. Gaithersburg, MD: National Institute of Standards and Technology.

[9] Bundesamt für wirtschaftliche Landesversorgung BWL, IKT-Minimalstandard zur Verbesserung der IKT-Resilienz, Mai 2023

[10] Artikel 5a Stromversorgungsverordnung (StromVV) vom 14. März 2008 (Stand am 1. Januar 2025), SR 734.71

[11] 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

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

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

[14] 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

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

[16] Internet Engineering Task Force (IETF). (2022). *RFC 9116: A file format to aid in security vulnerability disclosure*. Abgerufen von https://www.rfc-editor.org/rfc/rfc9116.pdf

[17] Bundesamt für Cybersicherheit BACS, Cybersicherheit in der Lieferkette, 2024, https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/lieferkette.html

[18] Bundesamt für Cybersicherheit BACS, Technologiebetrachtung – Cloud Computing und Cybersicherheit, 2025

[19] Bundesamt für Cybersicherheit BACS, Technologiebetrachtung – Quantencomputer und Post-Quanten-Kryptografie, 2024

[20] Bundesamt für Cybersicherheit BACS, Technologiebetrachtung – SCION, 2025