Bernhard R. Barz

Security-System Engineering

Daten, Netze, Mensch-Maschine-Interaktionen und Automatisierung – Kernelemente der Digitalisierung – beherrschen die Entwicklung von Systemen und die Aktivitäten von Personen, Organisationen und Staaten. Daten sind längst zur Währung, zum Produktions- und Wirtschaftsfaktor geworden; „Persönlichkeit" wird in Sozialen Netzen virtualisiert. Die Durchdringung aller Lebensbereiche von der Digitalisierung ist somit unmittelbar mit dem Schutz digitaler Werte verbunden. Aufgrund der Immaterialität der Daten kann dieser Schutz immer nur indirekt bei den Verarbeitungsroutinen und -techniken sowie den beteiligten Endsystemen ansetzen.

Einleitung

Die Komplexität der Informationssicherheit erscheint derart umfangreich, dass es mit einer Handvoll „goldener Regeln" als Schutzgebote nicht getan ist. Eine entsprechende (englischsprachliche) Anfrage in Suchmaschinen bringt die schiere Unmenge von 111 Mio. „Antworten" zu Tage. Woran liegt das?

Im Jahr 2007 fragte der Sicherheitsexperte Bruce Schneier in einem Blog-Eintrag, ob der Sicherheits-Markt ein „Market for Lemons" sei [1]. Anlässlich der Nachricht, dass ein Memory-Stick mit angeblichen Verschlüsselungseigenschaften als völlig unsicher entlarvt wurde, warf er die Frage auf, warum sich mittelmäßige (Sicherheits-) Produkte auf dem Markt durchsetzen. Der Begriff „Market for Lemons" geht auf den Ökonomen und Nobelpreisträger George Akerlof zurück. Als „Zitrone" im übertragenen Sinne wird auch im Deutschen der Umstand bezeichnet, dass Käufer eines Produktes dessen wahre Qualitätseigenschaften nicht bewerten und so vom Verkäufer leicht getäuscht werden können; es wird „mit Zitronen gehandelt". Diese Asymmetrie der Informationen und Kenntnisse führt – so Akerlof – zu einer Verdrängung guter (und in der Regel teurerer) Produkte und Hersteller; oder andersherum: nicht die Qualität setzt sich durch, sondern die preisgetriebene Mittelmäßigkeit.

Schneier kommt zu dem Schluss, dass mangels wirksamer Prüfmöglichkeiten dem Käufer oftmals nichts anderes übrigbleibt, als auf Differenzierungs- und Vergleichsmerkmale zu achten, die als Kaufentscheidungen herangezogen werden können. Hierzu zählen technische Daten, Reputation des Herstellers, Standardisierungen und weitere.

Debate Security ist eine Vereinigung von Sicherheitsfirmen und Herstellern von Sicherheitsprodukten, die sich mit der Frage beschäftigt, ob und in welchem Umfang Cybersecurity Technology tatsächlich einen Sicherheitsgewinn liefert und wie dieser bemessen werden kann. Im Jahr 2020 veröffentlichte sie einen Forschungsbericht mit dem Titel: „Cybersecurity Efficiacy, Is cybersecurity the new ‚market for lemons'?" [2]. Dieser Frage wurde auf Basis von Interviews nachgegangen. Folgende Kernaussagen und Schlüsse wurden gezogen:

- Die Ausgaben für Cybersicherheit steigen von Jahr zu Jahr in beträchtlichem Umfang, obschon die Verantwortlichen die Risiken einer „Cyberattacke" weiterhin als (zu) hoch einschätzen.
- Der überwiegende Teil der Befragten gab an, dass die „Efficacy" der Lösungen nicht den Ansprüchen genügt. „Efficacy" wird dabei durch vier Eigenschaften charakterisiert: Die Technology muss die erforderlichen Fähigkeiten („Capabilities") in einer ausreichenden Qualität („Quality") für die vorgesehenen Einsatzzwecke aufweisen. Darüber hinaus muss sie praktisch nutzbar sein („Practicality"): Die Einführung, die Integration in die bestehende Systemlandschaft und der Betrieb inklusive Wartung müssen möglich sein. Abschließend wird mit der Eigenschaft Provenienz („Provenance") die Reputation des Herstellers inklusive seiner Lieferkette bewertet.

Für Debate Security ist das Problem vornehmlich ein ökonomisches und kein technisches, welches u. a. auch damit zusammenhängt, dass die Käufer aufgrund des dafür erforderlichen Zeit- und Kostenaufwands nicht in der Lage sind, die „Bewerbung" eines Produkts angemessen zu bewerten. Dieses Missverhältnis wird als Asymmetrie im Sinne von Akerlofs „Markt der Zitronen" gewertet.

Als Lösungsansatz schlägt Debate Security ein (Entwicklungs) Modell mit neuen Anreizen für Hersteller und Lieferanten sowie Möglichkeiten für Käufer vor. Im Kern sollen auf der Basis unabhängiger Technologiebewertungen durch vertrauenswürdige Instanzen die Informationsasymmetrie verringert und dadurch risikoreduziertere Entscheidungen ermöglicht werden.

Bernhard Barz

war fast 20 Jahre Informationssicherheitsbeauftragter eines IT-Dienstleisters. Sein Interesse gilt der Weiterentwicklung und Fundierung der Informationssicherheit durch Anwendung system- und ingenieurtechnischer Methoden.
E-Mail: barzbernhard@gmx.de

Beide Darstellungen konzentrieren sich auf die Informationsasymmetrie zwischen Käufern und Nutzern von Cybersecurity-Lösungen einerseits und den Produktherstellern andererseits. Dies ist jedoch nur ein Teilaspekt der Beherrschung der mit Informationssicherheit verbunden Risiken und Missstände. Eine erweiterte Betrachtung der Ansätze führt im Kontext der Sicherheitsbedürfnisse des Käufers und der Nutzer schnell zu einer Reihe von ökonomischen und ökologischen Fragestellungen:

- Besteht Klarheit darüber, welche geschäftlichen oder betrieblichen Sicherheits-Anforderungen durch ein Security-Produkt „gelöst" werden sollen („Tailoring")?
- Können der Nutzen und die Effizienz der Sicherheitsfunktionen des Security-Produkts im Sinne eines Sicherheits-(Zu)Gewinns a priori bestimmt werden? Gibt es dafür etablierte Kennzahlen?
- Kann der Sicherheitsgewinn („Security gain") einer isolierten Maßnahme im Kontext aller im eigenen Umfeld etablierten Sicherheitsmaßnahmen bestimmt werden?
- Wie kann die Beeinflussung von vorhandenen technischen, organisatorischen, personellen oder prozessualen Maßnahmen durch die Integration neuer Sicherheitsfunktionen geprüft und optimiert werden?
- Gibt es praktische, standardisierte Bewertungsmethoden zur Bewertung der Wirtschaftlichkeit von Investitionen und Ressourceneinsätzen bei Einzel- bzw. ergänzenden Maßnahmen?

Unabhängig davon ist das Risiko, von einem digitalen Einbruch oder Datendiebstahl betroffen zu sein, real. Dies führt zu dem Dilemma, dass der realen Gefährdungslage eine Unsicherheit über die Wirksamkeit von Sicherheitsinvestitionen und -kosten gegenübersteht. In diesem Sinne gleicht das Feld der Informationssicherheit eher einer Erfahrungswissenschaft. Stakeholder als Initiatoren und Empfänger der Informationssicherheit für „ihre" Geschäftssysteme und -prozesse haben eine diffuse Entscheidungsgrundlage und Prüfmöglichkeit für die Angemessenheit ihrer Investitionen. Die Entwickler und Betreiber der Sicherheitsmaßnahmen operieren – überspitzt – mit fehlender Verantwortungsübernahme für die Wirksamkeit der Sicherheitsmaßnahmen im Sinne eines Leistungserbringers.

Wünschenswert wäre eine steuerbare Fundierung und Ausprägung – eines Sicherheitsmanagements – nach wirtschaftlichen und methodischen Maßstäben. Dies bedingt nicht nur eine klare Aufgaben- und Verantwortungsabgrenzung zwischen Anforderern und Erbringern einzelner Sicherheitsmaßnahmen. Ausreichende Klarheit erfordert nach Auffassung des Autors die Betrachtung aller Sicherheitsmaßnahmen als ein geschlossenes funktionales Sicherheitssystem („Security-System"), das mittels standardisierter Methoden entwickelt und betrieben wird. Im Kontext technischer Systeme fällt hier der Blick auf Engineering-Methoden.

Engineering und Informationssicherheit

Ingenieurtechnische Begriffe werden derzeit nur vereinzelt in Literatur und Best-Practice-Werken der Informationssicherheit verwendet oder ausgeprägt. Der Begriff „Security Engineering" wurde von Ross Anderson als Titel des über 1000 Seiten umfassenden Werkes „A Guide to building dependable distributed systems" benutzt [3]. Initial merkt er an, dass schon der Begriff „Security" schrecklich überladen ist und von unterschiedlichen Akteuren vielfach in recht inkompatibler Art und Weise verwendet wird.

Unter „Security Engineering" versteht Anderson die Konzentration auf Werkzeuge, Prozesse und Methoden zur Erstellung von Systemen, die angesichts beabsichtigter und unbeabsichtigter Ereignisse weiterhin zuverlässig ihre Funktion erfüllen. Damit ordnet er allgemein einem System die Eigenschaften einer Zielsetzung (Funktion) und eines Qualitätsanspruches (Zuverlässigkeit) zu. Darüber hinaus wird ein wie auch immer geartetes (Betriebs-) Umfeld erfasst, mit dem das System beabsichtigt sowie unbeabsichtigt interagiert; hier ereignisorientiert. Er führt weiterhin aus, dass „Security Engineering" Kenntnisse in unterschiedlichen technischen und nicht-technischen Disziplinen erfordert. Er begnügt sich jedoch mit einer Beschreibung, *was* zu einer Entwicklung eines Systems erforderlich ist, und klammert aus, *wie* und *womit* dies vorgenommen werden kann.

Anderson entwickelt den Begriff „System" anhand unterschiedlicher Interpretation in einer Art Verständnispyramide von technischen Komponenten oder Produkten über den IT-Betrieb bis zum Nutzer bzw. Peer-Nutzer eines Geschäftsprozesses. Hierbei bleibt er jedoch im Kontext der einzelnen Komponente und versteht als System alle Aktivitäten rundherum, von der korrekten Auswahl über die Konfiguration, den Betrieb und die Nutzung derselben.

Eine andere Engineering-Sicht wird in der aktuellen Fassung der ISO/IEC 27002:2022 eingenommen. Mit Control 8.27 verwendet die ISO 27002 ergänzend zu „social engineering" ein weiteres Mal einen Engineering-Ansatz in der Kategorie der technischen Controls als „Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities" [4].

Hier wird Engineering jedoch ausschließlich im Kontext der Entwicklung von „Information Systems" verstanden, die gemäß der Definition in Kapitel 3 der Norm auf informationsverarbeitende (Hardware-/Software-)Komponenten begrenzt werden. Engineering-Aktivitäten sind also solche, die den Prinzipien „Security by Design" and „Security by Default" in Bezug auf einzelne Komponenten Genüge tun; so wird es von vielen Anwendern der ISO 27002 interpretiert.

Konsequenterweise ist die operative Komponente gemäß der Zweckbeschreibung dieses Controls – „To ensure that information systems are securely ... operated ..." – so zu interpretieren, dass implementierte Sicherheitsfunktionen im Sinne einer maximalen Nutzung der integrierten Sicherheitsansätze optimal konfiguriert werden (sollen).

Der Anwendung der „engineering principles" muss laut ISO 27002 eine vollständige Anforderungsanalyse („Requirement Engineering") im Kontext der Geschäftsprozesse vorausgehen. Interessanterweise umfasst dies auch Fragen zur Architektur sowie zum Zusammenspiel unterschiedlicher Security Controls. Dieser umfangreichere Ansatz wird jedoch im Lichte der Definition der „information systems" als datenverarbeitende Komponenten nicht weiterverfolgt. ISO 27002 bleibt somit ein Best-Practice-Katalog von Controls.

Die dargelegten „principles for engineering" umfassen Architektur-Prinzipien, Design-Prozesse, Dokumentations- und Entscheidungs-Aktivitäten sowie die Härtung von Systemen. Architektur-Prinzipien beziehen sich auf unterschiedliche Aspekte der Architektur, womit Design und Integration von Sicherheitsfunktionen in die Komponente umfasst sind. Sowohl die Vielfalt der

implementierten Sicherheits-Funktionen – möglichst keine Multi-Funktionalität – als auch die Konfigurationsmöglichkeiten sollen auf definierte Sicherheitsziele ausgerichtet sein.

Andere Prinzipien sind eher auf das Zusammenwirken und die Verknüpfung von Controls ausgerichtet. Die damit verfolgten Ansätze zielen auf die Reduzierung der Auswirkungen des Versagens eines einzelnen Controls in einem Gesamtverbund. Wenn ein Control bzw. eine Komponente versagt, sollen die (Gesamt) Auswirkungen möglichst kontrollierbar bleiben, indem Ausfälle durch andere Komponenten „aufgefangen werden". Interaktionsmechanismen von Controls werden gemäß dem einleitenden Kapitel (Kap. 0.4) mit dem Begriff „defense in depth" als Kriterium zur Auswahl von Controls verknüpft. So soll trotz Ausfalls möglichst ein kontrollierbarer Komponentenzustand bestehen bleiben („fail secure").

Die über die „architectur principles" hinaus gehenden Aspekte umfassen die Anforderung, dass das Design der Komponente einem regelmäßigen Review unterzogen wird. Dies zielt auf den Lifecycle-Ansatz, in dem auf neue oder bekannt gewordene Schwachstellen reagiert und mit Fokus auf Sicherheits-Anforderungen bearbeitet werden. Komponenten sind über den gesamten Lifecycle hinweg „a jour" zu halten. Damit wird nochmals unterstrichen, dass Engineering auch die Definition von Sicherheitsanforderungen als Design-Ziel der Komponenten einschließt.

Für die ISO gehört es zum Engineering-Kontext, dass die Ausprägung der Controls ggf. mit anderen Anforderungen wie beispielsweise Safety-Aspekten „in Konkurrenz" steht und die Balance ggf. mit oder unter formalen Anforderungen zu entscheiden ist. Das Hardening von Systemen ist zwar separat aufgeführt, wird jedoch grundlegend durch o. g. Aspekte wie „least functionality", „least privilege" oder „security by default" erfasst.

Ergänzend zur Vorläuferversion der ISO 27002:2022 wurde das Thema „zero trust" aufgenommen und separat aufgeführt. Zero Trust zielt auf die Kommunikation und den Datenaustausch zwischen Einheiten und stellt in Bezug auf das Engineering eines Informationssystems somit den Kontext bzw. die Umfeldbedingungen des Betriebs dar. Ähnlich wie „assume breach" oder „distrust external input" stellt dies nach Ansicht des Autors eine Management-Haltung dar, die von einem „worst case"-Betrieb ausgeht.

Zusammenfassend kann festgestellt werden, dass bisherige Engineering-Ansätze die Beschreibung der Anforderungen bzw. die Hinweise zur Umsetzung von Engineering-Prinzipien für einzelne Komponenten im Vordergrund stellen. Ansätze eines übergreifenden Architektur- und System-Verständnisses werden sichtbar. Dargestellt sind Anforderungen und Erläuterungen, *was* umzusetzen ist, jedoch nicht *wie* das im Detail erfolgen kann. Zudem lässt die gewählte Konzentration auf informationsverarbeitende Komponenten Fragen eines übergreifenden Zusammenspiels von Controls offen.

Systems Engineering

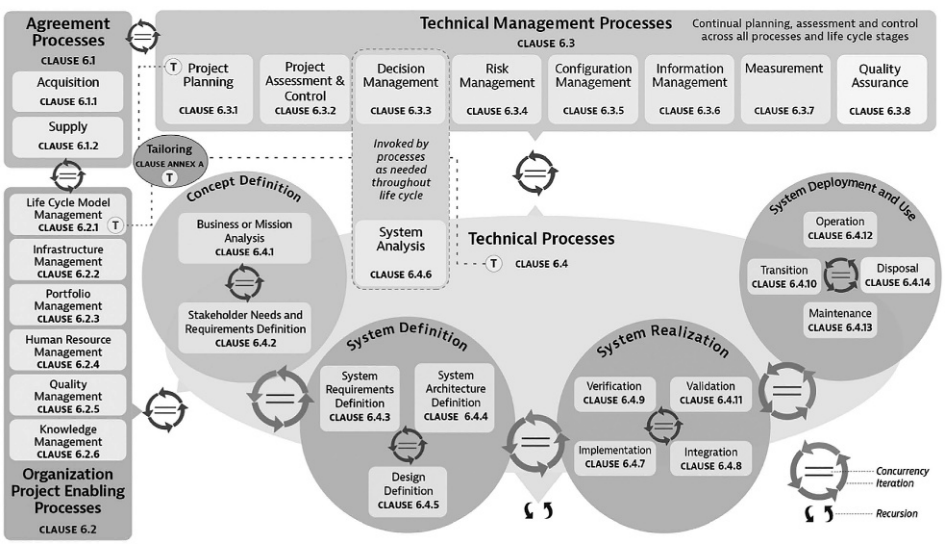
Die Lücken zur Definition, Entwicklung und zum Betrieb eines geschlossenen funktionalen Sicherheitssystems („Security-System") werfen die Fragen auf, ob es allgemeine Engineering-Ansätze zu Systemen gibt und wie diese in den Kontext der Informationssicherheit übertragen werden können.

Mit dem Standardwerk ISO 15288:2023 „Systems and software engineering – System life cycle processes" [5] steht ein generisches Framework von Prozessen aus Engineering-Sicht zur Verfügung. Als Zweck und Ausrichtung des Standards definiert die ISO die „Beschreibung von Prozessen zum Lifecycle von Systemen aus Engineering-Sicht. Dies dient der Kommunikation an der Schnittstelle zwischen unterschiedlichen Akteuren sowie als Basis zur Etablierung organisatorischer Rahmenbedingungen zur Anwendung/Umsetzung der Prozesse". Die ISO 15288 verfolgt die klare Ausrichtung, ingenieurtechnische Methoden und Prozesse zur Entwicklung, zum Design und Betrieb von Systemen anzuwenden. Ausdrücklich versteht die ISO 15288 „Systeme" als ein ganzheitliches Konstrukt, das eine Zielsetzung hat und bestimmte Anforderungen erfüllt. Die Definition, dass „Systeme ein Zusammenschluss von Teilen oder Elementen sind, die nur gemeinsam ein gewünschtes Gesamt-Verhalten ermöglichen" drückt aus, dass die Engineering-Aufgaben die Auswahl und Zusammenstellung von einzelnen Teilen unter der Zielsetzung eines gewünschten Gesamt-Verhaltens umfassen.

Als primäre abgegrenzte Akteure sind Anforderer („Acquirers") und (Leistungs-)Erbringer („Supplier") sowie „andere Stakeholder" definiert und adressiert, zwischen den Leistungsbeziehungen aufgespannt werden. Dies impliziert, dass die eine Seite Anforderungen definieren muss und die andere Seite in der Nachweispflicht zur Erfüllung der Anforderungen steht. Damit ist auch verbunden, dass der Leistungserbringer klar die wirtschaftlichen Entscheidungen verantwortet, die zu einem für den Anforderer akzeptablen oder zumindest akzeptierten Leistungspreis führen.

Ein zentrales Element des Standards sind die definierten Engineering-Prozesse und deren Zusammenwirken. Dies ist durch Abbildung 5 des Standards wie folgt verbildlicht (Abb. 1).

Abb. 1 | Engineering-Prozesse und deren Zusammenwirken (Quelle: ISO/IEC/IEE 15288:2023)



Die Norm gliedert die Prozesslandschaft in vier Hauptkategorien:

- Technische Prozesse umfassen u. a. die Anforderungsanalyse, die Systemarchitektur sowie die Verifikations- und Validierungsprozesse. Ziel ist es, die funktionalen und nicht-funktionalen Anforderungen eines Systems präzise zu spezifizieren und deren Erfüllung systematisch sicherzustellen.
- Projektbezogene Prozesse sind die Planung, Steuerung, Überwachung sowie das Risikomanagement. Sie dienen der effizienten, zielgerichteten und kontrollierten Durchführung komplexer Entwicklungsprojekte.
- Unter unterstützende Prozesse fallen das Konfigurations- und Qualitätsmanagement sowie das Informationsmanagement. Sie sichern die Konsistenz, Rückverfolgbarkeit und Qualität über alle Projektphasen hinweg.
- Schließlich adressieren organisatorische Prozesse u. a. das Ressourcenmanagement sowie die Definition übergeordneter Richtlinien und Strategien zur nachhaltigen Leistungssteigerung von Organisationen.

Von besonderer Relevanz sind die Interdependenzen dieser Prozesse: Die Anforderungsanalyse liefert beispielsweise die Grundlage für die Systemarchitektur; gleichzeitig stellen Qualitätssicherungsprozesse sicher, dass die Ergebnisse sämtlicher Aktivitäten den definierten Standards entsprechen. Nur durch die konsequente Integration dieser Prozesse kann ein konsistenter, robuster und effizienter Systemlebenszyklus gewährleistet werden.

Ein herausragendes Merkmal der ISO 15288 ist ihr systemischer, integrativer Ansatz, der sich deutlich von isolierten, komponenten- oder maßnahmenorientierten Vorgehensweisen abhebt. Die ISO 15288 stellt ein normatives Fundament für das moderne Systems Engineering dar. Sie bietet eine systematische Methodik zur Anforderungserhebung, Prozessstrukturierung und Qualitätssicherung, fördert eine transparente Zusammenarbeit der Akteure und unterstützt eine nachhaltige Entwicklung technischer Systeme. Ihre Anwendung ermöglicht das Design und die laufende Anpassung und Weiterentwicklung komplexer Systemlandschaften.

Security-System Engineering

Die Anwendung und der Betrieb von Sicherheitsmaßnahmen aus Normen und Best-Practices-Katalogen dienen grundlegend dem Schutz der Geschäftssysteme und -prozesse bzw. der Verarbeitung der Daten im Kontext der Digitalisierung derselben. Gerade die kataloghafte Darstellung und isolierte Abarbeitung einzelner Maßnahmen lenkt hierbei jedoch von einer durchgängigen Orientierung an Zielen und Anforderungen aus Geschäftssicht ab. Eine ganzheitliche Betrachtung und Ausrichtung der Summe aller Sicherheitsmaßnahmen als „eigenständiges" Konstrukt kann hier eine deutlichere Ausprägung im Sinne eines steuerbaren Security-Systems ermöglichen. Als abgeschlossenes System, welches die Sicherheitsmaßnahmen bündelt, ergeben sich eine Reihe vorteilhafter Konsequenzen.

Eine klare Trennung zwischen der Verantwortung für Geschäftssysteme/-prozesse und der für das Security-System fördert eine Schnittstelle als Anforderungs- und Leistungsbeziehung. Dies eröffnet Handlungsspielräume in Bezug auf die Entwicklung und den Betrieb des Security-Systems, in dem auf definierte Nachweis-Verpflichtungen im Sinne einer Zusicherung („Assurance") referenziert wird.

Investitionen und Aufwände / Ressourcen zu Sicherheitsmaßnahmen können somit transparenter gestaltet werden. Aus Sicht der Nutzer des Security-Systems bildet dies als Inhouse- oder externe Dienstleistung ein steuerbares Management-System.

Über das allgemeine Verständnis von Systemen hinaus sind mit einem Security-System einige Besonderheiten verbunden. Wesentlich ist bspw. ein direkter Eingriff in die Kommunikationsbeziehungen durch Prüfmechanismen zu Datenverarbeitungsentitäten; gleichzeitig erfolgt ein direkter Eingriff in die Datenkommunikation. Auch besteht die Notwendigkeit, Sicherheitsfunktionen in Geschäftsanwendungen zu integrieren. Diese teilweise tiefen Eingriffe in Geschäftsanwendungen und -prozesse erfordern, dass für Security-Systeme im Gegensatz zu physikalischen Systemen eine überwiegend funktionale Abstraktion und Sichtweise einzunehmen ist.

Unter Anwendung dieser funktionalen Prägung eines Security-Systems besteht die Möglichkeit die Bereitstellung, Entwicklung und den Betrieb gemäß allgemeiner Engineering-Methoden und Prozesse bspw. auf Basis der ISO 15288 umzusetzen. Dies impliziert Ansätze, das Sicherheitsniveau als Qualitätsmerkmal des Security-Systems funktional zu bestimmen. Damit verbunden ist die stärkere Ausprägung einzelner Maßnahmen an dem Sicherheits(zu-)gewinn, so dass eine optimierte Wirksamkeitspräferenz im Zusammenspiel aller Maßnahmen erzielt werden kann.

Strukturell kann das Design der System-Architektur mit einer Ausprägung an funktionalen Building-Blocks definiert werden. Zielführend ist hier eine konsequentere Definition und Anwendung des Begriffs „Concern". Die Norm ISO 2700x verwendet den Begriff „Concern" vornehmlich als Zuordnungskriterium, um die Mengen an Sicherheitsmaßnahmen ihren hauptsächlichen „Adressaten" zuzuordnen (ISO 27002, Kap. 4.2). Dies schafft ggf. Ordnung im Sinne von „wer stellt die Umsetzung sicher". Demgegenüber wird Engineering geprägt durch die Aspekte und Beeinflussungsmöglichkeiten, die bei der Systementwicklung zu bedenken sind, um eine Zielsetzung zu erreichen. Im Kontext des Security-Systems sind also eher komplexe Anliegen („Concerns"; sic!) - wie Sicherstellung, dass nur gewünschte Entitäten an Geschäftsprozessen und -verarbeitungen teilnehmen - prägend. Selbstredend ist, dass derartige „Concerns" durch unterschiedliche direkte und indirekte Sicherheitsmaßnahmen („Controls") unterstützt werden. Art und Anzahl der Maßnahmen zu einem „Concern" sind so differenziert und vollständig wie nötig und unter Berücksichtigung gegenseitiger Abhängigkeiten auszuwählen und auszuprägen. In diesem Sinne können die Maßnahmen eines „Concerns" auch als Sub-System aufgefasst werden; das Gesamt-System entspricht dann einem SoS - System of Systems; eben Building-Blocks.

Security-System Engineering Prozessframework

Auf Basis der Prozesse der ISO 15288 kann eine Adaption der Engineering-Prozesse auf Security-System grob wie folgt skizziert werden:

Seitens der Verantwortlichen der Geschäftssysteme und -prozesse erfolgt eine Definition der „Business Requirements" inkl. geschäftsorientierter Kennzahlen. Die Anforderungen sind auf

die Sicherheitsaspekte aus Geschäftssicht fokussiert und lassen sich in Form von Vermeidungsanforderungen formulieren (sog. „Loss of - Bedingungen"); Beispiele sind „Loss-of Assets", „Loss-of-Performance", etc. Äquivalent werden mittels „Security Requirements" grundlegende Rahmenbedingungen zur Umsetzung und Anwendung in weiteren Prozessschritten im Sinne einer Security-Governance definiert. Hierzu gehören neben Rahmenbedingungen zu Risiko-Assessments auch grundlegende Definitionen der anzuwendenden Sicherheitssichten; bspw. Daten-, Asset- oder Gefährdungssicht.

Sowohl grundlegende Geschäfts- als auch Sicherheits-Indikatoren sind im Sinne einer vertraglichen Regelung als „Assurance-Indicator" zu formulieren. Dies unterstreicht eine klare Trennung der Verantwortungsbereiche einerseits und ermöglicht andererseits eine Kopplung an Leistungsentgelte und Bonus-/Malusregelungen.

Zur Entwicklung des Security-Systems ist die initiale bzw. laufende Erfassung möglicher Störeinflüsse auf das Security-System durch ein umfassendes „Exposure-Management" erforderlich. Hierdurch werden interne und externe Bedrohungsquellen erfasst und mittels eines „Impact-Assessments" bewertet. Im Besonderen sind hierzu neben Bedrohungsquellen auch Bedrohungs-Pfade („Exposure-Vectors") zu erheben, da Einstiegspunkte und Wirkpunkte von Gefährdungen in der Regel nicht zusammenfallen.

Der wesentliche Kern des „Security Engineering" stellt das Design der Sicherheitsarchitektur („Security Architecture") dar. Ziel ist es, die wesentlichen Sicherheitsfunktionen und ihrer Struktur unter Anwendung geeigneter Architekturprinzipien für die definierten Geschäfts- und Sicherheitsanforderungen zu entwickeln.

Aufbauend hierauf erfolgt mit der Definition der Controls der Abschluss der Design-Phase sowie der Übertrag in die Betriebs-Phase des Systems. Kernaufgabe ist die nicht nur die Auswahl passender Controls, sondern die Erfassung der notwendigen organisatorischen, personellen und prozessualen Rahmenbedingungen, die zur vollständigen Entfaltung der (intendierten) Wirksamkeit von Controls erforderlich sind.

Bei allen Anforderungs- und Design-Prozessphasen sind die erforderlichen Maßnahmen zur Erfassung und Bewertung der genannten „Assurance Indicator" integriert zu bewerkstelligen. Diese bilden die Schnittstelle zwischen Stakeholder (Anforderer) an das Security-System und Leistungserbringer (Supplier). Definition und Nachweis sind das Kern-(Austausch-)Element für beide Verantwortungsseiten und elementar zur Sicherstellung, dass eben nicht „mit Zitronen gehandelt" wird. Im übertragenen Sinne wird ein Vertrauensverhältnis geschaffen, das mit dem Begriff „Trustworthiness" in der Definition als Schaffung eines Vertrauensverhältnisses („worth to be trusted") bezeichnet wird.

Weitere, ausführlichere Details und Informationen zum Security-Engineering-Prozess sowie Rahmenprozessen sind in der Hintergrundliteratur [6] dargestellt.

Ausblick

Die Sichtweise eines Security-Systems als System, in dem die Summe alle Sicherheitsmaßnahmen und -funktionen als eigenständiges Konstrukt betrachtet und betrieben wird, ist derzeit in der Informationssicherheit nicht etabliert. Sehr wohl sind hiermit eine Reihe von Vorteilen und natürlich auch Herausforderungen verbunden. Eigenständige Handlungsbereiche und eine Anforderungs-/Lieferantebeziehung stellen eine klare Zuweisung und Trennung der Verantwortungsbereiche dar.

Dies eröffnet gleichzeitig eine transparente Bewertung der Sicherheit und ermöglich so eine ökonomischere Bereitstellung und Steuerung erforderlicher Sicherheitsniveaus für die Geschäftssysteme und -prozesse.

Literatur

[1] Schneier B., *A Security Market for Lemons*, https://www.schneier.com/blog/archives/2007/04/a_security_mark.html (letzter Abruf: 05.05.2025)

[2] Debate Security, *Cybersecurity Technology Efficacy: Is cybersecurity the new "market for lemons"?*, Research Report, https://www.debatesecurity.com/downloads/Cybersecurity-Technology-Efficacy-Research-Report-V1.0.pdf (letzter Abruf: 05.05.2025)

[3] Anderson R., *Security Engineering A guide to building dependable distributed systems*, Third Edition, John Wiley&Sons, 2020, https://www.cl.cam.ac.uk/archive/rja14/Papers/SEv3.pdf (letzter Abruf: 14.07.2025)

[4] ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*, Third edition, corrected version, 2022-03

[5] ISO/IEC/IEEE 15288:2023-05, *Systems and software engineering - System life cycle processes*, 2023-05

[6] Barz, B., *Security-Systems Engineering, Ein Ansatz zu den Grundlagen der Informationssicherheit*, Springer Verlag, 2025