Begriffsdefinitionen in KASTEL

27. September 2013

Definitionen

1. *Angreifer*
   Ein Angreifer ist ein System, eine Person oder eine Personengruppe, die einen oder mehrere Angriffe durchführen.

2. *Angreifermodell*
   Ein Angreifermodell beschreibt die Fähigkeiten eines Angreifers, Angriffe auf ein System durchzuführen.

3. *Angriff*
   Ein Angriff ist die gezielte Realisierung einer Bedrohung.

4. *Architektur*
   Die Architektur eines Systems beschreibt die Struktur der einzelnen Komponenten des Systems und deren Zusammenwirken über ihre Schnittstellen.

5. *Authentizität*
   Ein System bewahrt Authentizität (Nachrichtenauthentizität/Datenursprungsauthentizität), wenn es schwache Integrität bewahrt

und es möglich ist, den Ursprung jedes Datums zu identifizieren (vgl. [20]).

6. *Autorisierung*
   Autorisierung ist die Erlangung einer Berechtigung.

7. *Autorisierungsverletzung*
   Eine Autorisierungsverletzung ist der Zugriff auf eine Ressource ohne im Besitz einer entsprechenden Berechtigung zu sein.

8. *Bedrohungen*
   Eine Bedrohung eines Systems ist eine Möglichkeit, ein oder mehrere Sicherheitsziele gezielt zu beeinträchtigen.

9. *Datenschutz-Schutzziel*
   Ein Datenschutz-Schutzziel ist ein Sicherheitsziel, das das abstrakte Gut der Privatsphäre schützt.

10. *Güter*
    Güter sind Ressourcen, die für mindestens einen Akteur einen (subjektiven) realen oder ideellen Wert besitzen.

11. *Integrität*
    Ein System bewahrt *starke* Integrität, wenn es nicht möglich ist, Daten unautorisiert zu manipulieren (vgl. [20]). Ein System bewahrt *schwache* Integrität, wenn es nicht möglich ist, Daten unautorisiert und unbemerkt zu manipulieren (vgl. [10]).

12. *Intervenierbarkeit*
    Intervenierbarkeit ist gegeben, wenn ein System jedem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam durch operationalen Zugriff auf Verfahren und Daten ermöglicht.

13. *Komponente*
    Eine Komponente ist ein Bestandteil eines technischen Systems,

der eine abgeschlossene (Teil-)Funktion des Systems realisiert und durch explizite Schnittstellen sowohl diese Funktion anbietet als auch Funktionen anderer Komponenten erfordern kann.

14. *Nichtabstreitbarkeit*
    Ein System bewahrt Nichtabstreitbarkeit in Bezug auf einen Vorgang gegenüber einem Akteur, wenn das Stattfinden des Vorgangs nicht nachträglich durch eine der beteiligten Instanzen gegenüber dem Akteur wirksam abgestritten werden kann.

15. *Nichtverkettbarkeit*
    Nichtverkettbarkeit ist dann gewährleistet, wenn personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können.

16. *Risiko*
    Das Risiko einer Bedrohung bildet die Höhe des potentiell entstehenden Schadens und die Eintrittswahrscheinlichkeit (oder relative Häufigkeit) auf einen Zahlenwert ab.

17. *Safety*
    Zustand des Geschütztseins von bestimmten Gütern vor bestimmten Gefahren.

18. *Security*
    Zustand des Geschütztseins von bestimmten Gütern vor bestimmten Bedrohungen.

19. *Sicherheit*
    Zustand des Geschütztseins von bestimmten Gütern vor bestimmten Bedrohungen und Gefahren (also Security *und* Safety).

20. *Sicherheitsanforderungen*
    Nicht-funktionale Anforderungen, um definierte Sicherheitsziele zu erreichen (vgl. [6]).

21. *Sicherheitsmechanismus*
    Ein Sicherheitsmechanismus ist ein Verfahren zur Durchsetzung eines oder mehrerer Sicherheitsziele.

22. *Sicherheitsrichtlinien*
    Sicherheitsrichtlinien geben vor, welche Sicherheitsanforderungen erfüllt werden müssen und welche Maßnahmen dafür durchgesetzt werden sollen.

23. *Sicherheitsvorfall*
    Ein Sicherheitsvorfall ist ein eingetretenes Ereignis, durch das ein Sicherheitsziel verletzt wurde.

24. *Sicherheitsziel*
    Ein Sicherheitsziel beschreibt eine Eigenschaft einer Komponente oder eines Systems, die erfüllt werden muss, um bestimmte Güter vor bestimmten Bedrohungen zu schützen.

25. *System*
    Ein System ist die Gesamtheit von Komponenten, die zusammenwirken, um eine bestimmte Funktionalität zu erfüllen.

26. *Transparenz*
    Transparenz ist die Möglichkeit, die Erhebung, Verarbeitung und Nutzung von Daten mit zumutbarem Aufwand planen, nachvollziehen, überprüfen und bewerten zu können.

27. *Verfügbarkeit*
    Die Verfügbarkeit eines Systems beschreibt, in welchem Maße die Funktionalität des Systems von berechtigten Subjekten unabhängig von Einflüssen in Anspruch genommen werden kann.
    Die Verfügbarkeit eines Systems in Gegenwart von Angreifern beschreibt, in welchem Maße die Funktionalität des Systems von berechtigten Subjekten unabhängig von gezielten Einflüssen in Anspruch genommen werden kann.

28. *Vertraulichkeit*
    Ein System bewahrt Vertraulichkeit, wenn es keine unautorisierte Informationsgewinnung ermöglicht.

29. *Verwundbarkeit*
    Verwundbarkeit ist eine Bedrohung, die von mindestens einem der betrachteten Angreifer realisiert werden kann.

30. *Zugriffsschutz*
    Alle Benutzer erhalten jeweils nur bestimmte Zugriffsrechte auf bestimmte Daten, Informationen und Ressourcen.

31. *Zurechenbarkeit*
    Zurechenbarkeit bezüglich eines Akteurs ist gegeben, wenn Vorgänge den beteiligten Instanzen gegenüber dem Akteur zugeordnet werden können.

Begründung

zu (1)

Erläuterung:
Es wird üblicherweise zwischen passiven und aktiven Angreifern unterschieden. Ein passiver Angreifer ist dadurch charakterisiert, dass er die Datenübertragung lediglich abhört, während ein aktiver Angreifer beliebig in das Kommunikationsprotokoll eingreifen kann (z. B. durch Vortäuschen einer fremden Identität, Veränderung/Fälschung von Nachrichten, Einschränkung der Verfügbarkeit etc.) (vgl. [31]).

Synonyme:
Adversary, Attacker

Verwandte Begriffe:
Angriff, Angreifermodell

zu (2)

Erläuterung:
Zu der Beschreibung der Fähigkeiten gehören die erlaubten Aktionen, die der Angreifer nach Annahme machen darf (beispielsweise könnte das Abhören von Nachrichten erlaubt, das Manipulieren derselben jedoch unmöglich sein), die verschiedenen Ressourcentypen, auf die er Zugriff hat (in einem Rechnernetz bestehend aus den Rechnern A,B,C könnte der Angreifer z. B. die Kontrolle über den Rechner A haben, während die anderen beiden Rechner nicht unter seiner Kontrolle stehen) sowie die Rechenleistung des Angreifers (z. B. könnte eine polynomielle Laufzeitbeschränkung in einem Sicherheitsparameter gefordert werden).

Verwandte Begriffe:
Angreifer, Angriff

Beispiele:
Das Dolev-Yao-Angreifermodell (vgl. [9]), Angreifermodelle für

Verschlüsselungsverfahren wie z. B. das Chosen-Ciphertext-Attack-Modell (vgl. [21])

zu (3)

Erläuterung:
Die Formulierung „gezielte Realisierung“ bringt zum Ausdruck, dass die im Rahmen eines Angriffs durchgeführten Aktionen *absichtlich* erfolgen. Beispielsweise ist die Änderung von Nachrichten durch zufällig hervorgerufene Bitfehler kein Angriff, sie bedroht aber dennoch deren Integrität.

Synonyme:
Attack

Verwandte Begriffe:
Angreifer, Angreifermodell, Bedrohungen

zu (4)

Erläuterung:
Diese Definition lehnt sich an die Definition von Kruchten, Obbink und Stafford (2006, p. 23 [22]) an: „Software architecture involves the structure and organization by which modern system components and subsystems interact to form systems, and the properties of systems that can best be designed and analyzed at the system level“. Wir lassen die Forderung nach der Organisation der Komponenten fallen, da auch ohne dies eine Architektur beschrieben werden kann und unklar ist, welche Mindestanforderungen eine Organisationsbeschreibung erfüllen müsste. Wir verzichten außerdem auf die unnötige Einschränkung auf moderne Komponenten und vermeiden die Nennung von Subsystemen, um auch Systeme ohne explizite Subsysteme abzudecken. Die Einschränkung auf Eigenschaften. die am besten auf Systemebene entworfen und analysiert werden können, haben wir nicht übernommen, da dies zwar für Architekturen wünschenswert, aber kaum objektiv messbar ist und nicht zwingend vorliegen muss, um von einer

Architektur zu sprechen. Gerade bei der Analyse der Sicherheit von Systemarchitekturen sind je nach Art der Analyse und des Systems unterschiedliche Eigenschaften nötig oder überflüssig.

Synonyme:
Systemarchitektur, Architecture

Beispiel:
Um beispielsweise eine Client-Server-Architektur nach dieser Definition zu beschreiben, muss ausgedrückt werden, welche Komponenten Dienste bereitstellen, welche Komponenten Dienste in Anspruch nehmen, es müssen die Schnittstellen für Dienstanfragen und Ergebnisse beschrieben und erläutert werden, welche Komponenten zur Bereitstellung eines Dienstes über diese Schnittstellen zusammenwirken.

zu (5)

Erläuterung:
Die hier eingeführte Definition lässt auch technische Systeme als Ursprung zu. Dies erlaubt eine modularere Handhabung des Begriffs der Authentizität, indem es beispielsweise ermöglicht, für ein Gesamtsystem Authentizität zu fordern, aber innerhalb eines technischen Systems zu erlauben, dass Authentizität für ein Subsystem auch dann gewährleistet ist, wenn als Datenursprung ein anderes technisches System identifizierbar ist, und von diesem System wiederum der Urheber in Form einer Person/eines Benutzers ermittelt werden kann.

Abgrenzung:
Aus rechtlicher Sicht ist Authentizität gegeben, wenn sichergestellt ist, dass empfangene Daten auch tatsächlich von authentisierten und autorisierten Benutzern stammen [15].

Synonyme:
Authenticity, Echtheit, Originalität

Verwandte Begriffe:
Integrität

Beispiel:
Die Authentizität von Daten kann mittels digitaler Signaturen überprüft werden.

zu (6)

Erläuterung:
Autorisierung sagt zunächst nichts darüber aus, ob die Erlangung rechtmäßig/bestimmungsgemäß erfolgt ist, d. h. sowohl die Erlangung einer Berechtigung aufgrund unrechtmäßig erlangter Autorisierungstokens oder aufgrund von Fehlkonfigurationen gilt als Autorisierung. Üblicherweise geschieht Autorisierung durch Authentifizierung der zu autorisierenden Instanz und anschließende Überprüfung der damit verbundenen Berechtigungen. Es gibt jedoch auch Verfahren, die unabhängig von der Identität funktionieren. Die Erlaubnis ist dann unabhängig von der Identität überprüfbar und liegt oftmals in Form eines Berechtigungsnachweises vor (z. B. eine nicht personengebundene Eintrittskarte).

Synonyme:
Authorisation

Verwandte Begriffe:
Authentizität, Zugriffsschutz

Beispiel:
Während eines Login-Vorgangs überprüft die autorisierende Instanz (Server), ob Benutzername und Passwort zusammenpassen. Eine erfolgreiche Überprüfung führt zur Autorisierung, also zur Berechtigung, Beiträge im Forum zu lesen.

zu (7)

Erläuterung:
Eine Autorisierungsverletzung oder Zugriffsverletzung bedeutet nach dieser Definition lediglich, dass der Zugriffsschutz unzureichend konzeptioniert oder realisiert wurde. Auch ohne Umgehung eines Zugriffsschutzes kann eine Autorisierungsverletzung zivilrechtliche Folgen, wie beispielsweise Schadensersatzansprüche aufgrund von Vertragsverletzungen, nach sich ziehen. Es kommt auch eine Schadensersatzpflicht nach §§ 7, 8 BDSG in Betracht, sofern eine verantwortliche Stelle Daten unzulässig oder unrichtig verwendet.

Abgrenzung:
Die Definition sagt nichts darüber aus, ob eine Berechtigung vorliegt und wann und auf welche Weise dies ggf. geprüft wurde. Ebenso wenig wird eine Aussage gemacht, ob Berechtigungen ablaufen, delegiert werden können oder weitere Berechtigungskonzepte vorliegen und korrekt überprüft wurden.

Synonyme:
Zugriffsverletzung, Access violation

Verwandte Begriffe:
Autorisierung, Zugriffsschutz

Beispiel:
Wenn der Finder eines mobilen Rechners Zugriff auf Ressourcen eines fernwartbaren Systems erlangt, die nur dem Besitzer des Rechners eingeräumt wurden, dann liegt eine Autorisierungsverletzung obwohl u. U. keine Zugriffskontrolle des fernwartbaren Systems selbst versagt hat.

zu (8)

Erläuterung:
Üblicherweise wird zwischen internen und externen Bedrohungen unterschieden (vgl. [6]). Beispielsweise ist der Geheimnisverrat

durch einen Mitarbeiter eine interne Bedrohung, während der potenzielle Angriff durch Hacker eine externe Bedrohung darstellt.

Verwandte Begriffe:
Angriff

Beispiel:
Man-in-the-middle, Denial-of-Service, Seitenkanäle

zu (9)

Erläuterung:
Der Begriff der Datenschutz-Schutzziel(e) ist entwicklungsoffen und nicht statisch (vgl. [7]). Neben den klassischen Schutzzielen Transparenz, Nichtverkettbarkeit und Intervenierbarkeit kommen weitere Schutzziele in Betracht. Das können sein: Vertraulichkeit, Nichtverfolgbarkeit, Unbeobachtetheit, Verdecktheit, Anonymität, Pseudonymität, Zurechenbarkeit, Authentizität, Revisionsfähigkeit, Integrität, Verlässlichkeit, Beherrschbarkeit, Nicht-Vermehrbarkeit, Verfügbarkeit und Kontingenz. (vgl. [7])

Abgrenzung:
Der Begriff Sicherheitsziel ist ein Oberbegriff und bezieht sich allgemein auf Komponenten bzw. Systeme und deren zu schützende Güter. Der Begriff Datenschutz-Schutzziel bezieht sich deshalb konkret auf Datensicherheit/technischen Datenschutz.

Verwandte Begriffe:
Sicherheitsziel

zu (10)

Erläuterung:
Sicherheitsziele schützen Güter vor Bedrohungen. Die Zuordnung eines Wertes wird stets aus der subjektiven Sicht eines Akteurs festgelegt. Aus datenschutzrechtlicher Sicht ist das „Recht auf informationelle Selbstbestimmung“ das schützenswerte Gut. Andere Rechtsgebiete schützen andere Güter (materiell und immateriell),

z. B. Urheberrechte, Eigentum (§ 242 StGB - Diebstahl), Vermögen (§ 263 StGB - Betrug).

Diskussion:
Die Definition entspricht sinngemäß der von Haley et al.:
„Security needs arise when stakeholders establish that some resource involved in a system, be it tangible (e.g., cash) or intangible (e.g., information or reputation), is of value to the organization. Such resources are called assets and the stakeholders naturally wish to protect themselves from any harm involving these assets. Security goals express this desire, describing the involved asset(s) and the harm to be prevented.“ (Abschnitt 2.1, [17]). Ebenso entspricht diese Definition sinngemäß der in der Common Criteria: „assets – entities that the owner of the TOE (target of evaluation) presumably places value upon“ (Abschnitt 4.1, Zeile 18, [12]).

Synonyme:
Assets

Verwandte Begriffe:
System, Sicherheit

Beispiel:
Daten bzw. Information, Ehrschutz und Privatsphäre (Ansehen), Geld, Gesundheit, Verfügbarkeit von aktuellen Nachrichten, Authentizität eines Steuerbefehls, usw.

zu (11)

Erläuterung:
Die starke Integrität fordert die Unmöglichkeit einer unautorisierten Datenmanipulation. Im Allgemeinen ist für komplexe Systeme eine solche Anforderung zu strikt als dass man sie sinnvoll realisieren könnte. Sie ist technisch allerdings für kleinere, sicherheitskritische Subsysteme durchaus sinnvoll, da sie mittels formaler Methoden unter Umständen nachgewiesen werden kann. In kom-

plexen Systemen würde eher eine schwache Integrität gefordert werden, da diese realistisch umsetzbar ist.

Abgrenzung:
Aus rechtlicher Sicht kann die Integrität bzw. Unversehrtheit von Daten durch elektronische Signaturverfahren erreicht werden [39].

Diskussion:
Die Definition der starken Integrität greift die Definition nach Jürjens [20] auf. Diese verlangt das Verhindern einer Manipulation. Die Definition der schwachen Integrität ist an die Definition nach Eckert [10] angelehnt. Hier ist es hinreichend, dass eine Manipulation der Daten festgestellt werden kann. Schwache Integrität ist eine Voraussetzung für Authentizität.

Die Definition der starken Integrität greift die Definition nach Jürjens [20] auf: Die Integrität einer Variable erhält ein System, falls kein Angreifer existiert, so dass zu irgendeinem Zeitpunkt während der Ausführung des Systems im Beisein des Angreifers die Variable einen anderen Wert enthält als sie soll. Problematisch ist bei dieser Definition, dass Sie den Angreifer und dessen Fähigkeiten direkt miteinbezieht. Es muss zusätzlich spezifiziert werden, welchen Wert eine Variable haben soll. Diese Definition entspricht außerdem einer Allquantifizierung über alle möglichen Zustände einer Variable des Systems und schließt somit auch Zwischenzustände ein, die eventuell wieder repariert werden könnten.

Synonyme:
Integrity, Unversehrtheit

Verwandte Begriffe:
Authentizität

Beispiel:
Schwache Integrität kann innerhalb eines einzelnen Systems mit Hilfe kryptographischer Hashfunktionen, wie z. B. SHA-256 überprüft werden. Soll Integrität bei einem Datenautausch zwischen

verteilten Systemen überprüft werden, dann schützen kryptographische Hash-Funktionen allein jedoch nicht vor absichtlicher Manipulation der übertragenen Daten durch einen (Man-in-the-middle-)Angreifer, da dieser den zur manipulierten Nachricht passenden Hashwert berechnen kann. Dieses Problem kann z. B. durch Message Authentication Codes (MAC), wobei ein gemeinsames Geheimnis von Sender und Empfänger in die Berechung des Hashwerts einfließt, oder durch kryptographische Signaturen (vgl. Authentizität) gelöst werden.

zu (12)

Erläuterung:
Intervenierbarkeit ist ein Datenschutz-Schutzziel, das seinen Ursprung im schleswig-holsteinischen Datenschutz hat. Intervenierbarkeit soll Betroffenen durch technisch-organisatorische Maßnahmen die Möglichkeit einräumen, in einer Weise auf Daten und Verfahren zugreifen zu können, die es ihnen erlaubt, personenbezogene Daten einzusehen (§ 34 BDSG) und deren Korrektur, Sperrung oder Löschung zu fordern. Technische bzw. funktionale Anforderungen, die sich durch die Forderung von Intervenierbarkeit ergeben, müssen für jedes konkrete System und dessen Einsatzszenario gesondert betrachtet und festgelegt werden.

In [29] wird argumentiert, dass Transparenz eine notwendige Bedingung für Intervenierbarkeit ist, beispielsweise um einem Betroffenen nachweisen zu können, dass ein von ihm initiiertes oder gefordertes Löschen von Daten sich auch tatsächlich auf sämtliche Generationen von Kopien und Backups erstreckt hat.

Synonyme:
Intervenability

Verwandte Begriffe:
Transparenz

Beispiel:
Intervenierbarkeit kann durch die Einrichtung eines Single-Point-Of-Contact für Betroffene umgesetzt werden, wo Betroffene beispielsweise ihren datenschutzrechtlichen Auskunftanspruch (§ 34 BDSG) einfordern können [29]. In Berlin wurde Intervenierbarkeit gesetzlich (§ 31a LDSG Berlin) durch ein Recht auf einen roten Not-Aus-Schalter an einem SmartMeter konkretisiert.

zu (13)

Erläuterung:
Die *Schnittstellen* erlauben den Zugriff auf die Funktion einer Komponente und die Interaktion mit anderen Komponenten oder Nutzern.

Abgeschlossenheit bedeutet, dass die Funktion einer Komponente unmittelbar verwendet werden kann, wenn die Funktionen der von ihr benötigten Komponenten zur Verfügung stehen (vergl. Szyperszki 2011, p. 41 [33]). Das heißt es gibt keine weiteren Bedingungen, die erfüllt werden müssen, um die Komponente zu verwenden. Diese Eigenschaft erlaubt es, Komponenten innerhalb eines Systems und über mehrere Systeme hinweg wiederzuverwenden. Die Möglichkeit der Komposition, also das Zusammenfügen mehrerer Komponenten zu einem Gesamtsystem, gibt der Komponente ihren Namen. Auch wenn Analysen zu einzelnen Komponenten für technische Disziplinen entscheidend sein können, sind solche isolierten Betrachtungen aus juristischer Sicht nicht zielführend. Eine Beurteilung kann immer nur im Gesamtkontext des Systems und seiner Verwendung erfolgen. So kann es beispielsweise eine entscheidende Rolle spielen, in welchem Land ein datenverarbeitender Server steht, auch wenn die technische Analyse der einzelnen Komponenten und des Gesamtsystems davon unbeeinflusst sein kann.

Abgrenzung:
Diese Definition sagt nichts über die Sicherheitseigenschaften und

Schutzziele von Komponenten aus. Es können keine pauschalen Aussagen darüber getroffen werden, ob Sicherheitseigenschaften bei der Komposition mehrerer Komponenten erhalten bleiben (Murdoch 2010 [24]). Wie schützenswert häufig wiederverwendete Komponenten aufgrund ihres höheren Einflusses auf das Gesamtsystem sind, lässt sich ebenfalls nicht allgemein feststellen.

Diskussion:
Diese Definition übernimmt die Forderung nach ausschließlich expliziten Abhängigkeiten von der Definition von Clemens Szyperski (Szyperszki 2011, p. 41). Sowohl die Forderung, dass Schnittstellen vertraglich festgelegt sein müssen, als auch die Betonung der Komposition und der unabhängigen Verwendung wurden nicht aufgegriffen. Der Grund dafür ist, dass die Festlegung der Schnittstellen sehr unterschiedliche Formen annehmen kann und Komposition und unabhängige Verwendung nicht zwingend vorliegen, sondern nur möglich sein müssen.

Synonyme:
Component

Verwandte Begriffe:
System

zu (14)

Erläuterung:
Als *Nichtabstreitbarkeit der Herkunft* bezeichnet man auch die Nichtabstreitbarkeit in Bezug auf das Abschicken einer Nachricht. Als Nichtabstreitbarkeit des Erhalts bezeichnet man auch die Nichtabstreitbarkeit in Bezug auf den Erhalt einer Nachricht. Damit tatsächlich alle Teilnehmer betrachtet werden, muss der Vorgang, für den Nichtabstreitbarkeit gefordert wird, entsprechend gefasst werden. So macht es beispielsweise bei einem Bestellvorgang einen Unterschied, ob der Vorgang zwischen Kunde und Online-Versandhaus oder technisch zwischen Client und Server inklusive der Netzinfrastruktur betrachtet wird. Der Grund für die

„doppelte Verneinung“ – also „nicht abgestritten“ statt „nachgewiesen“ – sind Einzelfälle, in denen z. B. eine Beweislastumkehr vorliegen kann und daher für diese Einzelfälle beide Formulierungen nicht äquivalent sind, auch wenn sie das für die Gesamtheit aller Fälle theoretisch wären.
Der Begriff *wirksam* wurde verwendet, um klar zu stellen, dass prinzipiell vieles abgestritten werden kann. Es soll hier aber ausgedrückt werden, dass ein Abstreiten einer dritten Instanz gegenüber glaubhaft ist. Möglichkeiten „wirksam“ zu ersetzen, wären „glaubhaft“ oder „glaubwürdig“.

Abgrenzung:
Nichtabstreitbarkeit (Non-Repudiation) und Unleugbarkeit sind Synonyme. Zurechenbarkeit (accountability) jedoch nicht, da Zurechenbarkeit zwar Nichabstreitbarkeit zur Folge hat, aber nicht unbedingt umgekehrt.

Diskussion:
Es ist zwischen Nichtabstreitbarkeit gegenüber unbeteiligten Dritten und einem Beteiligten zu unterscheiden. Man könnte sich etwa Kunden eines Cloud-Dienstleisters vorstellen, denen untereinander aber nicht nach außen Nichtabstreitbarkeit gewährleistet wird. In diesem Fall gäbe es keine unbeteiligte dritte Entscheidungsinstanz.

Synonyme:
Non-Repudiation, Unleugbarkeit

Verwandte Begriffe
Zurechenbarkeit

Beispiel:
Wird mit einem Online-Versandhaus ein Vertrag geschlossen, ist es notwendig, dass für den Eingang einer Bestellung Nichtabstreitbarkeit vorliegt. So kann nachgewiesen werden, dass ein Vertrag zustandegekommen ist.

zu (15)

Erläuterung:
Die Definition der Nichtverkettbarkeit ist dem Landesdatenschutzgesetz des Landes Schleswig-Holstein entnommen (§ 5 I 2 Nr. 5 LDSG-SH). Diese Definition basiert auf dem datenschutzrechtlichen Zweckbindungsgrundsatz bei der Erhebung, Verarbeitung und Nutzung von Daten. Sind Daten und Verfahren an bestimmte Zwecke gebunden, dann bedeutet Nichtverkettbarkeit, dass eine zweckübergreifende Verknüpfung von Daten sowie eine zwecküberschreitende Verarbeitung und Nutzung von Daten verhindert wird.

[7] und [29] weisen darauf hin, dass es in vielen Fällen zu Konflikten zwischen Unverkettbarkeit einerseits und den Schutzzielen der Transparenz und der Zurechenbarkeit andererseits kommen kann.

Diskussion:
[26] und [30] postulieren Definitionen, die darauf abstellen, dass Nichtverkettbarkeit erfüllt ist, wenn gewährleistet ist, dass ein externer Angreifer durch Beobachten eines gegebenen Szenarios keine neuen wechselseitigen Zuordnungen zwischen Subjekten, Objekten und Daten lernen kann.

Synonyme:
Unlinkability, Unverkettbarkeit, Unverknüpfbarkeit

Verwandte Begriffe:
Vertraulichkeit

Beispiel:
Nichtverkettbarkeit wäre gewährleistet, wenn aufeinanderfolgende Abrufe von Informationen auf verschiedenen Webservern im Internet nicht miteinander in Verbindung gebracht werden können ([30]). Nichtverkettbarkeit von Kommunikationsbeziehungen kann dann beispielsweise durch die Nutzung von Mix-Kaskaden erreicht werden (David Chaum).

zu (16)

Erläuterung:

Ermittlung: Klassischerweise wird Risiko als Produkt aus Eintrittswahrscheinlichkeit eines Ereignisses und dessen Konsequenz gesehen, sodass sich „Risiko=potentieller Schaden mal Eintrittswahrscheinlichkeit“ ergibt. Die Gewichtung und mathematische Kombination kann jedoch an unterschiedliche Risikobewertungen bzw. -definitionen angepasst werden.

Entstehung: Risiken entstehen aus der Benutzung, dem Besitz und dem Betrieb von IT-Systemen. Dabei wird davon ausgegangen, dass selten sämtliche Bedrohungen für ein System eliminiert werden können. Die Risiko-Ermittlung ist ein Ansatz, eine wirtschaftliche Bewertung vorzunehmen (siehe auch Behandlung). Ein Klassifikationsschema zu den Einflussfaktoren von Risiken ist z. B. von der Open Group erstellt worden [16].

Behandlung: Risikomanagement beschäftigt sich mit der Minimierung, dem Monitoring, und der Kontrolle der Wahrscheinlichkeit und/oder dem Eintreten unvorhergesehener Ereignisse [38]. Einige Risiken, die durch bestimmte Bedrohungen entstehen, lassen sich nicht mit technischen Hilfsmitteln reduzieren. Hier bieten lediglich Maßnahmen auf Management-Ebene (z. B. Versicherungen, Rücklagen, Abmahnungen) oder Gesetze (z. B. Bundesdatenschutzgesetz, §202c StGB) Abhilfe.

Diskussion:
Typischerweise gehen Definitionen zu (IT-)Risiko neben Bedrohungen auch auf Verwundbarkeiten von Systemen ein [25],[37], [5], [16].
Die oben erwähnte Definition und insbesondere die Formel zur Risikoermittlung sind nicht unumstritten [16]: Eintrittswahrscheinlichkeiten von seltenen Ereignissen lassen sich nur schwer ermitteln. Weiterhin kann der dann entstehende Schaden häufig noch

schwerer bemessen werden. Die in der Formel vorgenommene Verknüpfung von Eintrittswahrscheinlichkeit und potentiellem Schaden per Multiplikation steht ebenso häufig in der Kritik.

Verwandte Begriffe:
Risikomanagement, Risikoanalyse

zu (17)

Erläuterung:
Sowohl gezielte Angriffe als auch Gefahren, die nicht durch Bedrohungen durch Angreifer entstehen, können die Safety gefährden. Daher schließt die Definition beide Fälle mit ein. In bestimmten Kontexten (z. B. beim Betrieb von technischen Systemen) ist Safety gleichbedeutend mit *Betriebssicherheit*. Da sich KASTEL mit Sicherheit im Sinne von Security, also mit dem Schutz vor Bedrohungen beschäftigt, definieren wir den Begriff Safety lediglich zur Abgrenzung von Security. Daher wurden auch Gefahren und der Schutz davor nicht näher betrachtet oder definiert.

Verwandte Begriffe:
Gefahrlosigkeit, Sicherheit, Betriebssicherheit

zu (18)

Erläuterung:
Es ist schwierig, Aussagen über den Schutz aller Güter vor allen Bedrohungen zu treffen. Daher muss Security immer im Hinblick auf *bestimmte* Güter und bestimmte Bedrohungen definiert und analysiert werden, also festgelegt werden welche Güter und Bedrohungen konkret betrachtet werden sollen. Die Dauer, für die Schutz vor Bedrohungen besteht, ist nicht Teil der Definition, aber viele Schutzmaßnahmen haben eine zeitlich begrenzte Effektivität. Beispielsweise kann ein kryptographisches Verfahren die Vertraulichkeit von Daten nur solange sicherstellen, bis das zugrunde liegende mathematische Problem deutlich schneller, z. B. aufgrund technischer Innovationen, gelöst werden kann.

Verwandte Begriffe:
Sicherheit

zu (19)

Erläuterung:
Es gibt Gefahren, die nicht von einem Angreifer ausgehen. Bedrohungen hingegen müssen immer von einem Angreifer ausgehen. Dennoch kann eine Bedrohung zu einer Gefahr führen. Umgekehrt kann auch das Eintreten von Gefahren zu neuen Bedrohungen führen.

Verwandte Begriffe:
Safety, Security, Schutz (vgl.[3])

zu (20)

Erläuterung:
Nach Haley et al. ([17]) müssen drei Kriterien für Sicherheitsanforderungen erfüllt sein, damit sie in einem Entwicklungsprozess dazu dienen können, die Sicherheit eines Systems prinzipiell verifizierbar zu machen.

a) Sicherheitsanforderungen werden als nicht-funktionale Anforderungen an das betrachtete System formuliert. Dabei sind sie so zu formulieren, dass deren Einhaltung zur Erreichung der definierten Sicherheitsziele des Systems führen. Sie dienen Systementdesignern und -Entwicklern als konkrete Beschreibung, welche Einkschränkungen bei der Umsetzung von funktionalen Anforderungen eingehalten werden müssen.

b) Um überprüfen zu können, ob durch die formulierten Sicherheitsanforderungen die gesteckten Sicherheitsziele erreicht werden, müssen Annahmen über das Verhalten der Systemumgebung gemacht werden: Der Analyst muss entscheiden, welche Teile der realen Welt (Domains) in die Sicherheitsbetrachtungen mit einbezogen werden (damit wird der für die Analyse

betrachtete Systemkontext festgelegt). Eine wichtige Rolle bei der Festlegung der relevanten Domänen spielen die Vertrauensannahmen. Dazu sollten Vertrauensbeziehungen zwischen allen Instanzen der Domains definiert und betrachtet werden.

c) Erfüllung der Sicherheitsanforderungen: Beim Systemdesign muss überprüft werden, welche Sicherheitsanforderungen prinzipell erfüllbar sind. Bei der Entwicklung muss überprüft werden, ob die Implementierung die Anforderung erfüllt. Der stärkste Nachweis wäre ein Beweis, andernfalls lässt sich auch oft durch plausibles Argumentieren schließen.

Verwandte Begriffe:
Security Requirements

Beispiele:
Beispielsweise könnte ein Sicherheitsziel „Vertraulichkeit von Benutzerdaten“ in einem System Sicherheitsanforderungen an die Funktionalität „Darstellung von Benutzungstatistiken“ und „Anzeige Benutzerdaten“ umgesetzt werden. Diese könnten dann lauten „Bei der Darstellung von Statistiken dürfen Daten nur für Benutzergruppen, nicht aber für einzelne Benutzer dargestellt werden“, oder „Die Anzeige von Benutzerdaten anderer Benutzer ist nur Administratoren möglich“. Im Cloud-Computing-Umfeld könnte das Sicherheitsziel „Vertraulichkeit“ bei der funktionalen Anforderungen „Kunden können ihre Dateien herunterladen“ unter anderem in der Anforderung „Beim Herunterladen wird die Kommunikation verschlüsselt“ münden.

zu (21)

Erläuterung:
Ein Sicherheitsmechanismus setzt ein oder mehrere Sicherheitsziele durch, die in Form von Sicherheitsrichtlinien konkretisiert werden [6], [8]. Daraufhin können gewisse Garantien bzgl. Sicherheit eines Systems gegeben werden. Sowohl Benutzer als auch Angreifer haben Anreize, die Sicherheitsrichtlinien einzuhalten oder

gegen sie zu verstoßen und Sicherheitsmechanismen zu umgehen [6].

Diskussion:
Hier wird ein weitere gefasstes Verständnis des Begriffs zugrunde gelegt als dies z. B. in [32] oder [19] der Fall ist. Wir folgen mit unserer Definition [6] und [8].
In der Literatur mit engerem Verständnis wird häufig noch eine Unterscheidung von Sicherheitsmechanismen (security mechanisms) und Sicherheitsdiensten (security services) vorgenommen [32], [10]: Unter Sicherheitsmechanismen werden z. B. Verschlüsslung oder Signierung von Nachrichten verstanden. Ein Sicherheitsdienst hingegen wird mithilfe von Sicherheitsmechanismen implementiert. Ein Beispiel eines Sicherheitsdienstes ist ein Authentifizierungs- und Autorisierungsdienst, wie z. B. ein Kerberos-System. Die Unterscheidung in Sicherheitsmechanismen und Sicherheitsdienste ist jedoch häufig schwer vorzunehmen, weshalb hier darauf verzichtet wird.

Verwandte Begriffe:
Sicherheitsmaßnahmen, Sicherheitsanforderungen, Sicherheitsrichtlinien

Beispiele:
Verschlüsselung mithilfe des Advanced Encryption Standard (AES) zur Wahrung der Vertraulichkeit. Message Authentication Codes (MAC) zur Wahrung der Integrität. Transport Layer Security (TLS) bzw. Secure Sockets Layer (SSL) zur Wahrung der Vertraulichkeit und Authentizität (also auch Integrität) von Client-Server-Kommunikation über TCP-Verbindungen, indem die Kommunikationspartner – mindestens aber Server – über Zertifikate authentifiziert und die Kommunikation dann verschlüsselt sowie mit MAC versehen werden [18], [8], [32]. Replikation zur Sicherstellung der Verfügbarkeit [34].

zu (22)

Erläuterung:
Die in einem System oder einer Komponente umzusetzenden Sicherheitsziele sowie die hieraus abgeleiteten Sicherheitsanforderungen und Maßnahmen ergeben sich grundsätzlich aus schützenswerten Gütern beteiligter Akteure, sowie aus gesetzlichen Vorgaben. Prinzipiell sind diese bei der Umsetzung jedes einzelnen konkreten Systems abzuwägen und zu prüfen. Da bei verschiedenen Systeme häufig jedoch gleiche oder ähnlichen Schutzziele ergeben (etwa die Vertraulichkeit personenbezogener Daten), können Sicherheitsanforderungen für artverwandte Systeme oder auch für verschiedene Systeme die in gemeinsamen Umgebungen betrieben werden (zusammen mit Maßnahmen-Empfehlungen oder -vorgaben) oft in einer Sicherheitsrichtlinie zusammengefasst werden. Bei der Umsetzung eines einzelnes System helfen diese Richtlinien dann bei der Aufstellung relevanter Anforderungen und Maßnahmen.

Sicherheitsrichtlinien können rechtliche Vorgaben behandeln, oder selbst auferlegte Anforderungen formulieren. Beispielsweise setzen im Bereich des Energiemarkt das „Schutzprofil für ein Smart Meter Gateway“ [13] so wie eine technische Richtlinie [14] gesetzliche Vorgaben aus dem Energiewirtschaftsgesetz [2] um. Andererseits gibt es in vielen Unternehmen selbst auferlegte Sicherheitsrichtlinien, beispielsweise Richtlinien für den Umgang mit Kundendaten, oder interne Richtlinien zum Betrieb und Entwicklung von Informationssystemen.

Weiterhin unterscheiden sich Sicherheitsrichtlinien in ihren Geltungsbereich. Das Schutzprofil für Smart Meter Gateways beschreibt beispielsweise die konkreten Anforderungen an Smart Meter Gateways, also Geräten zur Übermittlung von Energieverbrauchs und -Steuerungsdaten. Akteure, Güter etc. sind hier fest vorgegeben und beschrieben. Andere Richtlinien, beispielsweise die IT Grund-

schutzkataloge des BSI [4], sind prinzipiell auf Informationssysteme aller Art anwendbar, und beschreiben Sicherheitsanforderungen und Maßnahmen allgemeine Art.

zu (23)

Erläuterung:
Ein Sicherheitsvorfall kann sowohl durch einen Angriff ausgelöst werden als auch durch unbeabsichtigte Ereignisse entstehen. Ein Sicherheitsvorfall kann auch dann vorliegen, wenn die für ein System formulierten Sicherheitsziele nicht vollständig sind, oder wenn die formulierten Sicherheitsanforderungen zwar umgesetzt wurden, aber nicht ausreichend sind, um die gesteckten Sicherheitsziele umzusetzen

Verwandte Begriffe:
Fehler, Security breach, Security incident

zu (24)

Erläuterung:
Die Begriffe Sicherheitsziel und Datenschutz-Schutzziel(e) können sich teilweise überschneiden.

Abgrenzung:
Der Begriff Sicherheitsziel ist ein Oberbegriff und bezieht sich allgemein auf Komponenten bzw. Systeme und deren zu schützende Güter. Der Begriff Datenschutz-Schutzziel bezieht sich deshalb konkret auf Datensicherheit/technischen Datenschutz.

Verwandte Begriffe:
Datenschutz-Schutzziel

Beispiele:
Vertraulichkeit, Authentizität, Integrität, Verfügbarkeit, Verlässlichkeit, Zurechenbarkeit (Accountability), Nichtabstreitbarkeit, Verbindlichkeit, Zugriffsschutz (vgl. [17]).

zu (25)

Erläuterung:

Komponenten können z. B. Ressourcen, Hardware- oder Softwareeinheiten sein, die selbst als (Teil-)Systeme aufgefasst werden können. Die Umgebung des Systems (z. B. Nutzer, Betreiber, Administratoren, physische Umgebung usw.) sollte für Sicherheitsbetrachtungen miteinbezogen werden. Die Systemgrenze beschreibt die Abgrenzung zwischen System und Umgebung.

Verwandte Begriffe:
Komponente (vgl. [17])

zu (26)

Erläuterung:
Die Transparenz von Erhebungs- und Verarbeitungsvorgängen ist eine grundlegende Voraussetzung, um das Recht auf informationelle Selbstbestimmung wahrnehmen zu können [28]. Eine wirksame Datenerhebung verlangt daher unter anderem die Unterrichtung über die Identität der verantwortlichen Stelle und den Zweck der Erhebung und Verarbeitung personenbezogener Daten eines Betroffenen[29]. Somit muss zum einen die Rechtsordnung als solche transparent gestaltet und zum anderen die individuelle Kenntnisnahme des Betroffenen über die Einzelumstände des Umgangs mit dessen personenbezogenen Daten ermöglicht werden. Konkrete gesetzliche Verankerungen finden sich daher in den Auskunfts- und Informationsrechten des Betroffenen (siehe hierzu §§ 4 Abs. 3, 4a Abs. 1, 19, 19a, 33, 34 BDSG).

Diskussion:
Problematisch an dieser Definition ist die Frage nach der Zumutbarkeit des Aufwands. Aus technischer Sicht stellt sich die Frage nach einem konkreten Maß zur Bestimmung des „zumutbaren Aufwands“. Aus rechtlicher Sicht ist hingegen anzumerken, dass es sich hierbei um einen unbestimmten Rechtsbegriff handelt, der in rechtlichen Normen dort verwendet wird, wo der Gesetzgeber eine dynamische Handhabung der rechtlichen Voraussetzungen (Tatbestandsseite) und der daran anknüpfenden Folgen (Rechtsfolgen-

seite) verlangt (vgl. [23]). Insbesondere im Verwaltungsrecht soll damit einer Behörde die Möglichkeit gegeben werden, selbst zu bestimmen, welche Voraussetzungen für den unbestimmten Rechtsbegriff erfüllt sein müssen [27]. Um diese Flexibilität und Dynamik der definitorischen Voraussetzungen beibehalten zu können, wurde daher im Ergebnis auf eine statische Definition des zumutbaren Aufwands verzichtet.

Beispiele:
Konkrete gesetzliche Verankerungen finden sich in den Auskunfts- und Informationsrechten des Betroffenen (siehe hierzu §§ 4 Abs. 3, 4a Abs. 1, 19, 19a, 33, 34 BDSG).

zu (27)

Erläuterung:
Verfügbarkeit wird häufig neben Verlässlichkeit (reliability) als ein Bestandteil oder Teilkonzept von Zuverlässigkeit (dependability) gesehen. Dies umfasst sowohl Aspekte von Security als auch von Safety, da eine Beeintrachtigung der Verfügbarkeit eines Systems z. B. durch Angriffe oder auch durch sonstige Systembeeinträchtigungen – Hardwaredefekte u. a. – verursacht werden kann [36], [10], [6]. Wir folgen bei unserer Definition dem Ansatz von C. Eckert [10] indem wir die berechtigte Inanspruchnahme der Funktionalität eines Systems von unberechtigter Inanspruchnahme unterscheiden. Dies soll z. B. geplante Einschränkungen der Verfügbarkeit ausnehmen.

Typische Kennzahlen, die im Zusammenhang von Verfügbarkeit genannt werden, sind [36], [10]: Mean time to failure (MTTF), Mean time to repair (MTTR), Mean time between failures (MTBF), Verfügbarkeit = MTTF/MTBF = MTTF/(MTTF+MTTR).

Abgrenzung:
Wir definieren Verfügbarkeit bewusst vornehmlich aus der Sicht von Security und nicht aus der Sicht von Safety.

Diskussion:
Eine Unterscheidung in Aspekte von Security und Safety ist bei Verfügbarkeit häufig schwierig vorzunehmen: Während z. B. bei Betrachtung der Ursachen einer Beeinträchtigung der Verfügbarkeit oft eine Unterscheidung möglich ist – wenn manchmal auch erst nach einer genauen Analyse der Ursachen durch forensische Maßnahmen –, ist aus der Perspektive eines Nutzers eines Systems eine solche Unterscheidung oft nicht möglich. Wenn das System nicht (oder nicht schnell genug) antwortet, kann es nicht genutzt werden. Aus diesem Grund gibt es z. B. auch Ansätze, die die Antwortzeit eines Systems als Kennzahl für Verfügbarkeit ansehen (siehe z. B. auch [11], [6]).

Im Landesdatenschutzgesetz des Landes Schleswig Holstein wird ebenfalls eine weitere Definition von Verfügbarkeit verwendet [1]: „Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz [...] ist durch technische und organisatorische Maßnahmen sicherzustellen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. Sie müssen gewährleisten, dass [...] [unter anderem] Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können (Verfügbarkeit) [...]“.

Verwandte Begriffe:
Security, Safety, Zuverlässigkeit, Verlässlichkeit, Ausfallsicherheit, Funktionsfähigkeit

zu (28)

Erläuterung:
Aus juristischer Sicht meint Vertraulichkeit, dass nur befugt (autorisiert) auf Daten und Verfahren zugegriffen werden kann (§ 5 Abs. 1 Satz 2 Nr. 3 LDSG-SH), mithin also Informationen eines IT-Systems nur Befugten (Autorisierten) zugänglich sind [7]. Aus technischer Sicht definiert Vertraulichkeit genau das, was unter

Zugriffsschutz verstanden wird. Der Unterschied zwischen diesen Begriffen besteht darin, dass Vertraulichkeit nur auf den lesenden Zugriff beschränkt ist, wohingegen Zugriffsschutz zusätzlich manipulativen Zugriff abdeckt. Wie stark hingegen der Vertraulichkeitsbegriff zu gewichten ist, hängt davon ab, welche Informationsgewinnung autorisiert werden kann. Es stellt sich dann beispielsweise die Frage, ob eine Information über die Länge des Chiffrats erlangt werden darf.

Diskussion:
Nach Jürjens [20] existiert eine Definition, die einen Angreifer und dessen Fähigkeiten direkt einbezieht. Danach wird ein Datum d geleakt, wenn ein Angreifer existiert, der Datum d initial nicht kennt, und eine Eingabesequenz an das System existiert, so dass nach der Ausführung der Sequenz durch das System im Beisein des Angreifers, dieser das Datum d kennt. Ein System, das Datum d nicht leakt erhält die Vertraulichkeit von Datum d.

Ein Alternativvorschlag nach Eckert [10] besagt, dass „das System (...) Vertraulichkeit gewährleistet, wenn es keine unautorisierte Informationsgewinnung ermöglicht."

Diese Definition beschränkt sich nicht auf den Zugang zu Daten o. ä., sondern bezieht explizit auch die Verarbeitung von Daten durch einen Angreifer ein. Außerdem wird nach dieser Definition die Unmöglichkeit der Informationsgewinnung gefordert. Die Möglichkeit, Schwachpunkte auszunutzen, wird also auf das Angreifermodell ausgelagert. Diese Definition ist technisch auf verschiedenste Arten verfeinerbar, so dass verschiedene Methoden zur Durchsetzung, zum Nachweis oder zur Analyse realisiert werden können. Die Definition nach Eckert birgt jedoch gewisse Unsicherheiten bezüglich des Begriffs Information. Daher könnte wie bei dem Begriff der Integrität zwischen starker und schwacher Vertraulichkeit unterschieden werden. Demzufolge würde ein System schwache Vertraulichkeit bewahren, wenn es keine unautorisierte

Datengewinnung ermöglicht. Starke Vertraulichkeit hingegen läge vor, wenn es keine unautorisierte Informationsgewinnung ermöglicht.

Synonyme:
Geheimhaltung

zu (29)

Erläuterung:
Die Definition wurde explizit auf betrachtete Angreifer eingeschränkt, da ein allmächtiger Angreifer jede Bedrohung zu realisieren vermag. Ein Angriff kann realisiert werden, wenn gar kein Schutz existiert oder ein existenter Schutz den Angriff nicht wirksam verhindern kann. Wirksamer Schutz kann dabei erreicht werden, wenn der Aufwand diesen/ihn zu umgehen höher ist als der Nutzen.

Diskussion:
Verwundbarkeit als rechtliche Kategorie ist nicht geläufig.
Andere Definitionen:
Anderson: „A vulnerability is a property of a system or its environment which, in conjunction with an internal or external threat, can lead to a security failure, which is a breach of the system's security policy. By security policy I will mean a succinct statement of a system's protection strategy (for example, each credit must be matched by an equal and opposite debit, and all transactions over 1,000 Dollars must be authorized by two managers)." [6]

The Open Web Application Security Project (OWASP): „A vulnerability is a hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application. Stakeholders include the application owner, application users, and other entities that rely on the application. The term vulnerability is often used very loosely. However, here we need to distinguish threats, attacks, and countermeasures." [35]

Eckert: „Unter einer Schwachstelle eines Systems verstehen wir eine Schwäche eines Systems oder einen Punkt, an dem das System verwundbar werden kann. Eine Verwundbarkeit ist eine Schwachstelle, über die die Sicherheitsdienste des Systems umgangen, getäuscht oder unautorisiert modifiziert werden können.“ [10]

Synonyme:
Vulnerability

Verwandte Begriffe:
Angriff

zu (30)

Erläuterung:
Zugriffskontrolle als Verhinderung nicht-autorisierter Zugriffe ist ein Schutzmechanismus mit dem häufig Zugriffsschutz realisiert wird. Allerdings liegt dort der Fokus auf Ressourcen und es wird zunächst nicht das Schließen auf neue Informationen aus der Kombination erlangter Informationen betrachtet.

Zugriffsschutz beschäftigt sich nur mit dem unmittelbaren Zugriff auf Daten, Informationen und Ressourcen aber nicht damit, was mit diesen Daten gemacht werden kann (z. B. kollaborierende Angreifer, secret sharing).

Diskussion:
Andere Definition nach Anderson: „Access control [...] is to control which principals (persons, processes, machines, ...) have access to which resources in the system—which files they can read, which programs they can execute, how they share data with other principals, and so on.“ ([6, Kapitel 4.1, Seite 93])

Synonyme:
access control

Verwandte Begriffe:
Autorisierung, Autorisierungsverletzung

zu (31)

Erläuterung:
Zurechenbarkeit wird auch als Nachweisbarkeit (detectability) bezeichnet. Für die Umsetzung ist ein Identitätsmanagement bzw. eine Authentifizierung notwendig. Zurechenbarkeit zielt auf Verantwortung ab. Es geht also nicht direkt darum, zu wissen wer etwas getan hat, sondern wer dafür zuständig ist. Die Abgrenzung zur Nichtabstreitbarkeit besteht darin, dass Nichtabstreitbarkeit zum Ziel hat, eine Aktion und dessen Urheber nachweisbar zu machen. Zurechenbarkeit soll lediglich sicherstellen, dass der Verantwortliche für einen Vorgang für einen zu definierenden Akteur identifizierbar ist. Dies muss nicht unbedingt gegenüber unbeteiligten Dritten (z. B. einem Richter oder Notar) möglich sein.

Diskussion:
Wir haben Zurechenbarkeit nur noch für Vorgänge und nicht mehr für Dokumente definiert, da wir über Erstellungs- oder Änderungsvorgänge die Dokumente abdecken können. Wir haben Zurechenbarkeit nicht mehr gegenüber Dritten, sondern gegenüber einem festzulegendem Akteur definiert, da wir uns nicht einig wurden, ob eine Definition, welche die Zuordnung gegenüber Dritten fordert, zu stark ist oder eine Definition, die eine Zuordnung gegenüber beliebigen Akteuren fordert, zu schwach ist.

Synonyme:
Nachweisbarkeit, Detectability

Verwandte Begriffe:
Nichtabstreitbarkeit

Beispiel:
In einem Versionierungssystem ist es sinnvoll, Zurechenbarkeit für Änderungen zu fordern, so dass klar ist, wer für entsprechende Änderungen an einem System verantwortlich ist.

Literatur

[1] *Landesdatenschutzgesetz Schleswig Holstein (LDSG SH), §5, Abs. 1.*

[2] *Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz - EnWG).* 2005.

[3] *Duden – Deutsches Universalwörterbuch.* Bibliographisches Institut, Mannheim, 6 edition, 10 2007.

[4] *IT-Grundschutz-Kataloge.* 2011.

[5] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing v3.0. `https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf`, 2011.

[6] Ross Anderson. *Security Engineering: A guide to building dependable distributed systems.* Wiley, 2nd ed. edition, 2008.

[7] Mark Bedner and Tobias Ackermann. *Schutzziele der IT-sicherheit*, volume 34. Springer, 2010.

[8] Roland Bless, Stefan Mink, Michael Conrad, Kendy Kutzner, Erik-Oliver Blaß, Hans-Joachim Hof, and Marcus Schöller. *Sichere Netzwerkkommunikation: Grundlagen, Protokolle und Architekturen.* X.systems.press. Springer, 2005.

[9] Danny Dolev and Andrew Yao. On the security of public key protocols. 1983.

[10] Claudia Eckert. *IT-Sicherheit : Konzepte - Verfahren - Protokolle.* Oldenbourg, München, 7., überarb. und erw. aufl. edition, 2012.

[11] Bundesamt für Sicherheit in der Informationstechnik. *Hochverfügbarkeit eine herausfordernde Aufgabenstellung für ein professionelles IT-Service Management.* Abrufdatum: 2013-07-05.

[12] Bundesamt für Sicherheit in der Informationstechnik. *Common Criteria for Information Technology Security Evaluation - Part*

1: Introduction and general model. Version 3.1 revision 4 edition, 09 2012.

[13] Bundesamtes für Sicherheit in der Informationstechnik. Schutzprofil für ein smart meter gateway (bsi-cc-pp-0073). 2013.

[14] Bundesamtes für Sicherheit in der Informationstechnik. Technische richtlinie bsi (tr-03109). 2013.

[15] Peter Gola, Christoph Klug, Barbara Körffer, and Rudolf Schomerus. Bundesdatenschutzgesetz. `http://beck-online.beck.de/?vpath=bibdata/komm/GolaSchomerusKoBDSG%5F11/cont/GolaSchomerusKoBDSG.htm`, 2012.

[16] The Open Group. Risk taxonomy. Technical report.

[17] Charles B Haley, Robin Laney, Jonathan D Moffett, and Bashar Nuseibeh. Security requirements engineering: A framework for representation and analysis. *Software Engineering, IEEE Transactions on*, 34(1):133–153, 2008.

[18] Internet Engineering Task Force (IETF). The transport layer security (tls) protocol version 1.2.

[19] International Telecommunication Union (ITU). Recommendation x.800 - security architecture for open systems interconnection for ccitt applications. `http://www.itu.int/rec/T-REC-X.800-199103-I/en`, 03 1991.

[20] J. Jürjens. *Secure Systems Development with UML.* Springer, 2005.

[21] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography: Principles and Protocols.* Chapman and Hall/CRC Cryptography and Network Security Series, 1. ed. edition, 2007.

[22] P. Kruchten, H. Obbink, and J. Stafford. The past, present, and future for software architecture. *Software, IEEE*, 23(2):22–30, 2006.

[23] Hartmut Maurer. *Allgemeines Verwaltungsrecht.* 18. Auflage 2011. § 7 Rn. 26 ff.

[24] S.J. Murdoch, S. Drimer, R. Anderson, and M. Bond. Chip and pin is broken. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 433–446, 2010.

[25] NIST National Institute of Standards and Technology. Guide for conducting risk assessments. `http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf`, 2012.

[26] Andreas Pfitzmann and Marit Köhntopp. Anonymity, unobservability, and pseudonymity—a proposal for terminology. In *Designing privacy enhancing technologies*, pages 1–9. Springer, 2001.

[27] Posser/Wolff (Hrsg.). Beck'scher online-kommentar zur verwaltungsgerichtsordnung (vwgo), stand 1.4.2013. 2013. § 114 Rn. 32 f.

[28] Alexander Rossnagel. *Handbuch Datenschutzrecht: die neuen Grundlagen für Wirtschaft und Verwaltung.* Verlag CH Beck, 2003. Kap. 2.5 Rn. 33.

[29] Martin Rost and Kirsten Bock. Privacy by design und die neuen schutzziele. *Datenschutz und Datensicherheit-DuD*, 35(1):30–35, 2011.

[30] Martin Rost and Andreas Pfitzmann. Datenschutzschutzziele—revisited. *Datenschutz und Datensicherheit-DuD*, 33(6):353–358, 2009.

[31] William Stallings. *Data and Computer Communications.* Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 8th ed. edition, 2006.

[32] William Stallings. *Cryptography and Network Security.* Pearson, New York, NY, USA, 2011.

[33] Clemens Szyperski. *Component Software: Beyond Object-Oriented Programming.* Addison-Wesley Professional, 2nd edition, 2011.

[34] Andrew S. Tanenbaum and Maarten van Steen. *Distributed systems : Principles and Paradigms*. Pearson, Prentice Hall, Upper Saddle River, NJ, 2nd ed. edition, 2007.

[35] The Open Web Application Security Project. Owasp website. `http://www.owasp.org`, 2013. abgerufen am 1. April 2013.

[36] Maria Toeroe and Francis Tam. Service availability: Principles and practices. 2012.

[37] Wikipedia. It-risk. `http://en.wikipedia.org/wiki/IT_risk`, 2013.

[38] Wikipedia. Risk management. `http://en.wikipedia.org/wiki/Risk_management`, 2013.

[39] Gesetz zur digitalen Signatur. Signaturgesetz–sigg, 2001.