Armin Lunkeit
Wolf Zimmer

Security by Design

Security Engineering informationstechnischer Systeme

EBOOK INSIDE

Springer Vieweg

Security by Design

Armin Lunkeit · Wolf Zimmer

Security by Design

Security Engineering informationstechnischer Systeme

Springer Vieweg

Armin Lunkeit
Berlin, Deutschland

Wolf Zimmer
Schildow, Deutschland

ISBN 978-3-662-62916-1 ISBN 978-3-662-62917-8 (eBook)
https://doi.org/10.1007/978-3-662-62917-8

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Planung: Petra Steinmüller
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Dieses Buch verdankt seine Entstehung und Entwicklung der engagierten Unterstützung unserer Familien, Freunden und Kollegen. Unser besonderer Dank gilt unseren Frauen Thea und Monika. Nicht nur, dass sie uns immer wieder bestärkt und den nötigen Freiraum geschaffen haben, den ein solches Buch braucht. Monika hat sich zudem die Mühe gemacht, die Texte immer wieder Korrektur zu lesen. Ihnen und ihrer Geduld vor allem ist dieses Buch gewidmet. Ohne sie würde es diese Buch nicht geben.

Wir danken Prof. Dr. Hartmut Pohl für die zahlreichen fachlichen Anregungen und Hinweise sowie Florian Friedebold für die grafische Beratung und Unterstützung. Viele Abbildungen verdanken wir Florians grafischem Talent und Engagement.

Dankbar sind wir auch dem Springer Verlag, insbesondere Frau Petra Steinmüller und Frau Heike Jung dafür, dass sie dieses Buch ermöglicht haben.

Vorwort

> The trouble with programmers is that you can never tell what a programmer is doing until it's too late.
> – Seymour R. Cray

Die zunehmende Komplexität und Verflechtung informationstechnischer Systeme in den *smart factories*, den *smart cities* und *smart homes* erhöhen die Risiken für die Funktionsfähigkeit politischer, wirtschaftlicher und sozialer Strukturen der modernen Informationsgesellschaft. Selbst geringfügige Fehler können durch die Verkettung unvorhergesehener Abhängigkeiten zu folgenschweren und weitreichenden Ereignissen werden. So geschehen beim Absturz einer Boeing 737 Max am 10. März 2019 über Äthiopien, als die automatische Trimmung durch die Verarbeitung falscher Sensordaten nicht richtig funktionierte. Der wachsende Einsatz der Informationstechnik in nahezu allen Bereichen unserer Arbeits- und Lebenswelten führt daher zwangsläufig zu der Frage, ob und welche Möglichkeiten wir haben, die Sicherheit informationstechnischer Systeme nachhaltig zu erhöhen.

Inhaltlich hat die Vorstellung der Sicherheit von Informationssystemen zwei wesentliche Aspekte: Zuverlässigkeit und Vertrauenswürdigkeit. Der Begriff der Zuverlässigkeit informationstechnischer Systeme beschreibt im Näheren die Eigenschaft eines Systems über einen bestimmten Zeitraum die Dienste korrekt und entsprechend den Benutzererwartungen zu liefern. Vertrauen in ein informationstechnisches System gründet maßgeblich auf der Zuversicht, dass das System bestimmte erwünschte und spezifizierte Eigenschaften besitzt und bei normaler Benutzung über den Zeitraum der Nutzung verfügbar ist sowie sich seiner Bestimmung gemäß verhält. Im sozialen Miteinander erwächst Vertrauen vor allem aus Nähe, persönlicher Erfahrung von Integrität, Kompetenz und Verlässlichkeit oder Reputation. Sämtlich Kategorien, die schwerlich auf informationstechnische Komponenten oder Systeme übertragbar sind. Hier ist der Nutzer angewiesen, auf die Kompetenz, Sorgfalt und Verlässlichkeit von Hard- und Softwareherstellern oder Dienstleistern zu vertrauen, zu denen er weder Nähe noch persönliche Erfahrung herstellen kann.

Sicherheit ist natürlich selten statisch und schon gar nicht schwarz-weiß, Zusammenhänge wichtiger als Technologie, vollständige und umfassende Sicherheit ist bestenfalls nur ein theoretisches Versprechen. Die Vorstellung aber, dass die Sicherheit informationstech-

nischer Systeme etwas Besonderes ist, ist ein Trugschluss. Tatsächlich ist Sicherheit ein Attribut der Zuverlässigkeit. Wir können keine zuverlässigen Anwendungen und Systeme haben, wenn diese nicht sicher sind. Diese Einsicht in der Praxis umzusetzen, ist nur möglich, wenn Sicherheit und Zuverlässigkeit von Beginn an im Design informationstechnischer Systeme zusammengedacht werden.

Motiv und prägender Leitfaden dieses Buches ist darum die Überzeugung, dass die Entwicklung zuverlässiger Systeme immer auch sicherheitsrelevante Fragen berührt, Systems Engineering immer auch Security Engineering ist. Es ist vor allem das Engineering, das die systematische Anwendung modellbasierter Methoden für die Beschreibung der Strukturen und des Verhaltens systemkritischer Bausteine und ihrer Umgebung verlangt. Nur so wird es möglich, den Entwurf von Sicherheitskonzepten und deren Umsetzung transparent, verständlich und damit nachvollziehbar zu machen. Daher richtet sich das Buch an alle, die mit dem Thema direkt oder auch indirekt in Berührung kommen – sei es als Systemarchitekt, Entwickler, Test-Ingenieur, Entscheidungsträger, Betreiber oder auch Anwender.

Selbstverständlich kann ein solches Buch nicht alle Aspekte oder Fragen zu diesem Thema behandeln. Darum haben wir eine Auswahl getroffen, für die wir selbst die Verantwortung tragen. Unser Anspruch ist es auch nicht, eine neue Methode oder ein neues Vorgehensmodell zu entwickeln. Im Mittelpunkt dieses Buches steht vor allem der ingenieurmäßige Zugang zu den Sicherheitsaspekten informationstechnischer Systeme und das nach unserer Auffassung dafür geeignete methodische Rüstzeug. Wir sind der Überzeugung, dass die Entwicklung sicherer und zuverlässiger informationstechnischer Systeme weniger mit Kunsthandwerk zu tun hat, sondern versierte Ingenieure braucht, die in der Lage sind, das gesamte Arsenal moderner Systementwicklung einzusetzen. Der Softwareingenieur von heute muss die mit dem Begriff des Security Engineerings bezeichnete Disziplin der Entwicklung sicherer informationstechnischer Systeme verstehen. Nicht, weil es eine „gute Idee“ ist, sondern weil unsere Arbeits- und Lebenswelten zunehmend auf die Funktionsfähigkeit und die Sicherheit hochkomplexer und dynamischer informationstechnischer Infrastrukturen angewiesen sind. Systems Engineering ist darum immer auch Security Engineering.

Um Missverständnisse zu vermeiden, haben wir uns im Text und in den Abbildungen in den meisten Fällen für die englischen Originalbegriffe entschieden. Das sollte für unsere Leser kein unüberwindliches Hindernis darstellen.

Berlin / Schildow, Januar 2021

Armin Lunkeit
Wolf Zimmer

Inhaltsverzeichnis

Abkürzungen

AES	Advanced Encryption Standard
API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CEM	Common Methodology for Information Technology Security Evaluation
CMVP	Cryptographic Module Validation Program
CPU	Central Processing Unit
CSE	Communications Security Establishment of the Government of Canada
DAC	Discretionary Access Control
DMA	Direct Memory Access
DMZ	Demilitarisierte Zone
DSGVO	Datenschutz Grundverordnung
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange v2
IP	Internet Protocol
IPsec	Internet Protocol Security
LAN	Local Area Network
LDAP	Leightweight Directory Access Protocol
MAC	Mandatory Access Control
NFC	Near Field Communication
NIST	National Institute for Standards and Technology
OWASP	Open Web Application Security Project

PKCS#11	Public Key Cryptography Standard #11
RBAC	Role Based Access Control
RFC	Request for Comment
SAML	Security Assertion Markup Language
SMGW	Smart Meter Gateway
SSH	Secure Shell
ST	Security Target
SysML	System Modeling Language
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UML	Unified Modeling Language

Kapitel 1
Was ist das Problem?

Die digitale Welt ist nicht einfach die alte Welt plus Internetanschluss. Sie ist eine völlig andere. Angetrieben von der Plattformökonomie, sozialen Netzwerken und Industrie 4.0 verwandelt sie die Arbeits- und Lebenswelten der Gesellschaft auf fundamentale Weise. Mehr als die Hälfte der Weltbevölkerung hat heute schon Zugang zum Internet und täglich kommt eine Million neuer Nutzer hinzu [1]. Computer werden in immer mehr Produkte eingebaut, die mit dem Internet verbunden und miteinander vernetzt werden können. Das schwedische Unternehmen Ericsson schätzt, dass im Jahr 2024 weltweit 22,3 Milliarden eindeutig identifizierbare physische Objekte über ihre virtuelle Repräsentation im sogenannten Internet der Dinge verknüpft sein werden [2].

Die wachsende Abhängigkeit unserer Gesellschaft von den Artefakten moderner Informationstechnologien wird begleitet von einer Vielzahl von Bedrohungen des öffentlichen und privaten Lebens, industrieller und gesellschaftlicher Infrastrukturen durch Fehlverhalten, Versehen oder Vorsatz. Internet und Intranet verbinden schon heute nicht nur Menschen und Rechner weltweit, sondern auch Fernseher, Stromzähler und Alarmanlagen, industrielle Sensoren und Steuerungen sowie in wachsendem Maße unzählige andere Geräte, Maschinen und Lebenswelten. Derart komplexe und miteinander verflochtene technische Systeme teilen wenigstens zwei grundlegende Gefahren. Zum einen können selbst geringfügige Fehler durch die Verkettung unvorhergesehener Ereignisse zu folgenschweren und weitreichenden Problemen werden. Zum anderen sind solche komplexen und eng gekoppelten Systeme immer wieder ein reizvolles Ziel von Angreifern aus dem Netz. Vor diesem Hintergrund ist die Entwicklung vertrauenswürdiger und zuverlässiger Informationssysteme von grundlegender Bedeutung für die Funktionsfähigkeit unserer modernen Gesellschaft. Das aber kann nur gelingen, wenn man die Vielfalt und Komplexität der Herausforderungen in einem ganzheitlich analytischem Systemkonzept in den Blick nimmt und in einen methodisch strukturierten und antizipatorischen, den Artefakten der Informationstechnologien adäquaten Handlungsrahmen einbettet, der nach unserer Überzeugung mit dem Begriff des *Security Engineerings* angemessen beschrieben ist. Dies wiederum setzt voraus, dass man sich der Komplexität der Handlungsziele bewusst wird. Darum beginnt dieses Buch auch mit der Beschreibung von Problemstellungen, die im Kontext des Security Engineerings von Bedeutung sind.

A. Lunkeit und W. Zimmer, *Security by Design*,
https://doi.org/10.1007/978-3-662-62917-8_1

1.1 Dimension

Die schon heute kaum mehr vorstellbare Anzahl vernetzter und interagierender physischer und virtueller Agenten lassen die ungeheure Dimension und Komplexität des durch die informationstechnischen Artefakte und Infrastrukturen aufgespannten "Cyber-Raums" nur erahnen. Komplexität aber ist der Feind von Sicherheit und Vertrauen. Und so mischt sich in die Euphorie über die neuen Chancen und Möglichkeiten der digitalisierten Welt auch ein wachsendes Unbehagen hinsichtlich der Gefahren und Risiken durch Versehen oder Vorsatz. Der Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur IT-Sicherheit in Deutschland für das Jahr 2020 lässt keinen Zweifel daran, dass die Gefährdungslage informationstechnischer Systeme, wenn auch in verschiedenen Bereichen der Gesellschaft unterschiedlich ausgeprägt, nach wie vor hoch ist. Dabei sehen sich nicht zuletzt die Betreiber kritischer Infrastrukturen, wie beispielsweise Energieversorger, zusätzlich zu bekannten Angriffsmustern aus dem Internet auch neuen und technisch verfeinerten Angriffen ausgesetzt [3]. Insbesondere die beiden Megatrends „Mobilität“ und „Vernetzung“ haben neue Angriffsflächen enormen Ausmaßes auf essenzielle Bereiche unseres täglichen Lebens mit sich gebracht.[1]

Sicherheitsexperten weltweit sehen sich zunehmend einer immer vielschichtigeren Bedrohungslandschaft gegenüber, die vielen das Gefühl gibt, unzureichend ausgerüstet zu sein, um ihr wirkungsvoll begegnen zu können. Medienwirksame Meldungen über Datendiebstahl und Datenmissbrauch in und von Unternehmen, in öffentlichen Einrichtungen und bei Privatpersonen untergraben stets aufs Neue das Vertrauen in die Sicherheit der Informationstechnik. Nach einer repräsentativen Umfrage im Auftrag des Digitalverbands Bitkom war im Jahr 2018 fast jeder Vierte Onliner vom Missbrauch seiner Daten betroffen [4]. Große Aufmerksamkeit wurde im Jahre 2017 den Cyber-Angriffen durch die Schadsoftware *WannaCry* und *NotPetya* zuteil. Sie haben eindrucksvoll verdeutlicht, dass zahlreiche Organisationen und Unternehmen anfällig für die Risiken und Bedrohungen durch die Digitalisierung sind. Mehr als 200.000 Rechner in 150 Ländern wurden binnen kurzer Zeit von WannaCry infiziert [4]. Die wachsende Komplexität informationstechnischer Systeme

[1] Bereits im Jahr 2013 wurden kritische und leicht auszunutzende Sicherheitslücken in einem Systemregler für das Heizungsgerät ecoPOWER 1.0 der Firma Vaillant gefunden. Dieser Regler unterhält eine Verbindung ins Internet, um Service-Technikern und dem Besitzer der Anlage die Möglichkeit zum Fernzugriff zu geben. Ein Fehler in der Authentisierungsfunktion ermöglichte es Dritten, sich als Besitzer auszugeben und die Temperatur zu regeln (https://www.spiegel.de/netzwelt/gadgets/vaillant-sicherheitsluecke-bedroht-hightech-heizungen-a-894665.html).
Am 08. Dezember 2020 vermeldete der Heise Newsticker, dass im TCP/IP Stack 33 neue Sicherheitslücken entdeckt wurden, die sich auf vier von insgesamt sieben untersuchten TCP/IP-Implementierungen verteilen. Davon betroffen sind vor allem IoT-Geräte, industrielle Steuerungssysteme und Gebäudeautomationssysteme sowie Drucker, Switches und WLAN-Access-Points. Bis auf drei als „Medium“ eingestufte Sicherheitslücken gehe von den übrigen ein hohes Risiko aus. Bei den meisten handele es sich um DoS-Sicherheitslücken, gefolgt von der Gefahr des Datendiebstahls, der unbefugten Codeausführung aus der Ferne (Remote Code Execution) in vier Fällen sowie Cache Poisoning in einem Fall. Die Tatsache, dass es sich bei dem verwundbaren TCP/IP Stack ausnahmslos um (modularen) Open-Source-Code handelt, mache eine Eingrenzung betroffener Produkte und Unternehmen sehr schwierig. Darüber hinaus sei die Eingrenzung zusätzlich dadurch erschwert, dass manchem Geräte- oder Ausrüstungshersteller gar nicht bewusst ist, dass zugekaufte Komponenten von Drittherstellern den verwundbaren Code benutzen (https://www.heise.de/-4982063).

und Infrastrukturen, die ungenügende Sensibilität für Risiken und unzureichende Abwehrmaßnahmen, erhöhen die Chancen für erfolgreiche Cyber-Angriffe. Dabei hat allein im Zeitraum vom 1. Juni 2019 bis 31. Mai 2020 nach Beobachtung des BSI die Anzahl neuer Schadprogramm-Varianten um 117,4 Millionen zugenommen [3].

1.2 Vertrauen

Vertrauen ist vor allem eine soziale Kategorie und im Sinne eines Zutrauens zu eigenen Erwartungen ist Vertrauen ein wesentliches Element in unserem sozialen Alltag. Im Kern ist Vertrauen ein hoffnungsvoller Vorschuss hinsichtlich bestimmter Erwartungen. Der Vertrauensvorschuss gründet in Form und Dimension vor allem auf Erfahrungen und Reputation. Natürlich haben Menschen in vielen Situationen die Wahl, ob sie aus bestimmten Blickwinkeln Personen oder Objekten aus ihrer Umwelt Vertrauen schenken. Ohne jegliches Vertrauen könnten wir weder morgens unser Bett verlassen noch ein bestimmtes Misstrauen formulieren. Denn letzteres würde ja voraussetzen, dass wir in anderen Momenten bereit sind, Vertrauen zu schenken. Das bedeutet, Vertrauen wird erst unter den Bedingungen von Ungewissheit relevant und setzt sich über diese hinweg. Vertrauen ist ein Mittel zur Absorption von Ungewissheit und Komplexität.

In informationstechnischen Umgebungen stützt sich Vertrauen wesentlich auf das Leistungsversprechen von Entwicklern und Herstellern, dass sich das System wie erwartet verhält und die Wirksamkeit der in das System eingebauten Kontrollen eine zuverlässige Funktion garantieren.[2] Der Nutzer hat wenig oder gar keine Möglichkeiten, das System selbst zu kontrollieren. Das ist bei der Komplexität informationstechnischer Artefakte und Systeme auch unrealistisch. Er ist schlicht darauf angewiesen, dem Leistungsversprechen der Entwickler und Hersteller zu vertrauen.

1.3 Komplexität

In der Systemtheorie wird Komplexität mit der Größe und der Vielschichtigkeit von Systemen in Verbindung gebracht. Demnach wächst die Komplexität von Systemen mit der Anzahl seiner Komponenten und der Anzahl möglicher Verbindungen zwischen diesen Komponenten und ihrer Funktionalität. Die Komplexität von Systemen hat daher grundsätzlich zwei Aspekte: eine Struktur und ein Verhalten der Komponenten selbst, wie auch ihrer Verknüpfungen.

Komplexe Struktur bedeutet: das System hat viele oder vielfältige Komponenten, die intensive Wechselbeziehungen aufweisen. Jede Komponente ist mit anderen verknüpft, die Art der Verknüpfungen kann ihrerseits nicht-trivial, bspw. nicht-linear oder scheinbar un-

[2] Nach Lioy und Ramunno [5] gilt ein informationstechnisches System als verlässlich (trusted), wenn es sich wie erwartet, d.h. gemäß seiner Spezifikation und seinem Design verhält. Ein System gilt als vertrauenswürdig (trustworthy), wenn die Übereinstimmung zwischen dem erwarteten und dem tatsächlichen Verhalten auf überzeugende Weise nachgewiesen werden kann.

regelmäßig sein. Komplexes Verhalten bedeutet: das System hat vielfältige, voneinander unterschiedene Reaktionsmöglichkeiten. Obgleich prinzipiell deterministisch kann das System, abhängig vom Input und der Systemumgebung und selbst bei geringfügig veränderten Eingangswerten, verschiedene und ggf. auch unerwartete Reaktionen zeigen. In solchen Fällen droht das System die strikt deterministische Ursache-Wirkungs-Beziehung zu verlassen und lässt sich möglicherweise nur noch mit den Mitteln der Stochastik beschreiben.

Für komplexe Informationssysteme bedeutet Komplexität auch eine Vervielfältigung möglicher Sicherheitslücken (engl. *vulnerability)*[3], die beispielsweise für das Einbringen von Schadprogrammen genutzt werden können oder ein mögliches Fehlverhalten durch Versehen auslösen. Das gilt auch dann, wenn die Gefährdungen für einzelne Systemkomponenten nicht anwachsen. Unter diesen Umständen steigt zudem die Wahrscheinlichkeit einer *Bedrohungskaskade*, das heißt einer Fortpflanzung von Bedrohungen über die Grenzen von Komponenten oder Subsystemen hinweg.

Mit steigendem Vernetzungs- und Verbreitungsgrad informationstechnischer Artefakte muss man davon ausgehen, dass sich nicht nur das Produkt- und Anwendungsportfolio erhöht, sondern auch das Risiko eines erfolgreichen Cyber-Angriffs oder eines technischen Versagens größer wird, verbunden mit einer möglichen Gefährdung der Nutzer. Der Lagebericht des BSI macht darauf aufmerksam, dass unter Laborbedingungen beispielsweise bereits nachgewiesen werden konnte, dass verschiedene medizinische Geräte (Herzschrittmacher, Defibrillatoren, Beatmungsgeräte, Infusionspumpen) nicht sicher vor einem Cyber-Angriff sind. Auch KI-Systeme sind bisweilen ein Sicherheitsrisiko. „Wir haben den Punkt erreicht"“, warnen die KI-Experten Nicholas Papernot und Ian Goodfellow in ihrem Blog cleverhans.io, „bei dem das maschinelle Lernen zwar funktioniert, aber leicht geknackt werden kann. Die meisten Maschinenlernsysteme wurden für ein schwaches Bedrohungsszenario entwickelt, in dem es keine echten Gegner gibt“ [6].

1.4 Struktur des Cyber-Raums

Die ersten Computer waren vereinzelte Maschinen, heute finden wir Computer nahezu überall, eingebettet in physische Objekte wie Kameras, medizinische Geräte oder autonome Fahrzeuge, die drahtgebunden oder drahtlos miteinander kommunizieren und mit der physischen Welt über Bildschirme, Sensoren und Stellglieder oder Antriebe in einer permanen-

[3] Nach der Definition des US-amerikanischen National Instituts of Standards ist eine *vulnerability* „a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source“. Eine *threat source* ist „the intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.“ (siehe bspw. NIST SP 800-30.) In der deutschsprachigen Literatur wird der Begriff der *vulnerability* zumeist synonym für eine *Sicherheitslücke* oder *Schwachstelle* in der Programmierung, der Implementierung oder Konfiguration eines Systems gebraucht, durch die Schadcode in einzelne Rechner oder ganze Systeme eingeschleust werden kann. Aus der Perspektive der IT-Sicherheit ist eine vulnerability (wörtlich übersetzt mit: Verwundbarkeit) eine *potenzielle Sicherheitslücke*, d. h. eine mögliche oder auch nur denkbare Gefährdung oder Beeinträchtigung der Sicherheit eines informationstechnischen Systems, die ihren Ursprung im System selbst oder auch in seiner Umgebung haben und von einem Angreifer ausgenutzt werden kann. Wir verwenden grundsätzlich den Begriff der *Sicherheitslücke*.

ten Rückkopplungsschleife interagieren. Begrifflich unter der Bezeichnung *cyber-physische Systeme* gefasst, bilden sie die konstituierenden Elemente des so genannten Cyber-Raums.

Seine erste wörtliche Erwähnung findet der Cyber-Raum (engl. Cyberspace) 1982 in der Kurzgeschichte „Burning Chrome“ des Science-Fiction-Autors William Gibson. Gibson beschreibt den Cyberspace als Trugbild eines von Computern erzeugten grafischen Raums. Tatsächlich ist er ein abstrakter Raum, seine Elemente – wie in Abbildung 1.1 veranschaulicht – abstrakte Gebilde, implementiert auf physikalischen Objekten. Seine besonderen Merkmale sind Diskretheit und Inhomogenität. Sämtliche informationstechnische Artefakte und Systeme, die dazu dienen, Information zu speichern, zu verarbeiten und zu kommunizieren, können zu möglichen aktiven oder passiven Objekten des Cyber-Raums werden. Sie partizipieren an seiner Funktionalität und interagieren mit anderen Objekten. Cyber-Objekte können reguläre (unabhängige) oder auch Service-Objekte sein. Cyber-Objekte selbst können wieder Unterstrukturen enthalten.

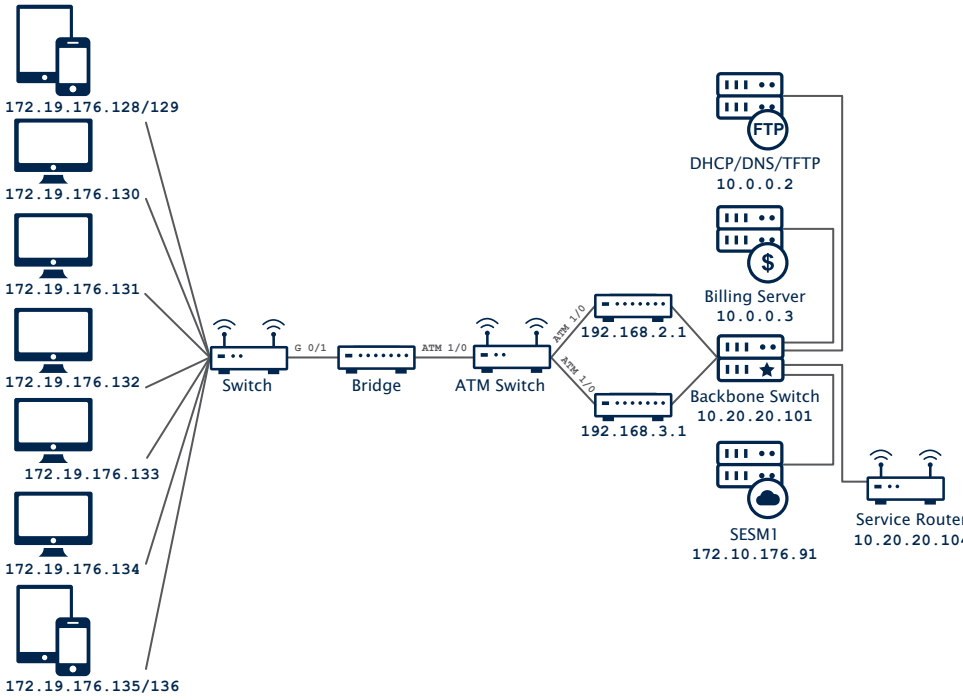

Abb. 1.1: Cyberraum am Beispiel eines Netzwerkes

Objekte im Cyber-Raum haben wie ein Punkt in der Geometrie keine Ausdehnung. Der „Ort“ eines Objektes im Cyber-Raum ist - wie für den Punkt in der analytischen Geometrie - bestimmt durch ein Tupel von „Cyber-Koordinaten“, im einfachsten Fall seine IP-Adresse. Weitere Kandidaten für das Cyber-Koordinatensystem sind beispielsweise die von Programmen oder Diensten genutzten Portnummern, die MAC-Adresse eines Gerätes, eine Telefonnummer, ein Dateiname usw. Im Grunde kann jeder Parameter in einem informations-

technischen System oder einer informationstechnischen Infrastruktur als Cyber-Koordinate dienen.

Die „Identität“ eines Objektes wird durch einen vollständigen Satz seiner Cyber-Koordinaten beschrieben und ist Bedingung für seine „Existenz“ im Cyber-Raum. Allerdings ist die Identität eines Objektes strikt gültig nur in einem bestimmten Kontext und für einen bestimmten Zeitpunkt oder Zeitraum. Überdies kann ein Objekt mehrere Identitäten haben und man kann grundsätzlich das „Original“ nicht von der „Kopie“ unterscheiden. Wenn ein Computer beispielsweise mehrere IP-Adressen hat agiert er im Cyber-Raum als Repräsentant unterschiedlicher Objekte. Die „Identität“ eines Cyber-Objekts ist daher nicht mehr und nicht weniger als die „Position“ im Cyber-Raum, nicht das Objekt selbst. Darüber hinaus ist die „Sichtbarkeit“ eines Cyber-Objektes keineswegs gewährleistet. So kann ein Cyber-Objekt durchaus nur für in einer bestimmten Art und Weise ausgezeichnete Personen oder Geräte „sichtbar“ sein.

Damit Cyber-Objekte miteinander interagieren können, müssen Daten von einem Punkt A zu einem Punkt B transportiert und verarbeitet werden. Daten sind primitive sachbezogene Zeichengruppen, Informationen bedeutungsvoll prozessierte Daten, die Cyber-Objekte Ausgangs- oder Endpunkte oder auch nur Durchgangspunkte von Daten. Im physikalischen Raum versteht man unter einer Distanz einen normierten Betrag für die Entfernung zwischen zwei durch ihre Koordinaten im Raum bestimmten Punkten. Im Cyber-Raum sind Koordinaten Parameter wie die IP-Adresse. In diesem Fall haben Begriffe wie Distanz oder Entfernung keine Bedeutung mehr. Was zählt, ist die Latenz, das heißt die Zeit, die es braucht, um ein Datenpaket von einem Computer A zu einem Computer B zu senden. Die größtmögliche Entfernung auf der Erde beträgt 40.075 km. Die theoretische minimale Latenz beträgt für diese Entfernung etwa 134 Millisekunden. Darüberhinausgehende Verzögerungen haben ihre Ursachen in der physikalischen Infrastruktur des Cyber-Raums. Aber selbst, wenn man in Rechnung stellt, dass ein Cyber-Angriff einen gewissen Zeitraum braucht, um einen Computer zu übernehmen und die nächsten Angriffsschritte auszuführen, muss man davon ausgehen, dass sich ein Angriff weltweit in weniger als 15 Minuten ausbreiten kann [7].

1.5 Asymmetrie der Cyber-Sicherheit

Jede unerwünschte oder auch nur unerwartete Veränderung der Eigenschaften oder des Verhaltens eines Cyber-Objektes ist per se eine Sicherheitsbedrohung. Der Cyber-Raum, seine Objekte und Prozesse sind zwar keine realen Ziele, aber ein Netzwerk für Angriffe oder Versagen, die im physikalischen Raum beginnen und enden. Mit anderen Worten, sämtliche Bedrohungen der Sicherheit und der Zuverlässigkeit des Cyber-Raums haben ihren Ursprung außerhalb des Cyber-Raums. Dies gilt für eine fehlerhafte Kommunikation, Verarbeitung oder Speicherung von Daten ebenso wie für Gefährdungen durch Versehen oder Vorsatz herbeigeführt von Menschen. Das bedeutet aber umgekehrt, auch Sicherheit und Zuverlässigkeit informationstechnischer Systeme und Infrastrukturen haben ihren Ausgangspunkt außerhalb des Cyber-Raums.

Das Schlüsselkonzept für die nachhaltige Abwehr von Bedrohungen der Cyber-Objekte heißt *Security by Design*. Der Grundgedanke richtet den Blick auf die ingenieurmäßige Entwicklung sicherer und zuverlässiger Produkte und Systeme. Die Sicherheit und Zuverlässigkeit informationstechnischer Artefakte und Systeme zu erhöhen beginnt damit, dass Sicherheit bereits in der Konzeption und über alle Schichten informationstechnischer Systeme angelegt und evaluiert wird. Nach wie vor aber wird *Security by Design* zwar immer wieder gefordert, aber viel zu wenig gelebt. Immer wieder streifen Sicherheitsexperten im Nachhinein durch die IT-Systeme auf der Suche nach der berühmten Nadel im Heuhaufen. Denn die Entdeckung von Fehlverhalten wird erschwert durch die Tatsache, dass wir es bei informationstechnischen Systemen in der Regel mit komplexen Strukturen zu tun haben und der Teil des Systems, der nicht erwartungsgemäß funktioniert häufig nie der Teil ist, in dem die Fehlfunktion sichtbar wird. An methodischen Werkzeugen für *Security by Design* auch komplexer Systeme mangelt es nicht, man muss sie nur nutzen und darf den Aufwand nicht scheuen. Sicherheit später dazu zu kaufen, taugt kurzfristig bestenfalls als Geschäftsmodell von Anbietern fokussierter IT-Sicherheitsprodukte. Sicherheit ist primär ein Prozess und kein Produkt.

Informationssysteme arbeiten im weitesten Sinne nach Anweisungen und Regeln. Die Analyse eines beobachteten Fehlverhaltens beginnt daher letztlich mit der Frage, welche Anweisungen und Regeln wie und warum versagt haben. Es ist der Versuch herauszufinden, an welchen Punkten eines informationstechnischen Systems der Zweck einer Anweisung oder einer Regel unzureichend oder missverständlich, in ihrer Formulierung und Anwendung nicht angemessen ausgedrückt oder nicht strikt durchgesetzt wurde. Mit Blick auf den Cyber-Raum handelt es sich dabei vor allem um die Einhaltung von Parameter- und Prozessgrenzen. Die Möglichkeiten der Implementierung und Durchsetzung von Regeln sind natürlich abhängig vom Stand der Technologie. Kommunikationsregeln zum Beispiel werden üblicherweise durch strikte Kommunikationsprotokolle durchgesetzt.

1.6 Technologische Abhängigkeiten

Die technologische Abhängigkeit spiegelt sich am deutlichsten in den Lebenszyklen von Technologien und Produkten. Unternehmen, Regierungen und Milliarden private Nutzer sind auf den Stand der Technik der digitalen Angebote Dritter angewiesen. „Make or Buy“ ist nicht nur für die Betreiber kritischer Infrastrukturen - Verkehr, Energie, Gesundheit, Ernährung, Finanzmärkte oder staatliche Verwaltung - eine ständige Herausforderung. Gemessen an den Vergaberichtlinien der öffentlichen Verwaltung für die Beschaffung von Informationstechnik gewinnt in der Regel der preiswerteste Anbieter, mitunter technologischen oder technischen Defiziten zum Trotz. Zweifellos aber nehmen Fahrlässigkeit und Arglosigkeit einen Spitzenplatz in der Ursachen-Hitparade für die Gefährdung der Sicherheit und Zuverlässigkeit von informationstechnischen Systemen ein. Die Schadsoftware WannaCry nutzte eine Sicherheitslücke im Microsoft Betriebssystem. Aber, obwohl Microsoft schon im März 2017 eine Softwarekorrektur ausgeliefert hatte, scheuten Millionen von Nutzern den Aufwand, ihre Rechner zu aktualisieren.

Die technologische Abhängigkeit ist nirgends so greifbar zu besichtigen wie in der Zukunftswelt von Industrie 4.0. Im Ergebnis des 30 Jahre währenden Feldbus-Krieges müssen sich Anwender mit rund 20 unterschiedlichen Feldbus-Varianten herumschlagen.[4] Aufgrund der langen Nutzungszeit von Anlagen und den darin verbauten Geräten sind bis heute noch Kommunikationsprotokolle und -geräte im Einsatz, bei denen von *Security by Design* noch keine Rede war. Jetzt sollen neue Kommunikationspfade (z. B. über IP-basierte Protokolle und Cloud Computing) die prozessnahe Echtzeitkommunikation der Komponenten im Shop Floor (der Produktion oder Fertigung) mit dem Zugriff auf die Verwaltungs- und Betriebsdaten dieser Komponenten im Office Floor verbinden und auf diese Weise datengetriebene Funktionen wie Condition Monitoring oder Predictive Maintenance erleichtern. Die Kehrseite davon ist ein enormer Zuwachs an Komplexität und Heterogenität des industriellen Internets der Dinge (IIoT) mit allen zu erwartenden Folgen und Erwartungen hinsichtlich der Sicherheit und Zuverlässigkeit der eingesetzten Komponenten und Protokolle. Man braucht sich nur vorzustellen, welche Auswirkungen ein überregionales Versagen oder eine Manipulation der Infrastruktur „intelligenter Stromzähler“ (smart meter) auf die Leistungsbereitstellung von Energieversorgern haben könnte.

„Cloud Readiness“ ist in der Welt der IT von heute zu dem am häufigsten benutzten Schlagwort für eine „überfällige“ Modernisierung von IT-Landschaften geworden, und das obwohl Cloud Computing keine neue Technologie ist, sondern lediglich IT- Ressourcen auf neue Art zur Verfügung stellt. Millionen von Nutzern gebrauchen die Rechnerwolken der Internetriesen um Kosten zu sparen und Rechenkraft hinzuzugewinnen. CIOs und Cloud-Anbieter haben jedoch recht bald lernen müssen, dass das Rechnen in virtuell verteilten und mandantenfähigen Umgebungen eine Änderung unserer Vorstellungen über die Sicherheit digitaler Infrastrukturen erfordert. In dem Maße wie Cloud-Anbieter die Architektur und Topologie ihrer Infrastrukturen mit dem Blick auf mögliche ökonomische Skaleneffekte diversifizieren, wächst auch der durch die zunehmende Komplexität aufgespannte Sicherheitsbereich. Natürlich ist Cloud Computing auch mit einer ganzen Reihe bereits aus der Client-Server-Welt bekannter Bedrohungen konfrontiert. Nicht zu übersehen aber ist, dass Cloud Computing mit der Steuerung virtualisierter und nahezu in Echtzeit dynamisch orchestrierter IT-Ressourcen auch neue Gefahrenpotenziale erzeugt. Die Cloud beherbergt insgesamt mehr Schichten im Rechenstapel (computing stack) und somit auch mehr wahrscheinliche Bedrohungen und Angriffsflächen.

Nicht immer sind technologische Abhängigkeiten so offensichtlich wie für das Cloud Computing. Eine inhärente Eigenschaft komplexer informationstechnischer Systeme ist die Tatsache, dass Bedrohungen und Angriffsflächen erst im Zusammenwirken von Komponenten entstehen können. Der im Dezember des Jahres 2020 bekanntgewordene erfolgreiche Angriff einer Hackergruppe auf ein Update der Netzwerkmonitoring-Software der Firma SolarWinds war, das legen erste Analysen von Sicherheitsexperten nahe [8], nicht allein durch eine Sicherheitslücke in der Software möglich. Der Erfolg des lange Zeit unentdeckten Angriffs wurde erst möglich, nachdem es den Angreifern gelungen war, sich Zugriff auf Signaturzertifikate zu verschaffen, die eigentlich die Authentizität der Softwareaktualisierung bestätigen sollten.

---

4 https://www.elektroniknet.de/design-elektronik/industrial-internet-industrie-4/tsn-schluss-mit-dem-feldbuskrieg-152329.html

1.7 Missverständnisse

So einleuchtend wie begründet die Forderung nach *Security by Design* auch ist, die Realität im Entwurf und der Implementierung informationstechnischer Systeme ist häufig genug eine andere. Vor allem der Wettbewerbsdruck auf Innovationen, raschen Markteintritt und Kosten sorgen dafür, dass im Lebenszyklus von Produkten und Technologien der Funktionalität und dem Markt der Vorrang gegenüber Sicherheit und Zuverlässigkeit eingeräumt wird, proprietäre Mechanismen und Protokolle inklusive. Bis heute beschränkt sich die Herstellung von Sicherheit von Informationssystemen in weiten Teilen auf Schutzfunktionen einzelner Produkte oder Add-on-Technologien wie Anti-Virenprogrammen, deren Nutzung letztlich dem Endkunden überlassen bleibt. Dieser Ansatz funktioniert schon lange nicht mehr, wenn er es überhaupt jemals getan hat. Mit einfach aufgesetzten Sicherheitsinstrumentarien, so lehrt die Erfahrung, können komplexe und weltweit vernetzte Systeme heute nicht mehr geschützt werden.

Der Lagebericht des BSI und das Unbehagen von Sicherheitsexperten weltweit nähren die Befürchtung, dass unsere aktuellen Sicherheits- und Verteidigungsstrategien auf Dauer ungeeignet sind, um den immer komplexeren Bedrohungen gerecht zu werden. Nicht nur, dass sie nahezu ausnahmslos post mortem, also Reaktionen auf bereits ausgeführte Angriffe sind. In der Regel verwenden sie zudem das Instrumentarium mittelalterlicher Stadtbefestigungen. „Brandmauern“ (Firewalls) sollen helfen, Angreifern den Weg zu versperren. Das semantische Meisterstück aber verschleiert den Blick auf die Tatsache, dass die digitalen Brandmauern lediglich darauf spezialisiert sind, nur einen definierten Datenstrom passieren zu lassen. Die Brandmauer ist also nur so gut wie ihre Konfiguration. Einem Angreifer genügt es, zu beobachten, welchen Datenverkehr die Firewall akzeptiert, um sich entsprechend zu „verkleiden“. Intrusion Detection Systeme (IDS) machen da konzeptionell keinen Unterschied. Wir erfahren, dass jemand in unser System eingefallen ist und versuchen herauszufinden, wer der Angreifer ist und was er vorhat. Das Ganze ähnelt einer forensischen Autopsie. Der Patient ist tot und der Pathologe macht sich auf die Suche, was genau den Patienten getötet haben kann. Das mag zwar für Patienten, die noch am Leben sind, möglicherweise hilfreich sein, im Falle einer Pandemie aber ist es ein Kampf auf verlorenem Posten. Eine zusätzliche Erschwernis für Intrusion Detection Systeme ist der Trend, dass die Anwendungen auf unseren Computern immer anspruchsvoller werden und immer ausgeklügeltere Protokolle verwenden. Der Anwender eines Intrusion Detection Systems ist also immer wieder mit der Herausforderung konfrontiert, eine praktikable Balance zwischen falsch-positiven und falsch-negativen Bedrohungswarnungen zu finden.

Die Erkennung von Angriffen basiert in der Regel auf einer syntaktischen und semantischen Datenanalyse. Doch selbst im Erfolgsfall braucht es im Allgemeinen beim „Verteidiger“ deutlich mehr Rechenkapazität, um mögliche Angriffsmuster rechtzeitig zu erkennen, als für den Angreifer die Taktik des Angriffs zu verändern. Etwas verkürzt ausgedrückt: das Verteidigungssystem muss möglichst alle, auch potenzielle Löcher überwachen, dem Angreifer genügt eine Sicherheitslücke. Das aktuelle Zauberwort in diesem Zusammenhang heißt künstliche Intelligenz (KI). Die künstliche Intelligenz soll helfen, Angriffsmuster schneller zu erkennen und Bedrohungen immer einen Schritt voraus zu sein [9]. Für die IT-Beratungsfirma CapGemini ist die künstliche Intelligenz gar die Zukunft der Cyber-Sicherheit. Ian Goodfellow, KI Experte und Mitglied im Google Brain Team hält dagegen,

dass es leicht ist, KI-Systeme zu überlisten. „Nahezu alles Schlechte, was man sich vorstellen kann, dass es von einem maschinellen Lernmodell ausgeführt wird, kann heute getan werden ...“ In den letzten Jahren haben Experten viele Möglichkeiten aufgezeigt, wie maschinelle Lernprogramme manipuliert werden können, indem man ausgerechnet ihre Fähigkeit, Muster in Daten zu erkennen, ausnutzt [10].

Virtuelle Private Netzwerke (VPN) stellen immerhin zwei Sicherheitsfunktionen bereit: den kryptografischen Schutz privater Kommunikationskanäle und die zuverlässige Authentisierung der Kommunikationsteilnehmer. Punkt-zu-Punkt VPNs gelten daher als adäquate Sicherheitsmaßnahmen für die meisten Angriffe. Ausgenommen sind davon freilich Attacken, die mit einer enormen Rechenleistung (beispielsweise mit Hilfe von Botnetzen) ausgeführt werden. Eine weitere Schwachstelle ist die Tatsache, dass der für die Verschlüsselung erforderliche Schlüssel auf dem zu schützenden Computer gespeichert ist. Mit anderen Worten, wenn es gelingt, sich Zugang zu diesem Rechner zu verschaffen, dann wird eine geeignete Schadsoftware auch den Schlüssel finden.

1.8 Nutzer

Ein fundamentales Problem der Sicherheit informationstechnischer Systeme ist der Konflikt zwischen starken Sicherheitsmechanismen und der Nutzerfreundlichkeit. Je vielschichtiger und komplexer die Sicherheitsmechanismen, um so schwieriger und fehleranfälliger sind die Implementierung, die Konfiguration, die Verwaltung, die Wartung und die Nutzung. Nach wie gehört beispielsweise eine schwache Authentisierung durch einfache Passwörter zu den häufigsten Sicherheitslücken. Andererseits schaffen komplizierte Authentisierungsmechanismen wenig Akzeptanz bei den Nutzern. Aus verhaltenspsychologischer Sicht wäre der Idealfall, dass der Zugriff auf Informationssysteme nicht viel schwieriger ist, als wenn es die Sicherheitsmaßnahmen gar nicht gäbe. Ein immer wiederkehrendes Problem menschlicher Faktoren im Ökosystem informationstechnischer Systeme ist deshalb die Auswahl sicherer Passwörter. Einfache Passwörter sind einfach zu merken und ebenso einfach zu entdecken. Zufällig ausgewählte Zeichenkombinationen erhöhen zwar die Sicherheit, zugleich aber auch das Risiko vergessen oder in irgendeiner Weise schriftlich aufbewahrt zu werden. Nutzerfreundlichkeit und Sicherheit sind aber kein unauflösbarer Gegensatz. Der Konflikt muss jedoch schon beim Design informationstechnischer Artefakte und Systeme beachtet werden.

1.9 Analyse-Placebo

Der angemessene Umgang mit Sicherheitsrisiken und Bedrohungen in der Informationstechnik wird nicht zuletzt beeinträchtigt durch eine unzureichende Risikoanalyse und Risikobewertung. Die meisten Organisationen flüchten sich bei der Bewertung von Sicherheitsrisiken in eine Art Punktesystem, das schlussendlich in einer „Risikomatrix“ endet, in der bspw. „Eintrittshäufigkeit“ und „Auswirkungen“ eines potenziellen Sicherheitsvorfalls auf

einer subjektiven Skala von Werten zwischen 1 und 5 beurteilt und gewichtet werden. Als Grund für dieses Analysis-Placebo wird immer wieder aufgeführt: eine quantitative Risikobetrachtung sei sehr aufwändig und setze umfangreiches statistisches Datenmaterial voraus. Darum sei es praktikabler mit qualitativen Kategorien zu arbeiten [11]. Aus der Perspektive des Security Engineerings ist dies jedoch auf Dauer eine unbefriedigende Situation. Insbesondere bei der Bewertung kaskadierender und einander bedingender Bedrohungen helfen Punktesysteme nicht weiter. Selbst für erfahrene Sicherheitsexperten ist es immer wieder eine enorme Herausforderung, aufeinanderfolgende und ursächlich zusammenhängende Risiken in dynamischen Netzwerken klar zu erkennen und zu benennen. Ohne objektive qualitative und quantitative Methoden und Werkzeuge fällt es ihnen schwer, vorbeugende Strategien und Maßnahmen zu entwickeln sowie Entscheidungsprozesse zu begründen, die den Zielkonflikt zwischen Sicherheitsgewinnen und Sicherheitskosten reduzieren helfen.

Der Begriff des Risikos hat mehrere Bedeutungen, eine davon ist die Ungewissheit. Aus Ungewissheit wird ein Risiko, wenn sie sich als Zahlenwert in Form einer Wahrscheinlichkeit oder (statistischen) Häufigkeit auf der Basis empirischer Fakten ausdrücken lässt. Auf die typische Frage eines CEO's nach einem großen Datendiebstahl wie bei Sony oder Facebook: „Kann das auch bei uns passieren?", gibt es daher auch keine vernünftige Antwort. Sinnvoller wäre es zu fragen: Wie groß ist die Wahrscheinlichkeit eines massiven Datendiebstahls in unserem Unternehmen innerhalb der nächsten 12 Monate?

Das methodische Instrumentarium für die Beschreibung und den Umgang mit Ungewissheit liefern die Wahrscheinlichkeitsrechnung und die (schließende) Statistik. Die (schließende) Statistik sucht Antworten auf die Frage, welche Schlussfolgerungen man aus ungewissen Situationen auf der Grundlage vorhandener Daten oder Wissens ziehen kann. Dabei darf man nicht vergessen, die Schlussfolgerungen gelten nicht mit Sicherheit, sondern nur mit „großer Wahrscheinlichkeit" und selbst dies nur, wenn man über die Entstehung der Daten bestimmte, wohldefinierte Annahmen macht. In der schließenden Statistik unterscheidet man zudem die klassische schließende Statistik und die Bayes-Statistik. Beide nutzen das methodische Inventar der Wahrscheinlichkeitsrechnung. Während aber die klassische schließende Statistik sich mit Stichproben aus Datenhaufen begnügt, um Parameter zu schätzen, versucht die Bayes-Statistik zusätzlich in Betracht zu ziehen, was man sonst noch über das Problem weiß. „Die Unterscheidung", begründet der Mathematiker Wolfgang Tschirk, „beruht letztlich auf der unterschiedlichen Meinung darüber, was Wahrscheinlichkeit bedeutet: relative Häufigkeit in zufälligen Ereignissen (klassische Sicht) oder einen Ausdruck des Wissens (Bayes'sche Sicht)"[12]. Natürlich kann man auch in der klassischen Sichtweise Wahrscheinlichkeit als einen Ausdruck von (subjektivem) Meinungen oder Wissen betrachten. Beim Test von Hypothesen aber ist die klassische schließende Statistik darauf beschränkt, zu entscheiden ob eine Stichprobe zur Hypothese passt. Sie kann nicht angeben, wie wahrscheinlich es ist, dass die Hypothese stimmt. Dies ist erst mit der Bayes-Statistik möglich. Instrumente wie die Bayes-Statistik sind daher für eine solide quantitative Risikobeschreibung und Risikobewertung unverzichtbar.

1.10 Murphy's Gesetz

„Anything that can go wrong will go wrong". Die Gründe sind vielfältig. Ein wesentlicher Aspekt ist: der Systembegriff des Systems Engineerings – und das Security Engineering ist ein Teil davon – schließt den Begriff des Modells ein. Der Begriff System beschreibt das Modell einer Ganzheit, die (a) aus einer Menge unterscheidbarer Elemente oder Subsystemen besteht, zwischen denen (b) eine Reihe von Verknüpfungen und funktionalen Beziehungen bestehen und die (c) von ihrer Umgebung oder einem Supersystem abgegrenzt werden kann.

Modelle aber sind – wie in Abbildung 1.2 veranschaulicht – naturgemäß Vereinfachungen; ihre Bewertung und ihre Schlussfolgerungen sind abhängig von der Perspektive der Analyse und den Konzepten, die ihnen zugrunde liegen und den Zielen, die wir ihnen zuschreiben. Kein Modell aber kann die Komplexität der Welt, auch nicht von Ausschnitten, vollständig wiedergeben. Oder wie es so treffend heißt: das beste Modell einer Katze ist immer noch eine Katze. Für die Reduktion von Komplexität ist Vereinfachung aber nicht immer eine gute Lösung. Vereinfachung ist per se unvollständig und birgt die Gefahr der Illusion von Sicherheit. Vereinfachung schafft auch nicht automatisch Klarheit, sondern hinterlässt Ungewissheit.

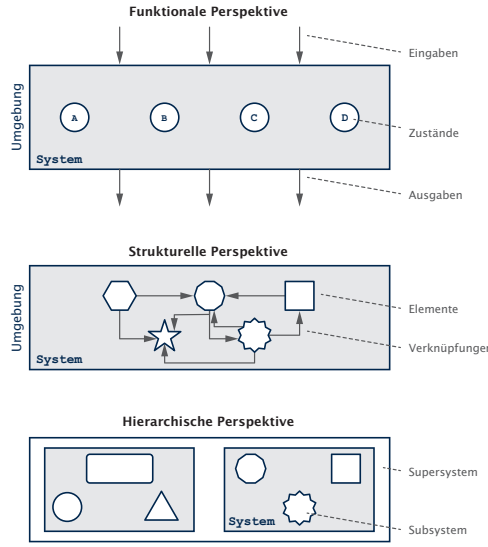

Abb. 1.2: Systemperspektiven

Vor diesem Hintergrund ist das Engineering informationstechnischer Systeme immer eine Gratwanderung in der Abwägung eines Minimums akzeptierbarer Risiken. Es sind vor allem drei Faktoren, die dieses Minimum maßgeblich beeinflussen:

- das Nutzerverhalten,
- unvorhergesehene Ereignisse und
- die Ungewissheiten, die nicht zuletzt dem Modell entwachsen.

Systems Engineering hat das System als Ganzes im Blick. Es schaut ebenso sehr von „außen“ auf das System, das heißt auf seine Wechselwirkungen mit anderen Systemen und seiner Umgebung, wie auch von „innen“ auf Strukturen und Verknüpfungen der Systemelemente. Es ist eben nicht nur mit der „inneren“ Entwicklung des Systems, sondern auch mit externen Faktoren befasst, die in erheblichem Maße die Entwicklung beeinflussen können. Das umfasst die Identifikation von Nutzeranforderungen, die Inbetriebnahme und die Einsatzumgebung, Schnittstellen, logistische Supportanforderungen, die Fähigkeiten des Bedienpersonals usw. usf. Sämtliche dieser Faktoren haben eine operationale, logisch-funktionale und physikalisch-technische Perspektive. Sämtliche dieser Faktoren haben aber auch einen operationalen, logisch-funktionalen und physikalischen Sicherheitshorizont, der die Entwicklung des Systems von der Bedarfsanalyse und Konzeptstudien bis zum Betrieb und Support maßgeblich bestimmt.

Ziel des Systems Engineerings ist die Entwicklung zuverlässiger Systeme. Ein System ist zuverlässig, wenn es in einer beabsichtigten Einsatzumgebung die Aufgaben erfüllt, für die es entwickelt wurde, und keine negativen Auswirkungen hat. Die Zuverlässigkeit eines Computersystems ist die Fähigkeit, Dienstleistungen bereitzustellen, denen man vertrauen kann. Die Zuverlässigkeit eines Computersystems gründet daher auf der Sicherheit, dass das System nur berechtigten Nutzern zur Verfügung steht, die Dienstleistungen die für den beabsichtigten Zweck erforderliche Vertraulichkeit und Integrität wahren, und imstande ist, auf unbeabsichtigte oder absichtsvolle Fehleingaben so zu reagieren, dass negative Auswirkungen verhindert oder zumindest minimiert werden. Die Ingenieursdisziplin, die sich mit dieser Aufgabe befasst, heißt *Security Engineering*. Darum ist Systems Engineering immer auch Security Engineering und Security Engineering immer auch Systems Engineering.

Der Begriff der Zuverlässigkeit für ein bestimmtes System hat natürlich so lange keine nützliche Bedeutung, bis die Aufgaben und die beabsichtigte Umgebung durch eine klare Artikulation der Anforderungen an das System und der Vorstellungen über seine Umwelt deutlich gemacht werden. Informationssicherheit ist daher keinesfalls nur eine technische Herausforderung und Kryptografie auch keine Wunderwaffe, wie Bruce Schneier schon im Jahre 2000 betonte. Nicht weil Kryptografie über die Jahre schwächer geworden wäre, sondern weil die Schwachpunkte nichts mit Mathematik zu tun haben [13]. Nötig ist ein strategischer und multi-disziplinärer kollaborativer Prozess für eine proaktive und ganzheitliche „Sicherheitsvorsorge“, die im Kontext des vorgesehenen Einsatzes eines geplanten Systems und über den gesamten Entwicklungszyklus die Ursachen und Bedingungen für ein Versagen durch Fehlverhalten oder Vorsatz, und unsere Fähigkeiten darauf angemessen zu reagieren, in den Blick nimmt. Die Vorstellung von Sicherheit ist ohne Ziele und Kontext bedeutungslos.

Literaturverzeichnis

1. von Blazekovic J (2019). 2019 werden wir 1,2 Milliarden Jahre online verbringen. Frankfurter Allgemeine Zeitung (FAZ) am 01.02.2019, https://www.faz.net, 2019.
2. Ericsson Mobility Report June 2019, 2019.
3. Die Lage der IT-Sicherheit in Deutschland 2020. https://www.bsi.bund.de/.

4. Alsabah N, Krösmann C (Bitkom e. V. 2019). Jeder zweite Internetnutzer von Cyberkriminalität betroffen. https://www.bitkom.org/.
5. Lioy A, Ramunno G (2010). Trusted Computing. In Stavroulakis P, Stamp M, editor, *Handbook of Information and Communication Security*. Springer Berlin Heidelberg, 2010.
6. Papernot N, Goodfellow I (2016). Breaking things is easy. http://www.cleverhans.io/, 12 2016.
7. Saydjari, O. Sami (2018). *Engineering Trustworthy Systems*. McGraw-Hill, 2018.
8. Pohl H (2021). Der Patch ist der Angriff. https://www.it-daily.net/it-sicherheit/cybercrime/26735-der-patch-ist-der-angriff, Januar 2021.
9. IBM (2019). Künstliche Intelligenz für intelligentere Cybersicherheit. https://www.ibm.com/.
10. Knight W (2016). How Long Before AI Systems Are Hacked in Creative New Ways? - Research points to ways that machine-learning programs could be tricked into doing unwanted things. https://www.technologyreview.com/, 12 2016.
11. Bundesamt für Sicherheit in der Informationstechnik (BSI). BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz.
12. Tschirk W (2014). *Statistik: Klassisch oder Bayes*. Springer Spektrum Berlin Heidelberg, 2014.
13. Schneier B (2004). *Secrets & lies: IT-Sicherheit in einer vernetzten Welt*. dpunkt-Verlag Heidelberg, 2004.

Kapitel 2
Zum Stand der Dinge

Insbesondere zwei Entwicklungen greifen derzeit tief in unsere Arbeits- und Lebenswelten ein: cyber-physische Systeme (CPS) und das Internet-der-Dinge. Ihre Allgegenwart wird nur noch übertroffen von der immensen Kapazität der Datenverarbeitung und der Fähigkeit, autonome Entscheidungen zu treffen. Die Implikationen auf die Sicherheit informationstechnischer Artefakte sind nicht zu übersehen. Die Sicherheitslandschaft ist, wie in Abbildung 2.1 veranschaulicht, umfangreicher und komplexer geworden. Sicherheitsanforderungen können sich zudem in wechselnden Einsatzumgebungen viel rascher ändern.

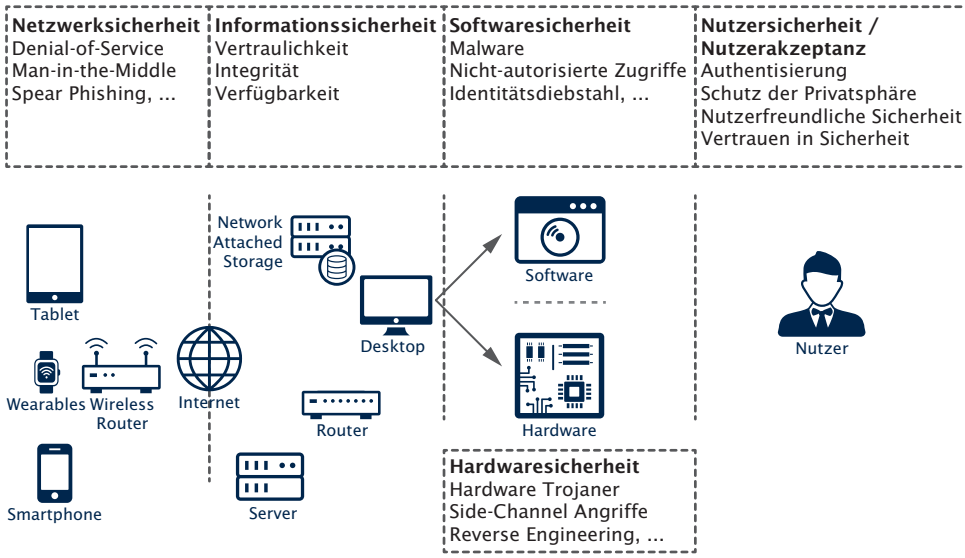

Abb. 2.1: Die Sicherheitslandschaft moderner Computersysteme

Die Kommunikation zwischen Maschinen vergrößert die Bedrohungen durch unsichere Verbindungen und kompromittierte Artefakte. Daraus erwachsen völlig neue Anforderungen an die Zuverlässigkeit, die Vertrauenswürdigkeit und den Schutz informationstechnischer Systeme. Sicherheitseigenschaften unserer Computer, Netze, Smartphones und Mikrocontroller

A. Lunkeit und W. Zimmer, *Security by Design*,
https://doi.org/10.1007/978-3-662-62917-8_2

werden zu Sicherheitseigenschaften von nahezu Allem. Hinzu kommt: die Massenproduktion von Hard- und Softwarekomponenten und deren Nutzung in informationstechnischen Monokulturen erleichtert Angreifern gleichzeitig eine Vielzahl von Systemen weltweit zu attackieren.

Sicherheit ist ebenso wie Vertrauen transitiv. Wir vertrauen auf der Grundlage eigener positiver Erfahrungen oder den Erfahrungen Dritter, von denen wir annehmen dürfen, dass ihr Urteil vertrauenswürdig ist. Dem vermeintlichen Zirkelschluss entkommen wir nur durch Annahmen. In unserem Alltag stellen wir diese Annahmen regelmäßig, ohne das wir uns dessen in jedem Falle bewusst werden, auf die Probe. Nichts davon, so scheint es, ist gewiss, wenn es um die Entwicklung softwareintensiver Produkte geht. Beispielsweise ist die Vorstellung, dass eine kritische Komponente schon deshalb sicher sei, weil sie Kryptografie nutzt, ein gefährlicher Trugschluss. Ken Thompson konnte schon 1984 zeigen, dass es möglich ist einen Trojaner in einem Compiler zu „verstecken“ und so ein Backdoor in jede ausführbare Datei einzubringen, die mit diesem Compiler erzeugt wurde [1]. Der Schutz und die Sicherheit informationstechnischer Artefakte und Systeme ist ein Thema, dass sich, wie aus Abbildung 2.2 ersichtlich, über den gesamten Computing Stack erstreckt und zugleich permanent in einer Art „Technologie-Sandwich“ aus Hardware, Software und Kommunikation bewegt.

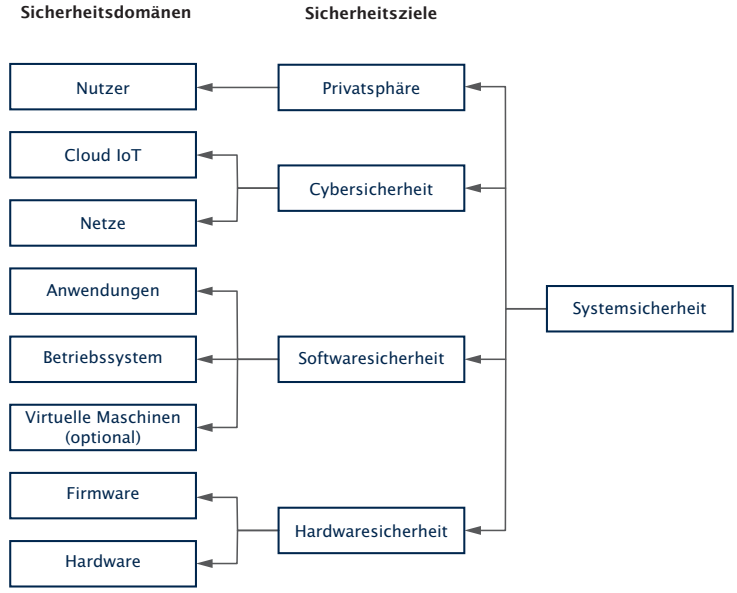

Abb. 2.2: Problemdomänen der IT-Sicherheit

Sicherheit ist ohne Frage leichter zu erreichen, wenn man eine klare Vorstellung davon hat, was geschützt werden soll und warum. Aus der Perspektive der IT-Sicherheit werden die zu schützenden Einheiten eines informationstechnischen Systems (CPUs, Speichermedien, Prozesse, Dateien, Daten und Netzwerkverbindungen) Informationsobjekte (Entitäten) genannt. Die Benutzer eines Systems und alle Einheiten, die im Auftrag von Benutzern tätig

werden können (Prozesse, Anwendungen, Server und Prozeduren), werden als Informationssubjekte (Akteure) bezeichnet. Ein informationstechnisches System hat in der Regel viele Entitäten, die geschützt werden müssen. Jede dieser Entitäten hat einen Namen und eine endliche Menge von Aktionen, die auf dieser Entität ausgeführt werden können. Um den Schutzbedarf informationstechnischer Artefakte und Systeme adäquat beschreiben zu können, führte Jacobs das Konzept der *Sicherheitsdomäne* und des *Sicherheitskontextes* ein [2].

Nach Jacobs ist eine Sicherheitsdomäne ein durch die Komponenten und Eigenschaften eines Systems konstituierter Schutzbereich, in dem das Ziel einer Aktion erwarten kann, dass eine Quelle den relevanten Sicherheitsrichtlinien des Ziels entspricht. Die Perspektive des Begriffs der Sicherheitsdomäne ist die Kontrolle der Interaktion der Systemkomponenten, von denen erwartet wird, dass sie eine Reihe gemeinsamer Sicherheitsbeschränkungen, -anforderungen und -verpflichtungen einhalten.[1]

Etwas vereinfacht ist eine Sicherheits- oder Schutzdomäne D ein logisches Konstrukt für die Vorstellung der Verknüpfung einer Menge zulässiger Aktionen A $(a_1, a_2, \cdots a_n)$ mit einer Menge von Entitäten O $(o_1, o_2, \cdots o_n)$, d. h.

$$D := A \times O := \{(a,o) | a \in A, o \in O\} \tag{2.1}$$

Im einfachsten Fall ist die Sicherheitsdomäne eine Menge von (Objekt, Rechte)-Paaren. Jedes Paar spezifiziert ein Objekt und eine (Teil-)Menge von Operationen, die auf dieses Objekt ausgeführt werden dürfen. Oft entspricht eine solche Domäne einem einzelnen Benutzer oder Akteur und gibt an, was ein Benutzer oder Akteur tun darf oder nicht.

Der Sicherheitskontext umfasst nach Jacobs alle Ressourcen und Sicherheitsmechanismen, welche die Ausführung eines Prozesses in einer Sicherheitsdomäne unterstützen und beeinflussen. Der Sicherheitskontext wird bspw. durch eine Reihe von Daten und Programmen definiert, die gemäß einer Sicherheitsdomänenrichtlinie in einem informationstechnischen System ausgeführt werden.

Ausgerüstet mit diesen Vorstellungen kann man sagen: ein Informationssystem kann dann als sicher gelten, wenn es ausschließlich die seinem beabsichtigten Zweck entsprechenden und als zulässig spezifizierten Aktionen ausführt, ohne relevante Verknüpfungen von Aktionen mit Objekten zu verletzen oder zu gefährden. Es sei also für ein Informationssystem S_E in einer Umgebung E

> $R = \{R_a\}$ die Menge aller Spezifikationen der erwünschten Aktionen $\{a_1, \cdots a_n\}$ und $F = \{F_T\}$ die Menge der aus einem Bedrohungsmodell T abgeleiteten unerwünschten Aktionen.

Dann kann man mit einer gewissen Berechtigung sagen: ein System implementiert die spezifizierten Aktionen R_a sicher, wenn

- sämtliche Spezifikationen R_a in der Kombination aus S_E und E korrekt erfüllt werden, und

[1] Jacobs nimmt dabei Bezug auf die Definition der ITU-T Recommendations X.800 - Security Architecture for Open Systems Interconnection for CCITT Applications (Abschnitt 8.1.2) aus dem Jahre 1991: „Entities that are subject to a single security policy, administered by a single authority, are sometimes collected into what has been called a ‚security domain'"