Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

November 2025

Technologiebetrachtung

Cybersicherheit und -resilienz

1 Einführung

Bei der Sicherheit geht es um den Schutz vor Ereignissen und Bedrohungen, die sich negativ auswirken und einen Schaden verursachen können. Es ist ein weit gefasster Begriff, der subjektiv unterschiedlich empfunden wird und sich auch deshalb nur schwer in einer objektiven und konkreten Zielfunktion ausdrücken lässt. In vielen Fällen scheint es sinnvoll, anstelle von Sicherheit Resilienz anzustreben. Dank einer starken Resilienz können Ereignisse und Bedrohungen akzeptiert werden, solange sie nicht die eigene Widerstandsfähigkeit übersteigen bzw. das Überleben gefährden. Auch werden dadurch neue Handlungsvarianten eröffnet: Ereignisse und Bedrohungen müssen nicht mehr zwingend nur mit Hilfe von präventiven Sicherheitsvorkehrungen und -massnahmen verhindert werden. Stattdessen können Risiken bewusst in Kauf genommen werden, solange sie nicht kritische Bereiche betreffen. Voraussetzung dafür ist, dass die Risiken erkannt werden und adäquat auf sie reagiert werden kann.

In dieser Technologiebetrachtung wird aufgezeigt, worin sich Sicherheit und Resilienz unterscheiden, weshalb sich Resilienz als übergeordnetes Ziel besser eignet, und warum das gerade auch im Cyberraum besonders wichtig ist. Letztlich wird es im Allgemeinen darum gehen, die heutigen Bestrebungen im Hinblick auf Cybersicherheit vermehrt auch auf die Anforderungen der Cyberresilienz auszurichten.

2 Sicherheit

Während die deutsche Sprache für den Begriff «Sicherheit» nur ein Wort kennt, gibt es in der englischen Sprache deren zwei:

- Beim Begriff der «safety» geht es primär um die Sicherheit und den Schutz vor äusseren und nicht beabsichtigten Ereignissen und Bedrohungen. Dies können Unfälle oder natürliche Ereignisse sein (z. B. Erdbeben, Überschwemmungen, Stürme, Blitzschläge oder Brände.[1]

[1] Häufig wird in der Literatur dieser Aspekt der Sicherheit auch mit dem Begriff «Betriebssicherheit» umschrieben bzw. präzisiert.

- Demgegenüber geht es beim Begriff der «security» primär um die Sicherheit und den Schutz vor absichtlichen Handlungen und böswilligen Angriffen durch meist menschliche Akteure.

Damit drehen sich beide Begriffe um die Sicherstellung eines ordnungsgemässen Betriebs, der frei von Unfällen, Störungen und Ausfällen ist und gemäss der Spezifikation des zu schützenden Objektes verläuft. Während im Falle von «safety» nicht beabsichtigte und in einem gewissen Sinne auch zufällig auftretende und natürliche Ereignisse und Bedrohungen betrachtet werden, sind es im Falle von «security» beabsichtigte Ereignisse und Bedrohungen, die von menschlichen (bzw. menschlich gesteuerten) Akteuren mit böswilligen Absichten ausgelöst sind.

Oft wird in Diskussionen argumentiert, dass es bei «safety» um Bedrohungen von Leib und Leben von Menschen geht, während es bei «security» um Bedrohungen geht, die zwar einen störungsfreien Betrieb eines Systems beeinträchtigen können, bei denen aber grundsätzlich keine Menschen zu Schaden kommen. Diese Unterscheidung über mögliche Auswirkungen auf Menschen greift zu kurz und ist aufgrund der Vernetzung von heutigen Systemen kaum mehr aufrecht zu halten. So können viele «Security»-Probleme in diesem Sinne auch «Safety»-Probleme werden, und ob sie das tun, ist bis zu einem gewissen Grad zufällig. Beispielsweise kann eine Schwachstelle in einem Betriebssystem zu einem finanziellen Verlust führen, wenn das Betriebssystem ein IT-System kontrolliert, das Finanztransaktionen steuert. Es wäre dann ein «Security»-Problem. Demgegenüber kann die gleiche Schwachstelle Leib und Leben von Menschen gefährden, wenn das Betriebssystem z. B. in einem autonomen Fahrzeug verbaut ist, und würde dann eher ein «Safety»-Problem darstellen. Wenn – wie jüngst festgestellt[2] – ein elektrobetriebener Transportbus von seinem Hersteller aus der Ferne gestoppt oder ausser Betrieb genommen werden kann, dann stellt das zunächst ein «Security»-Problem dar. Wenn durch den Stopp aber Leib und Leben der Passagiere gefährdet werden kann, würde daraus ein «Safety»-Problem.

Aufgrund dieser Unklarheiten und terminologischen Unschärfen scheint es besser zu sein, wie oben erwähnt die zwei Aspekte der Sicherheit aufgrund des Ausgangspunkts einer entsprechenden Bedrohung (d. h. natürliche Bedrohung oder Akteur mit böswilligen Absichten) zu unterscheiden. Die erwähnte Bedrohung, die auf eine Schwachstelle in einem Betriebssystem zurückzuführen ist, stellt dann zunächst ein «Security»-Problem dar, weil die Schwachstelle absichtlich und gezielt ausgenutzt werden muss, um einen Unfall, eine Störung oder einen Ausfall zu bewirken.[3]

Die Berücksichtigung absichtlicher Handlungen und böswilliger Angriffe stellt einen eigentlichen «Game Changer» in vielen Sicherheitsdiskussionen dar; Das Bedrohungspotenzial durch menschliche Akteure ist viel grösser und vielfältiger als das Bedrohungspotenzial durch zufällige und natürliche Ereignisse. Damit stellt auch die Gewährleistung von Sicherheit im Sinne von «security» eine ungleich grössere Herausforderung dar als die Gewährleistung von Sicherheit im Sinne von «safety». Dafür gibt es viele Beispiele aus dem täglichen Leben.

- Während es z. B. relativ einfach ist, ein Haus zu bauen, das den meisten Naturgefahren[4] trotzen und damit Sicherheit im Sinne von «safety» bieten kann, ist es nahezu unmöglich,

---

[2] Autobusse in Norwegen: Sie können ferngesteuert werden (watson.ch)

[3] Der Vollständigkeit halber sei hier nur am Rande vermerkt, dass es natürlich auch Schwachstellen gibt, die ohne absichtliche und gezielte Ausnutzung zu einem solchen Zwischenfall führen können.

[4] Gemeint sind hier insbesondere meteorologische Naturgefahren, wie Hagel, Sturm, Regen, Schnee oder Blitzschlag, gravitative Naturgefahren, wie Hochwasser, Murgang, Lawinen oder Steinschlag, sowie tektonische und geologische Gefahren, wie Erdbeben oder Radonemissionen.

ein Haus zu bauen, das vor allen erdenklichen Bedrohungen durch Menschen und entsprechenden Angriffen schützt. Man denke etwa an Einbrüche oder an die Möglichkeit, im eigenen Haus Opfer eines Gewaltverbrechens zu werden. Baulich lassen sich solche Ereignisse zwar erschweren, aber nicht bzw. meist nur mit unverhältnismässig hohem Aufwand wirksam verhindern.

- Noch deutlicher ist der Sachverhalt bei der Konstruktion eines Safes. So scheint es relativ einfach zu sein, einen Safe zu konstruieren, der Naturgefahren trotzen kann. Hingegen einen Safe zu bauen, der nicht irregulär geöffnet werden kann, scheint fast unmöglich. Davon zeugt auch die Metrik, die zur Spezifikation der Sicherheit von Safes verwendet wird, nämlich die Zeit, die ein professioneller Einbrecher benötigt, um den Safe irregulär zu öffnen (der Fall, dass ein Safe grundsätzlich nicht irregulär geöffnet werden kann, wird gar nicht erst berücksichtigt).
- Das letzte hier aufgeführte Beispiel ist die Menschheit: Obwohl diese über Jahrtausende recht erfolgreich gelernt hat, Leib und Leben vor Naturgefahren zu schützen, gibt es immer noch zahlreiche Kapitalverbrechen, die sich nur schwer verhindern lassen und bei welchen Menschen sogar zu Tode kommen. Dem Einfallsreichtum und der Fantasie von Täterinnen und Tätern scheinen hier kaum Grenzen gesetzt zu sein.

Diese und viele andere Beispiele legen nahe, dass zumindest in der realen Welt die Gewährleistung von Sicherheit im Sinne von «security» eine grössere Herausforderung darstellt als jene im Sinne von «safety». So kann die Sicherheit im Sinne von «safety» oft durch den Einsatz von Redundanzen[5] verbessert werden. Im Hinblick auf die Sicherheit im Sinne von «security» können Redundanzen zu weiteren Sicherheitslücken und damit auch zu einer Vergrösserung der Angriffsfläche führen. Wenn in einem Flugzeug z. B. anstelle nur eines Piloten ein Pilot und ein Co-Pilot eingesetzt wird, dann hat diese Redundanz auch mit einer erhofften Verbesserung der Sicherheit im Sinne von «safety» zu tun. Dass damit aber die Sicherheit im Sinne von «security» nicht nur nicht verbessert, sondern sogar verschlechtert werden kann, zeigt das Beispiel eines Notausgangs, der eine redundante Möglichkeit darstellt, ein Gebäude in einem Notfall möglichst rasch verlassen zu können. Damit wird auf der einen Seite zwar die Sicherheit im Sinne von «safety» verbessert, auf der anderen Seite wird aber die Sicherheit im Sinne von «security» verschlechtert, weil der Notausgang eben auch eine zusätzliche Möglichkeit darstellt, auf nicht berechtigte Weise in das Gebäude einzudringen und damit die Angriffsfläche zu vergrössern.

Aufgrund der grösseren Herausforderungen und den entsprechenden Schwierigkeiten bei der Gewährleistung von Sicherheit im Sinne von «security» dominiert dieser Aspekt viele Sicherheitsdiskussionen. In der Tat drehen sich solche Diskussionen meist um präventive Sicherheitsvorkehrungen und -massnahmen, mit denen menschliche Akteure an ihren Taten gehindert oder diese Taten wenigstens hinreichend erschwert werden können. Beispiele sind der Häuserbau, bei dem man mit Hilfe von Türschlössern, abschliessbaren Fenstergriffen und Alarmanlagen einen präventiven Schutz erreicht, oder bauliche Vorkehrungen, die verhindern sollen, dass im Rahmen von terroristischen Anschlägen Täterinnen und Täter mit schweren Fahrzeugen ungehindert in grosse Menschenansammlungen hineinfahren können. Solche und ähnliche Sicherheitsvorkehrungen und -mass-nahmen gibt es in fast allen Bereichen des täglichen Lebens.

---

[5] Das bewährteste und bekannteste Mittel zur Sicherstellung der Verfügbarkeit technischer Einrichtungen ist die Redundanz. Im einfachsten Fall ist damit gemeint, dass einem erforderlichen System ein weiteres zur Seite gestellt wird, das bei Ausfall des ersten Systems dessen Funktion übernimmt.

3 Resilienz

Aus der Realität wissen wir, dass ausreichend starke und motivierte Täterinnen und Täter nahezu alle präventiven Sicherheitsvorkehrungen und -massnahmen umgehen oder aushebeln können, um ihre Ziele zu erreichen. Entsprechend wichtig ist es, Angriffe möglichst zeitnah erkennen und adäquat darauf reagieren zu können. Wenn z. B. ein Einbruch stattfindet, dann ist die Erkennung trivial und eine adäquate Reaktion besteht in einem Anruf bei der Polizei. Andere Ereignisse und Sicherheitsverletzungen erfordern andere Wege der Erkennung («Detection») und Reaktion («Response»), und ein gutes und umfassendes Sicherheitsdispositiv muss entsprechende Möglichkeiten aufzeigen.

Um zu verdeutlichen, dass präventive Sicherheit für sich allein betrachtet in der Realität nicht ausreichend ist, sondern durch erkennende (d. h. detektive) und reaktive Aspekte ergänzt werden muss, wird in Sicherheitsdiskussionen oft von Resilienz (anstelle oder in Ergänzung zur Sicherheit) gesprochen. Dabei geht es bei der Resilienz um die Widerstands- und Überlebensfähigkeit einer Organisation oder eines Unternehmens. Damit ist insbesondere die Fähigkeit gemeint, die kritischen Leistungen und dafür notwendigen Geschäfts- und Produktionsprozesse trotz aller Bedrohungen und Angriffe permanent aufrecht zu halten bzw. nach einem Ausfall so schnell wie möglich weiterführen zu können. Entscheidend ist dabei nicht primär nur die Verhinderung von Angriffen, sondern vor allem auch die Fähigkeit, in Notfällen handlungsfähig zu bleiben, die Schäden wirksam zu begrenzen und so rasch als möglich zum Normalbetrieb zurückzukehren. Obwohl das nicht immer möglich und selten einfach ist, muss es das erklärte Ziel aller Überlegungen und Bestrebungen sein. Wenn sich ein sicherheitsrelevanter Vorfall ereignet, muss dieser zeitnah erkannt und adäquat darauf reagiert werden können. Diese Fähigkeit ist zwingend erforderlich, damit das durch den Vorfall verursachte Problem überschau- und handhabbar bleibt und sich für die Organisation oder Unternehmung nicht zu einer Krise auswachsen kann. Entsprechend sollte sich eine Organisation oder Unternehmung weniger auf Sicherheit als vielmehr auf Resilienz ausrichten. Denn erst durch Resilienz lassen sich Ereignisse so bewältigen, dass einer Organisation oder Unternehmung kein, respektive ein möglichst geringer, Schaden entsteht.

Bildlich gesprochen könnte man die Sicherheit mit einer Schildkröte assoziieren, die sich bei bestimmten Gefahren in ihren Panzer zurückziehen kann und dann relativ gut geschützt ist.[6] Demgegenüber könnte man die Resilienz mit einem Axolotl[7] assoziieren, bei dem einzelne Körperteile bei Verlust nachwachsen können. Diese einzigartige Fähigkeit erlaubt es dem Lurch, in seinem Lebensraum zwar nicht unbedingt sicher, dafür aber relativ resilient zu sein. Die Natur hat damit zwei unterschiedliche Ansätze ausgebildet, wie Lebewesen mit gefährdenden Ereignissen umgehen können. Auf der einen Seite können sie – wie die Schildkröte – eine Physis entwickeln, die bestmöglich vor solchen Ereignissen schützt. Auf der anderen Seite können sie – wie der Axolotl – solche Ereignisse zwar in Kauf nehmen, aber sich bestmöglich auf eine Heilung vorbereiten. Beide Ansätze haben Vor- und Nachteile, wobei in beiden Fällen die Nachteile wohl überwiegen. Der hauptsächliche Nachteil eines Panzers besteht darin, dass er nur vor bestimmten Ereignissen schützt und im Hinblick auf andere sogar kontraproduktiv ist. So schützt ein Panzer z. B. gut vor Steinschlag und Angriffen von kleineren Raubtieren, Feuer und menschlichen Angriffen kann er aber kaum etwas entgegensetzen bzw. wirkt sich sogar hemmend auf allfällige Reaktionsmöglichkeiten aus. Demgegenüber hilft

---

[6] Natürlich trifft dieses Bild vor allem auf die Sicherheit im Sinne von «safety» und weniger gut auf die Sicherheit im Sinne von «security» zu.

[7] In der englischen Sprache wird der mexikanische Schwanzlurch als «Axolotl» bezeichnet, wobei der Begriff aus der aztekischen Sprache Nahuatl stammt.

die Fähigkeit, einzelne Körperteile bei Verlust nachwachsen lassen zu können, zwar bei seltenen Ereignissen, läuft aber bei Ereignissen, wie beispielsweise ein Angriff durch einen Fressfeind ins Leere. Natürlich schliessen sich beide Ansätze nicht aus und können idealerweise miteinander und mit weiteren Ansätzen kombiniert werden. Diese Suche nach neuen Ansätzen und Kombinationsmöglichkeiten zur Gewährleistung der Sicherheit und Resilienz findet in der Natur im Rahmen der Evolution laufend statt.

4 Sicherheit und Resilienz im Cyberraum

Alle bisherigen Ausführungen gelten für die physische Welt und in sogar verstärktem Masse auch für die digitale Welt. So muss ein böswilliger Akteur im Cyberraum z. B. nicht einmal physisch am Tatort in Erscheinung treten. Stattdessen kann er einen Angriff aus sicherer Entfernung auslösen bzw. steuern. Aus dieser Ortsunabhängigkeit und der Möglichkeit, Angriffe von irgendwo auszulösen bzw. zu steuern, ergeben sich noch grössere Vorteile für mögliche Angreifer. Die Kluft zwischen der Sicherheit im Sinne von «safety» und der Sicherheit im Sinne von «security» wird damit noch grösser. Im Umkehrschluss heisst das aber auch, dass die Gewährleistung der Sicherheit im Sinne von «security» gegenüber der Sicherheit im Sinne von «safety» im Cyberraum eine noch viel grössere Herausforderung darstellt als in der physischen Welt (wobei sich im Fall von cyber-physischen Systemen[8] die Herausforderungen sogar noch kumulieren).

Weil viele Geschäftsmodelle im Cyberraum auf Daten basieren und die Wiederherstellung von Daten – im Gegensatz zu den meisten physischen Gütern – nicht immer möglich ist, kommt der Resilienz im Cyberraum eine entsprechend grosse Bedeutung zu. Wie können Daten nach einem Sicherheitsvorfall wieder hergestellt werden? Wie kann überhaupt erkannt werden, ob Daten verändert worden und damit nicht mehr authentisch und integer sind, und wie kann sichergestellt werden, dass sie es über eine möglicherweise lange Zeit bleiben? Solche Fragen betreffen die digitale Welt und damit die Cyberresilienz. Natürlich könnte man die Fragestellungen auch unter der Cybersicherheit subsummieren, aber unter dem Begriff der Cyberresilienz werden – wie oben erwähnt – die Aspekte «Detection» und «Response» stärker hervorgehoben. Das scheint auch deshalb wichtig zu sein, weil im Cyberraum noch mehr als in der physischen Welt davon ausgegangen werden muss, dass Angriffe nicht nur möglich sind, sondern in vielen Situationen auch erfolgreich durchgeführt und vielleicht nicht oder erst (zu) spät erkannt werden können (so gibt es in den Diskussionen rund um «Zero Trust» z. B. die oft erwähnte «Assume Breach»-Annahme, die davon ausgeht, dass erfolgreiche Angriffe sowieso immer stattfinden können).

Aufgrund dieser Überlegungen müssen sich Organisationen und Unternehmen in Zukunft noch stärker auf Resilienz (und vor allem Cyberresilienz) ausrichten und dazu insbesondere auch ihre erkennenden und reaktiven Fähigkeiten stärken. Sie sollten sich je länger, je weniger darauf verlassen, sicherheitsrelevante Vorfälle ausschliesslich mit präventiven Vorkehrungen und Massnahmen beherrschen zu können. Angreifern kann und wird es stets gelingen, Sicherheitsmassnahmen zu überwinden. Die Fähigkeit dies zeitnah zu erkennen und adäquat darauf zu reagieren, wird zunehmend zu einem Schlüsselfaktor einer effizienten Cyberabwehr. Entsprechend stellt die Cyberresilienz die zentrale Fähigkeit einer Organisation oder Unternehmung dar, um im Cyberraum langfristig bestehen zu können. Dabei gilt es, systemisch zu denken und das gesamte Geschäftsumfeld (inklusive Lieferanten, Kunden, usw.) in

[8] Cyber-physische Systeme sind Systeme, bei denen informations- und softwaretechnische mit mechanischen Komponenten verbunden sind, wobei Datentransfer und -austausch sowie Kontrolle bzw. Steuerung über eine Infrastruktur wie das Internet in Echtzeit erfolgen können.

die Überlegungen mit einzubeziehen und dabei auch die Brücke zum Business Continuity Management (BCM) zu schlagen. Die heutigen Bestrebungen im Hinblick auf Cybersicherheit müssen vermehrt auf die Anforderungen der Cyberresilienz ausgerichtet werden. Ähnlich wie bei Schildkröten und Lurchen in der Natur wird es auch im Cyberspace keine «One size fits all»-Lösung geben. Sowohl die IT-Landschaften als auch deren Umgebungen ändern sich ständig, so dass ein heute sinnvoller Ansatz zur Sicherstellung der Cyberresilienz vielleicht morgen den Anforderungen nicht mehr genügt und entsprechend angepasst werden muss.[9] Entsprechend ist die Gewährleistung der Cyberresilienz eine andauernde Aufgabe, die es entsprechend auszugestalten gilt. Mit Sicherheit zählt die Vorbereitung auf Cyberbedrohungen zu den wichtigsten Aufgaben von Organisationen und Unternehmen – in der Gegenwart wie in der Zukunft.

[9] Natürlich gilt das nicht immer und viele Ansätze sind universell und bis zu einem gewissen Grad auch zeitlos. Insbesondere gilt das für Ansätze, die aus dem Bereich des IT-Grundschutzes bekannt sind.