

Mark Bedner, Tobias Ackermann

Schutzziele der IT-Sicherheit

IT-Sicherheit hat den Schutz von elektronisch gespeicherten Informationen und deren Verarbeitung als Ziel. Abzusichernde Eigenschaften und Zustände dieser Informationen und Systeme werden in Form von Schutzzielen der IT-Sicherheit beschrieben.

Einleitung

Zielsetzung dieses Aufsatzes ist eine Sammlung, Beschreibung und Systematisierung der derzeit bekannten und anerkannten Schutzziele der IT-Sicherheit. Zur besseren Vergleichbarkeit werden jeweils auch die entsprechenden englischen Begriffe der Schutzziele genannt. Zusätzlich erfolgt eine Nennung geläufiger Maßnahmen, die eingesetzt werden, um die Ziele zu erreichen.

Auch für die rechtliche Betrachtung ist die nachfolgende Begriffsbeschreibung nötig, da beispielsweise § 2 Abs. 2 BSI-Gesetz¹ zwar eine Legaldefinition für „Sicherheit in der Informationstechnik“ formuliert und in diesem Zusammenhang

die Verfügbarkeit, die Unversehrtheit und die Vertraulichkeit von Informationen erwähnt, es jedoch vermeidet, die Begriffe ihrerseits näher zu beschreiben.

Historie

Die Informationssicherheit ist ein hochdynamisches Handlungsfeld, das der technischen Entwicklung folgt. Die verschiedenen Schutzziele haben sich parallel dazu im Laufe der Zeit entwickelt. Vor zwanzig Jahren wurde Sicherheit nahezu mit Vertraulichkeit gleichgesetzt. Vor fünfzehn Jahren wurden Integrität der Information und Verfügbarkeit der Funktionalität hinzugefügt und vor zehn Jahren kam die Zurechenbarkeit als viertes Schutzziel hinzu.² Heutzutage sind zahlreiche weitere Schutzziele, wie etwa Authentizität, Verdecktheit, Nachweisbarkeit, Verlässlichkeit und Anonymität anerkannt. Alle diese zusätzlichen Ziele wurden bisher jeweils unter einen der drei Oberbegriffe Vertraulichkeit, Integrität oder Verfügbarkeit eingeordnet (sogenannte „CIA-Triad“³). Beispielsweise sind Verdecktheit, Anonymität und Unbeobachtbarkeit Vertraulichkeitseigenschaften.⁴

Seit dem Jahr 2009 kann man auch die „Kontingenz“ zu den Oberbegriffen hinzuzählen.⁵ Während Verfügbarkeit und Vertraulichkeit „dual“ zueinander stehen, soll die Kontingenz das „Dual“ zur Integrität sein.⁶ Außerdem wird das Datenschutz-Schutzziel „Transparenz“ in den Kreis der untergeordneten IT-Schutzziele aufgenommen und als Pendant zur Unverkettbarkeit angesehen.⁷ Konsequenz ist es

jedoch die Transparenz und die Vertraulichkeit gegenüberzustellen und die Transparenz als fünftes übergeordnetes IT-Schutzziel aufzuwerten.

Im Folgenden sollen die einzelnen über- und untergeordneten Schutzziele näher erläutert werden.

Vertraulichkeit (confidentiality)

Informationsvertraulichkeit ist bei einem IT-System gewährleistet, wenn die darin enthaltenen Informationen nur Befugten zugänglich sind.⁸ Dies bedeutet, dass die sicherheitsrelevanten Elemente nur einem definierten Personenkreis bekannt werden.⁹ Dazu sind Maßnahmen zur Festlegung sowie zur Kontrolle zulässiger Informationsflüsse zwischen den Subjekten des Systems nötig (Zugriffsschutz und Zugriffsrechte), sodass ausgeschlossen werden kann, dass Informationen zu unautorisierten Subjekten „durchsickern“.¹⁰ Zu den Schutzobjekten der Vertraulichkeit gehören unter anderem die gespeicherten oder transportierten Nachrichteninhalte, die näheren Informationen über den Kommunikationsvorgang sowie die Daten über den Sende- und Empfangsvorgang.¹¹ Andere unterscheiden zwei Bereiche, nämlich den „Schutz des Informationsverhaltens“,¹² also den Schutz des Benutzers vor Beobachtung, Aufzeichnung und Auswertung seines Verhaltens während der



**Mark Bedner,
LL.M.**

Ass. iur., Mitarbeiter in der „Projektgruppe verfassungsrechtliche Technikgestaltung (provet)“ und Stipendiat des CASED (Center for Advanced Security Research Darmstadt).

E-Mail: markbedner@uni-kassel.de



**Dipl.-Wirtsch.-
Inform. Tobias
Ackermann**

Wissenschaftlicher Mitarbeiter am Fachgebiet

Information Systems / Wirtschaftsinformatik an der TU Darmstadt und Stipendiat der CASED (Center for Advanced Security Research Darmstadt) Graduiertenschule.

E-Mail: tobias.ackermann@cased.de

¹ Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz).

² Siehe hierzu *Roßnagel/Pfützmann/Garstka*, Modernisierung des Datenschutzrechts, 2001, 229.

³ Confidentiality, Integrity, Availability (CIA).

⁴ *Federrath/Pfützmann*, IT-Sicherheit, in: Martin Wind, Detlef Kröger, Handbuch IT in der Verwaltung, 2006, 274.

⁵ *Rost/Pfützmann*, DuD 2009, 353.

⁶ *Rost/Pfützmann*, DuD 2009, 353.

⁷ *Rost/Pfützmann*, DuD 2009, 354 f.

⁸ *Holznapel*, Recht der IT-Sicherheit, 2003, 13.

⁹ *Stelzer*, Sicherheitsstrategien in der Informationsverarbeitung, 1993, 35.

¹⁰ *Eckert*, IT-Sicherheit, Konzepte, Verfahren, Protokolle, 4. Auflage 2006, 9.

¹¹ *Holznapel* (Fn. 8), 13 f.

¹² *Grochla/Weber/Albers/Werhahn*, Ein betriebliches Informationsschutzsystem, Notwendigkeit und Ansatzpunkt für eine Neuorientierung, Angewandte Informatik, 189.

Nutzung eines IT-Systems und den „Schutz der Informationsinhalte“.¹³

Das zentrale Instrument zur Gewährleistung der Vertraulichkeit ist, neben einem wirksamen Zugriffsschutz, die Verschlüsselung von Daten.¹⁴ Das Ziel der Verschlüsselung liegt darin, die Daten geeignet zu transformieren, sodass unautorisierte Dritte ohne den korrekten Schlüssel nicht in der Lage sind, die Daten sinnvoll zu interpretieren.¹⁵ Die Verschlüsselung kann symmetrisch oder asymmetrisch erfolgen.¹⁶

Im Gegensatz zu den meisten anderen IT-Schutzzielen ist der Schutz der Vertraulichkeit von Daten und Informationen rechtlich vergleichsweise gut abgesichert. Regelungen zum Schutz der Vertraulichkeit finden sich in Art. 10 GG und einfachgesetzlich in § 88 TKG und § 206 StGB, soweit das Fernmeldegeheimnis betroffen ist. Datenschutzrechtlich sind insbesondere § 5 BDSG (Verpflichtung der Mitarbeiter auf das Datengeheimnis) und die technisch-organisatorischen Maßnahmen in der Anlage zu § 9 BDSG, insbesondere die Nummern 1 bis 3 (Zutritts-, Zugangs- und Zugriffskontrolle), erwähnenswert. Zum Schutz von Privat- oder Betriebsgeheimnissen sind § 203 StGB und § 17 UWG einschlägig.

Unverkettbarkeit (unlinkability)

Unverkettbarkeit¹⁷ soll gewährleisten, dass mehrere kommunikative Ereignisse, etwa aufeinander folgende Abrufe von Informationen auf verschiedenen Webservern im Internet, nicht miteinander in Verbindung gebracht werden können.¹⁸ Allgemeiner formuliert bedeutet die Unverkettbarkeit von Subjekten, Objekten oder Aktionen, dass durch Beobachtungen des Szenarios die Wahrscheinlichkeit einer Relation zwischen enthaltenen Elementen unverändert bleibt.¹⁹

Eine Maßnahme zur Gewährleistung der Unverkettbarkeit ist die Nutzung von sogenannten „Mischen“, das heißt Servern,

die die einzelne Zuordnung eines Datenpakets zu einem Nutzer verschleiern, indem Nachrichten nicht direkt vom Sender zum Empfänger, sondern über mehrere Zwischenstationen (eben diese „Mix“-Server) übertragen und untereinander verwürfelt werden.²⁰ Begründer dieses Konzepts war der Informatiker und Ökonom David Chaum²¹ im Jahr 1981.²²

Zu beachten ist, dass auch der Gegenbegriff, nämlich die Verkettbarkeit, im Zusammenhang mit der Zurechenbarkeit als Ziel angesehen werden kann.

Nicht-Verfolgbarkeit (untraceability)

Eng mit der Unverkettbarkeit und der Zurechenbarkeit zusammenhängend ist die Nicht-Verfolgbarkeit, auch als Unverfolgbarkeit oder Nicht-Rückverfolgbarkeit bekannt. Im Unterschied zur Unverkettbarkeit, die allgemein auf die fehlende Möglichkeit der Relation von Subjekten, Objekten oder Aktionen abstellt, meint Nicht-Verfolgbarkeit die Unmöglichkeit Handlungen oder Kommunikationsinhalte einer ganz bestimmten identifizierbaren Person nachverfolgen zu können.

Ein Beispiel für die Umsetzung von Anonymität durch Nicht-Verfolgbarkeit ist die Abwicklung von E-Commerce-Geschäften mittels des digitalen Zahlungsverkehrs. Ist dieser entsprechend ausgestaltet, beispielsweise bei der Geldkarte, können Teilnehmer in einer computerisierten Umgebung genauso agieren wie bei herkömmlichen Bargeschäften des täglichen Lebens. Sie bezahlen mit digitalem Geld, ohne ihre Identität offenbaren zu müssen,²³ da die Zahlungsströme nicht mehr nachträglich einzelnen identifizierbaren Personen zugeordnet werden können.

Unbeobachtbarkeit (unobservability)

Die Unbeobachtbarkeit ist gewährleistet, wenn sich nicht erkennen lässt, wer Daten sendet oder empfängt,²⁴ aber auch wenn

der oben erwähnte Schutz des Informationsverhaltens gewährleistet ist. Dritte können weder die Nutzung der (Kommunikations)systeme noch das eigentliche Senden und Empfangen von Nachrichten beobachten. Das Problem an Letzterem ist, dass in den bestehenden Netzen die Ereignisse des Sendens oder Empfangens eines Datenpaketes stets beobachtbar sind. Allerdings kann durch das Generieren von „Dummy Traffic“ ein Angreifer daraus keinen Nutzen ziehen. „Dummy Traffic“ bedeutet, dass ein Nutzer Lernnachrichten, die für einen Beobachter von außen nicht von echten Botschaften zu unterscheiden sind, sendet, solange er keine echten Nachrichten zu senden hat.²⁵ Damit wären zumindest das Senden und der Erhalt von einzelnen konkreten Nachrichten verheimlicht. Um die eigentliche Dienstenutzung an sich durch einen bestimmten Nutzer unbeobachtbar zu gestalten, bietet sich das oben dargestellte Mix-Verfahren an, das mehrere Beteiligte beinhaltet, sodass aufgrund der verwendeten Verwürfelungsmethoden nicht auf einen einzelnen Nutzer geschlossen werden kann.

Soweit das Schutzziel die Unbeobachtbarkeit der Nutzung von Systemen betrifft, beispielsweise durch heimliches Beobachten oder Abhören des Nutzers mittels Kameras, Mikrofonen oder Auffangen von elektromagnetischer Abstrahlung, so sind die Maßnahmen der optischen und elektromagnetischen Abschirmung, zum Beispiel fensterlose und als Faradayscher Käfig ausgestaltete Räume und die Überprüfung dieser Räume auf „Wanzen“ in Betracht zu ziehen.

Verdecktheit (covertness, obscurity)

Während bei der Unbeobachtbarkeit klar ist, dass irgendwann eine Datenübertragung stattfindet, diese jedoch hinsichtlich der Sender und Empfänger, des genauen Zeitpunkts und des Inhalts für Angreifer nicht auszumachen ist, geht die Verdecktheit einen Schritt weiter. Diese bedeutet, dass niemand außer den Kommunikationspartnern überhaupt weiß, dass Kommunikation stattfindet. Steganographie, also das Verstecken von Informationen im Datenrauschen von Bild- oder Musikdateien, ist ein Beispiel für eine reale Anwendung.

13 Grochla/Weber/Albers/Werhahn (Fn. 12), 192.

14 Witt, IT-Sicherheit kompakt und verständlich, 2006, 67; Eckert, 2006, 9.

15 Eckert (Fn. 10), 9.

16 Witt (Fn. 14), 67.

17 Auch als „Unverknüpfbarkeit“ bekannt.

18 <http://www.weka.de/datenschutz/4742978-Unverkettbarkeit.html>.

19 Stritter, MozPEts-PeMar. Entwicklung eines Gateways zum anonymen E-Mailversand über Remailer-Netzwerke und Anbindung von Mozilla Mail, 2006, 11.

20 Siehe <http://anon.inf.tu-dresden.de/JAP-TechBgPaper.pdf> für eine genauere Beschreibung; Holznagel, 2003, 31.

21 Chaum, Communications of the ACM, 1981, 84.

22 Danz/Federrath/Köhntopp/Kritzenberger/Ruhl, Anonymer und unbeobachtbarer Webzugriff für die Praxis, in: IT-Sicherheit ohne Grenzen? Tagungsband 6. Deutscher IT-Sicherheitskongress des BSI 1999, 60 f.

23 Biskup, Security in Computing Systems – Challenges, Approaches and Solutions, 2009, 44.

24 Roßnagel/Pfutzmann/Garstka (Fn. 2), 230; Biskup (Fn. 23), 43.

25 Danz/Federrath/Köhntopp/Kritzenberger/Ruhl (Fn. 22), 60.

Anonymität (anonymity)

Anonymität meint den Schutz vor Identifizierung.²⁶ Sie ist Folge der Unverkettbarkeit. Demgemäß werden auch Dienste, die die Verkettbarkeit unterbrechen als Anonymisierungsdienste bezeichnet.

Rechtlich erlangt die Anonymität im Rahmen des Datenschutzrechts Bedeutung. In § 3 Abs. 6 BDSG wird der Vorgang des Anonymisierens definiert: „Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmaren natürlichen Person zugeordnet werden können.“ Hauptziel ist also die Kappung der Zuordnung von Daten zu bestimmten Personen, sprich deren Identifizierung erheblich zu erschweren oder gänzlich unmöglich zu machen.

Pseudonymität (pseudonymity)

Pseudonymität bedeutet Schutz vor namentlicher Identifizierung. Die datenschutzrechtliche Maßnahme der Pseudonymisierung ist beispielsweise in § 3 Abs. 6a BDSG geregelt und meint „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren“. Im Gegensatz zur Anonymisierung wird bei der Pseudonymisierung der Bezug zu einer bestimmten Person jedoch nicht endgültig aufgehoben, denn es besteht immer eine Aufdeckungsmöglichkeit. Durch eine Zuordnungsregel kann das Pseudonym nachträglich wieder dieser bestimmten Person zugeordnet werden. Derjenige, der die Zuordnungsregel kennt, kann Pseudonyme mit realen Personen verketteten, diese Personen wiedererkennen und soweit nötig zur Verantwortung ziehen. Pseudonymität ist folglich ein Kompromiss aus Vertraulichkeit und Transparenz. Wenn die Zuordnungsregel verloren geht oder bewusst vernichtet wird, dann entsteht Anonymität im obigen Sinne.

Anonymisierung und Pseudonymisierung sind für die Prinzipien der Datenvermeidung und Datensparsamkeit von erheblicher Bedeutung. Gemäß § 3a Satz 2

BDSG sollen personenbezogene Daten, soweit der Verwendungszweck dies erlaubt und keinen unverhältnismäßigen Aufwand darstellt, anonymisiert oder pseudonymisiert werden.

Transparenz (transparency)

Transparenz ist das Gegenstück zur Vertraulichkeit und somit ein übergeordnetes IT-Schutzziel. Im Gegensatz zur Computer- und Netzwerktechnik, in der ein transparenter Teil eines Systems nicht wahrgenommen werden soll, hat Transparenz im Kontext der Schutzziele die entgegengesetzte Bedeutung. Analog zum datenschutzrechtlichen und politischen Verständnis bedeutet Transparenz Klarheit, Erkennbarkeit und Nachverfolgbarkeit.²⁷ Systeme und ihr technischer Aufbau sollen – soweit wie möglich – durchschaubar und ihre Funktions- und Arbeitsweise nachvollziehbar und verständlich sein (Gegenteil einer „Blackbox“). Die darin verarbeiteten Daten und insbesondere die beteiligten Personen und deren Handlungen sollen erkennbar sein.

Einige der Transparenz untergeordneten Schutzziele lassen sich als Gegenbegriffe der Vertraulichkeitsschutzziele bezeichnen. So kann es erwünscht oder nötig sein, dass Handlungen verkettbar und nachverfolgbar sind oder Kommunikation beobachtbar und unverdeckt erfolgt.

Maßnahmen zur Gewährleistung von Systemtransparenz sind Audits, Code Review oder die Nutzung von Open Source Software. Nutzungstransparenz wird beispielsweise durch die Authentisierung von Personen oder die Protokollierung von Ereignissen unter Verwendung von digitalen Signaturen und Zeitstempeln sichergestellt.

Zurechenbarkeit (accountability)

Die Zurechenbarkeit hat Bezüge zur Transparenz, Authentizität, Integrität und Nicht-Verfolgbarkeit. Sie wird auch als Nachweisbarkeit (detectability), Unleugbarkeit oder Nicht-Abstreitbarkeit (non-repudiation) bezeichnet. Sie hatte ursprünglich nur für Kommunikationsbeziehungen Bedeutung und meinte, dass Sendern und Empfängern von Informationen das Senden und der Empfang der Informationen nachgewiesen werden kön-

nen.²⁸ Im Umkehrschluss sollen die Beteiligten ihre jeweilige Beteiligung nicht abstreiten können und somit das Gegenüber geschützt werden. Die Nachweisbarkeit der Identität des Absenders schützt den Empfänger davor, dass der Absender den Versand der Nachricht abstreitet, wohingegen die Nachweisbarkeit des Versendens den Absender davor schützt, dass der Versand der Nachricht bestritten wird (Nicht-Abstreitbarkeit der Herkunft). Die Nachweisbarkeit der Zustellung und des Empfangs schützt den Absender und den Empfänger davor, dass die Zustellung oder der Empfang bestritten werden können (Nicht-Abstreitbarkeit des Versands oder des Erhalts).²⁹

Mittlerweile wurde die Definition allgemein um Handlungen und Transaktionen erweitert. Zurechenbarkeit bezeichnet demnach den Umstand, dass Aktionen oder Dokumente den urhebenden Personen oder Institutionen (Veranlassern) zugeordnet werden können.³⁰ Es muss bei jeder in einem IT-System ausgeführten Aktion (Vorgang, Prozess) während ihres Ablaufs und danach feststellbar sein, welcher Instanz – insbesondere welcher Person – eine Aktion zuzuordnen ist, welches Subjekt sie ausgelöst und wer sie letztlich zu verantworten hat.³¹ Zurechenbarkeit ist somit das Gegenstück der Nicht-Verfolgbarkeit angereichert um den Aspekt der Verantwortlichkeit.

Maßnahmen zur Gewährleistung der Zurechenbarkeit sind, wie bei der Transparenz allgemein, die Protokollierung und der Einsatz von digitalen Signaturen und Zeitstempeln.

Authentizität (authenticity)

Authentizität³² ist gewährleistet, wenn durch geeignete Kontrollmaßnahmen sichergestellt wird, dass Daten und Informationen wirklich aus der angegebenen

²⁸ Roßnagel/Pfützmann/Garstka (Fn. 2), 230; Biskup (Fn. 23), 42.

²⁹ <http://www.demonium.de/th/home/sicherheit/grundlagen/sachziele.phtml#nachweisbarkeit>.

³⁰ Muntermann/Roßnagel, H./Rannenber, Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen, in: Jan von Knop, Wilhelm Haverkamp, Eike Jessen: E-Science und GRID, Ad-hoc-Netze und Medienintegration; Proceedings der 18. DFN-Arbeitstagung über Kommunikationsnetze; Juni 2007, 11.

³¹ Dierstein, Sicherheit in der Informationstechnik – der Begriff IT-Sicherheit, Informatik Spektrum, 2004, 349.

³² Auch als „Echtheit“ bezeichnet.

²⁶ Biskup (Fn. 23), 44.

²⁷ Ähnlich Rost/Pfützmann, DuD 2009, 355.

Quelle stammen und dass die Identität eines Benutzers oder eines angeschlossenen Systems korrekt ist. Im Rahmen einer Kommunikationsbeziehung muss außerdem sichergestellt sein, dass diese Identität über die Dauer einer Kommunikationsbeziehung erhalten bleibt.³³ Die Identifikation eines Benutzers basiert auf der Vergabe von eindeutigen Benutzerkennungen. Charakterisierende Eigenschaften zum Nachweis der Identität (Authentisierung) sind beispielsweise Passwörter, deren Kenntnis der Benutzer beim Systemzugang nachweisen muss, oder biometrische Merkmale, zum Beispiel Fingerabdrücke.³⁴ Auch der Besitz von Chip- oder Magnetstreifenkarten gehört dazu.³⁵ Identitätsnachweise werden häufig allgemein als „Credentials“ bezeichnet.³⁶

Zur Abgrenzung der Begriffe „Authentifizierung“, „Authentisierung“ und „Autorisierung“: Durch eine erfolgreiche Authentisierung identifiziert sich ein Benutzer oder ein System an einem anderen System. Benutzer oder anfragendes System werden bei erfolgreichem Abgleich der Credentials vom angefragten System authentifiziert. Bei der Autorisierung erhalten Nutzer meist aufgrund ihrer Zugehörigkeit zu festgelegten Gruppen oder Rollen bestimmte Rechte im IT-System zugewiesen.

Revisionsfähigkeit (reviewability)

Revisionsfähigkeit bedeutet Nachprüfbarkeit und Nachvollziehbarkeit und wird durch Protokollierung und Dokumentation von Handlungen gewährleistet und lässt sich demzufolge als Unterfall der Transparenz einordnen.³⁷ In der Literatur wird die Revisionsfähigkeit als „Eigenschaft eines Systems, die Funktionsweise lückenlos nachzuvollziehen und damit feststellen zu können, wer, wann, welche Daten in welcher Weise verarbeitet hat (Prüfende Wiederdurchsicht)“ beschrieben.³⁸

Nach den Verwaltungsvorschriften zum Gesetz zum Schutz personenbezogener Daten der Bürger in Sachsen-Anhalt sind Daten revisionsfähig, „wenn nachprüfbar ist, wie sie in einen Datenbestand gelangt sind und welche Veränderungen

sie im Laufe der Zeit erfahren haben. Nachprüfbar muss sein, wer für das Aufnehmen bestimmter Daten in einen Datenbestand oder ihr Entfernen daraus die Verantwortung trägt“.³⁹ In § 9 Abs. 1 Nr. 4 RefiRegV⁴⁰ wird die Revisionsfähigkeit damit umschrieben, dass „sämtliche Zugriffe (Eingeben, Lesen, Kopieren, Ändern, Löschen, Sperren) auf ein Datenverarbeitungssystem revisionssicher protokolliert werden“.

Die Begriffe Zurechenbarkeit und Revisionsfähigkeit sind nicht vollkommen trennscharf voneinander, jedoch kann man eine grobe Abgrenzung dahingehend vornehmen, dass Zurechenbarkeit überwiegend Personen und deren Handlungen zum aktuellen Zeitpunkt und nachträglich betrifft, während Revisionsfähigkeit eher auf das System abstellt und nur die nachträgliche, auf die Vergangenheit bezogene, Möglichkeit der Überprüfbarkeit meint. Oft ist es so, dass durch diese Überprüfungsmöglichkeit, also vorwiegend durch Protokollierung, auch gleichzeitig eine Zurechenbarkeit von Handlungen zu Personen ermöglicht wird.

Verfügbarkeit (availability)

Die Verfügbarkeit betrifft sowohl informationstechnische Systeme als auch die darin verarbeiteten Daten und bedeutet, dass die Systeme jederzeit betriebsbereit sind und auf die Daten wie vorgesehen zugegriffen werden kann.⁴¹ Zum einen muss die Datenverarbeitung inhaltlich korrekt sein und zum anderen müssen alle Informationen und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden.⁴²

Im Geschäftsleben wird die Verfügbarkeit eines Systems oder Dienstes als das Verhältnis der Zeit innerhalb eines vereinbarten Zeitraums, in der das System tatsächlich zur Verfügung stand (sogenannte Betriebszeit oder „operation time“) zu der gesamten vereinbarten Zeit verstanden. Dieses Verhältnis wird üblicherweise in Prozent angegeben. Idealzustand sind

100 Prozent, also die jederzeitige Verfügbarkeit. Dieses Verhältnis hat Auswirkungen bei der Vereinbarung von Service-Level-Agreements und darin eventuell festgelegten Strafzahlungen im Fall von Vertragsverstößen. Der Zeitraum ohne Verfügbarkeit des Systems wird als Ausfallzeit (downtime) bezeichnet. Eine Maßnahme zur Erhöhung der Verfügbarkeit ist der Einsatz redundanter Systeme.

Integrität (integrity)

Integrität oder Unversehrtheit⁴³ bedeutet zweierlei, nämlich die Vollständigkeit und Korrektheit der Daten (Datenintegrität) und die korrekte Funktionsweise des Systems (Systemintegrität).⁴⁴ Vollständig bedeutet, dass alle Teile der Information verfügbar sind. Korrekt sind Daten, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben.⁴⁵ Die Integrität bedeutet, dass Daten im Laufe der Verarbeitung oder Übertragung mittels des Systems nicht beschädigt oder durch Nichtberechtigte unbefugt verändert werden können.⁴⁶ Beschädigungs- oder Veränderungsmöglichkeiten sind das Ersetzen, Einfügen und Löschen von Daten oder Teilen davon.

Manipulationen dürfen nicht unbemerkt bleiben.⁴⁷ Das bedeutet, dass Techniken erforderlich sind, mit deren Hilfe unautorisierte Manipulationen nachträglich erkennbar sind. So kann verhindert werden, dass unautorisiert manipulierte Daten weiterverarbeitet werden, sodass der mögliche Schaden begrenzt wird.⁴⁸ Zur Erkennung von durchgeführten Datenveränderungen werden kryptographisch sichere Hashfunktionen eingesetzt.⁴⁹ Neben der Erkennbarkeit ist auch die (automatische) Verbesserung verfälschter Inhalte, sprich die Wiederherstellung des Ausgangszustands, wünschenswert, was jedoch nicht immer technisch realisierbar ist.⁵⁰

Ein Sonderaspekt der Korrektheit von Daten ist die zeitliche Korrektheit. Hierbei kommt es nicht auf die inhaltliche Unver-

33 Holznel (Fn. 8), 14; Biskup (Fn. 23), 42.

34 Eckert (Fn. 10), 7.

35 Holznel (Fn. 8), 14.

36 Eckert (Fn. 10), 7.

37 Rost/Pfützmann, DuD 2009, 355.

38 Pohl, DuD 2004, 680.

39 Anweisungen zu § 6, Unterpunkt 6.2.5.

40 Verordnung über die Form des Refinanzierungsregisters nach dem Kreditwesengesetz sowie die Art und Weise der Aufzeichnung (Refinanzierungsregisterverordnung – RefiRegV).

41 Dustar/Gall/Hauswirth, Software-Architekturen für Verteilte Systeme – Prinzipien, Bausteine und Standardarchitekturen für moderne Software, 2003, 217.

42 Holznel (Fn. 8), 13.

43 So zum Beispiel in § 2 Abs. 2 BSIg.

44 <http://www.demonium.de/th/home/sicherheit/grundlagen/sachziele.phtml>.

45 Holznel (Fn. 8), 13; Biskup (Fn. 23), 41.

46 Holznel/Schumacher, MMR 2009, 3; Holznel (Fn. 8), 13; Biskup (Fn. 23), 42.

47 Biskup (Fn. 23), 42.

48 Eckert (Fn. 10), 8.

49 Eckert (Fn. 10), 8.

50 Biskup (Fn. 23), 42.

fälschtheit an, sondern auf die genaue Einhaltung einer gewissen zeitlichen Abfolge. So kann es notwendig sein, dass gewisse Informationen in einer bestimmten zeitlichen Reihenfolge empfangen werden (eben genau so wie vom Sender losgeschickt), um beispielsweise den übergeordneten Sinn- und Informationsgehalt aufrechtzuerhalten. Auch die simple Kenntnis, ob eine Nachricht „neu“ ist, kann manchmal entscheidend sein. Zu denken ist beispielsweise an Börsenkurse.⁵¹

Verlässlichkeit (dependability, reliability)

Mit der Integrität und Verfügbarkeit zusammenhängend sind die Verlässlichkeit und die Beherrschbarkeit von Systemen.

Unter Verlässlichkeit eines Systems versteht man die Eigenschaft keine unzulässigen oder undefinierten Zustände anzunehmen (dependability) und die Gewährleistung, dass die spezifizierte Funktion zuverlässig erbracht wird (reliability).⁵²

Die tatsächlich vorhandene Ist-Funktionalität soll folglich mit der vorher bestimmten Soll-Funktionalität übereinstimmen. Dieser Verlässlichkeitsaspekt wird auch als Funktionssicherheit oder Ordnungsmäßigkeit bezeichnet. Um eine hohe Verlässlichkeit zu erzielen, werden in der Praxis verschiedene Testverfahren eingesetzt, wie etwa Unit Tests, die Nutzungsszenarien einer Software simulieren und auf eventuell vorhandene Abweichungen zur Soll-Funktionalität prüfen.⁵³

Alternativ wird Verlässlichkeit als eine Sachlage definiert, bei der weder die Systeme, noch die mit ihnen verarbeiteten Daten (Informationen), noch die Datenverarbeitung (Funktionen und Prozesse) in ihrem Bestand, ihrer Nutzung oder ihrer Verfügbarkeit unzulässig beeinträchtigt werden.⁵⁴

Beherrschbarkeit (controllability)

Im Unterschied zur Verlässlichkeit, welche die Sicherheit des Systems betrifft, bezieht sich die Beherrschbarkeit auf die Sicherheit des Betroffenen. Beherrschbarkeit wird auch als „Freiheit von Nebenwirkungen“ ausgelegt und bedeutet konkret, dass das IT-System kein „Eigenleben“ entwickelt und damit keine nichttolerierbaren Nebenwirkungen auftreten. Ein IT-System ist beherrschbar, wenn der Einzelne und die Gesellschaft vor unerwünschten oder ungewollten Auswirkungen des Einsatzes des IT-Systems im Rahmen des vorzuziehenden Grenzzusatzes bewahrt bleiben.⁵⁵ Maßnahmen um Nebenwirkungen zu reduzieren sind die gründliche Validierung von Eingabedaten und das bewusste Abfangen von ungültigen Daten, die zu fehlerhaften Zuständen führen könnten.

⁵³ Frankl/Hamlet/Littlewood/Strigini, Choosing a testing method to deliver reliability, in Proceedings of the 19th International Conference on Software Engineering ICSE '97, ACM, New York, NY, 68-78.

⁵⁴ Dierstein (Fn. 31), 346.

⁵⁵ Dierstein (Fn. 31), 348.

⁵¹ Biskup (Fn. 23), 45.

⁵² Eckert (Fn. 10), 6.

Nicht-Vermehrbarkeit (non-propagation)

Nicht-Vermehrbarkeit von Informationen bedeutet, dass diese von Unberechtigten nicht kopiert oder im Rahmen von sogenannten „Replay-Angriffen“ nicht unerkannt wiederholt werden können. Im Falle eines Replay-Angriffs sammelt der Angreifer zuvor aufgezeichnete Daten, um diese später gezielt wieder einzuspielen und eine fremde Identität vorzutäuschen. Dies kann zum Beispiel zur missbräuchlichen Wiederholung einer finanziellen Transaktion führen.⁵⁶ Eine verbreitete Gegenmaßnahme gegen Replay-Angriffe ist die Verwendung von großen, nicht vorhersagbaren und nur einmalig gültigen Zeichenketten, sogenannten Nonces.⁵⁷

Kontingenz (contingency)

Kontingenz soll als ein Schutzziel gegen Einengungen durch Technik fungieren und stellt das „Dual“ zur Integrität dar. Trotz des Technikeinsatzes soll es möglich sein, Inhalte und Umstände der Technik-anwendung in der Schwebe zu halten, um nicht durch diesen Technikeinsatz ohne Interventionsmöglichkeit eingeengt zu werden.⁵⁸ Inhalt des Schutzziels „Kontingenz“ ist die Möglichkeit der Feststellung, dass „etwas anders sein könnte, als es scheint“.⁵⁹ Das Schutzziel „Integrität“ er-

laubt hingegen immer nur die Feststellung, dass „etwas so ist, wie es ist“.⁶⁰

Glaubhafte Abstreitbarkeit (plausible deniability)

Diese Möglichkeit Technik unter Bedingungen zu stellen,⁶¹ erinnert stark an das durch Kryptographie ermöglichte Konzept der glaubhaften Abstreitbarkeit, das technisch beispielsweise in der Verschlüsselungssoftware „Truecrypt“⁶² oder beim sogenannten „Off-the-Record Messaging“⁶³ umgesetzt wurde.

Bei Truecrypt wird es beispielsweise unmöglich gemacht nachzuweisen, dass überhaupt Verschlüsselung eingesetzt wird. Die verschlüsselten Daten sehen wie Zufallszahlen⁶⁴ aus. Eine daraus abgeleitete Umsetzung ist die Möglichkeit der Nutzung von versteckten Datencontainern oder ganzen Betriebssystemen innerhalb eines äußeren Dummycontainers. Wird der Nutzer beispielsweise mit Gewalt dazu gezwungen das vermeintlich richtige Passwort zu verraten, so kann er das Passwort des äußeren Containers angeben, ohne dass die Daten im inneren Container sichtbar werden. Weil die verschlüsselten Daten der beiden Container immer wie Zufallszahlen aussehen, ist es möglich, die Existenz des versteckten Containers plausibel abzustreiten. Ein Angreifer kann nicht beweisen, dass neben dem Dummycontainer weitere versteckte Container

existieren. Es scheint ein Container vorhanden zu sein, es könnten aber auch überhaupt keiner (lediglich Zufallszahlen) oder mehr als einer vorhanden sein.

Fazit

Die vorliegende Zusammenstellung soll zeigen, dass IT-Sicherheit nicht mehr nur auf den drei klassischen Schutzzielen Vertraulichkeit, Verfügbarkeit und Integrität aufbaut, sondern dass diese im Laufe der letzten zwanzig Jahre ergänzt und – nicht zuletzt wegen geänderter Sicherheitsanforderungen – immer feingliedriger ausgestaltet und damit konkretisiert wurden. So wie eine abstrakte Rechtsnorm im Laufe der Zeit durch die Rechtsprechung konkretisiert und möglicherweise rechtlich fortgebildet wird, so werden auch die Schutzziele der IT-Sicherheit, eben wegen der steigenden Bedeutung der IT-Sicherheit, auch in Zukunft durch die Wissenschaft und Praxis, immer detaillierter und konkreter weiterentwickelt werden.

Während einige der dargestellten Schutzziele, beispielsweise die Zurechenbarkeit oder die Authentizität, hauptsächlich die Reduzierung der Schadenseintrittswahrscheinlichkeit zum Inhalt haben, kann auch die Reduzierung des Schadenspotentials eine Zielsetzung der IT-Sicherheit sein, zum Beispiel durch den Einsatz von Pseudonymen. Stichworte in diesem Zusammenhang sind „Schadensvermeidung“ und „Schadensverminderung“.⁶⁵

60 Rost/Pfutzmann, DuD 2009, 354.

61 Rost/Pfutzmann, DuD 2009, 354.

62 <http://www.truecrypt.org/docs/hidden-volume-protection>.

63 <http://www.cypherpunks.ca/otr>.

64 Datenträger werden beispielsweise mit Zufallszahlen überschrieben, um die darauf enthaltenen Daten zu vernichten.

65 Näheres dazu siehe Hammer, Die 2. Dimension der IT-Sicherheit, 1999.

56 http://www.repges.net/IPSec/Angriffe_IPSec/INTERN_1/intern_1.HTM.

57 Kappes, Netzwerk- und Datensicherheit, 2007, 208.

58 Rost/Pfutzmann, DuD 2009, 353 f.

59 Rost/Pfutzmann, DuD 2009, 354.