Modul 2: Schutzziele

Verfügbarkeit, Auffindbarkeit, Vertraulichkeit, Verdecktheit, Integrität, Zurechenbarkeit, Verbindlichkeit, Ermittelbarkeit, Anonymität, Unbeobachtbarkeit, Unverkettbarkeit, Transparenz, Intervenierbarkeit, Abstreitbarkeit,

Pseudonymität, Nicht-Verfolgbarkeit, Authentizität, Beherrschbarkeit, Revisionsfähigkeit, Finalität, Nicht-Vermehrbarkeit

Mehrseitige Sicherheit

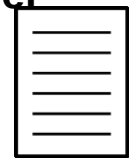
Ausgangssituation - Problemstellung

- Jeder Beteiligte hat seine individuellen Schutzziele.
- Die Schutzziele eines Beteiligten können je nach Situation unterschiedliche Bedeutung haben.
- Jeder Beteiligte kann und soll seine Interessen formulieren.
- Formuliert man die Schutzziele, so zeigen sich möglicherweise sogar gegensätzliche, unvereinbare Interessen.
- Konflikte werden erkannt und Lösungen können ausgehandelt werden.
- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen durchsetzen.

Definition

- Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte.

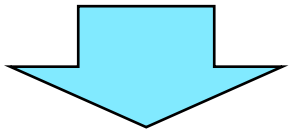
Quelle: A. Pfitzmann, A. Schill und A. Westfeld, Mehrseitige Sicherheit in offenen Netzen, Vieweg Verlagsgesellschaft, 2000



Mehrseitige Sicherheit und die Struktur der Schutzziele

Folgerungen aus dem Prinzip der mehrseitigen Sicherheit:

- **Schutzziele zu formulieren und dann zu fordern, dass alle eingehalten werden: So einfach geht es nicht!**
- **Schutzziele stehen in einem Spannungsverhältnis, ja sogar Widerspruchsverhältnis zueinander und müssen durch sorgfältige Abwägung in ein ausgewogenes Verhältnis gebracht werden.**
- **Damit diese Schutzziele sorgfältig abgewogen werden können, ist ein genaues Verständnis der Schutzziele sowie ihrer Beziehung zueinander notwendig.**
- **Das Abwägen der Schutzziele ist eine gesellschaftliche, soziale und rechtliche Fragestellung. Erst in einem zweiten Schritt erfolgt die technische und organisatorische Umsetzung der Schutzziele.**



Systematik der Datenschutzziele nach Martin Rost / Kirsten Bock

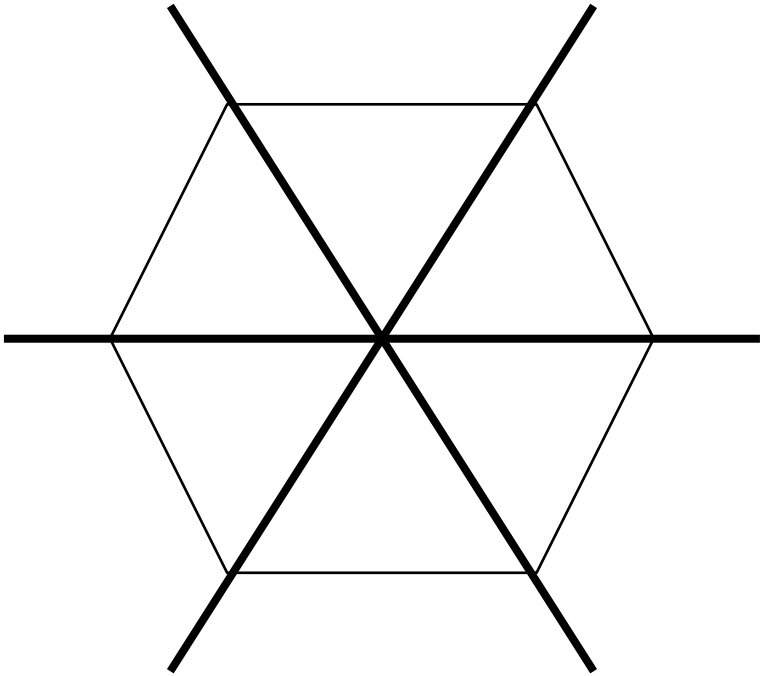
Struktur der Schutzziele nach Martin Rost / Kirsten Bock

Sechs elementare Schutzziele:

- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Transparenz
- Intervenierbarkeit
- Nichtverkettbarkeit

Grundlage bzgl. Schutzziele für das Landesdatenschutzgesetz Schleswig-Holstein 2012

http://www.datenschutzgeschichte.de/pub/privacy/DuD2011-01_RostBock_PbD_NSZ.html



Rost M., Bock K.: *Privacy By Design und die Neuen Schutzziele*; in: DuD, Jg. 35., Heft 1, S. 30-35, Januar 2011

Zusatzziel:

- Datenvermeidung

Verfügbarkeit (availability)

Definition

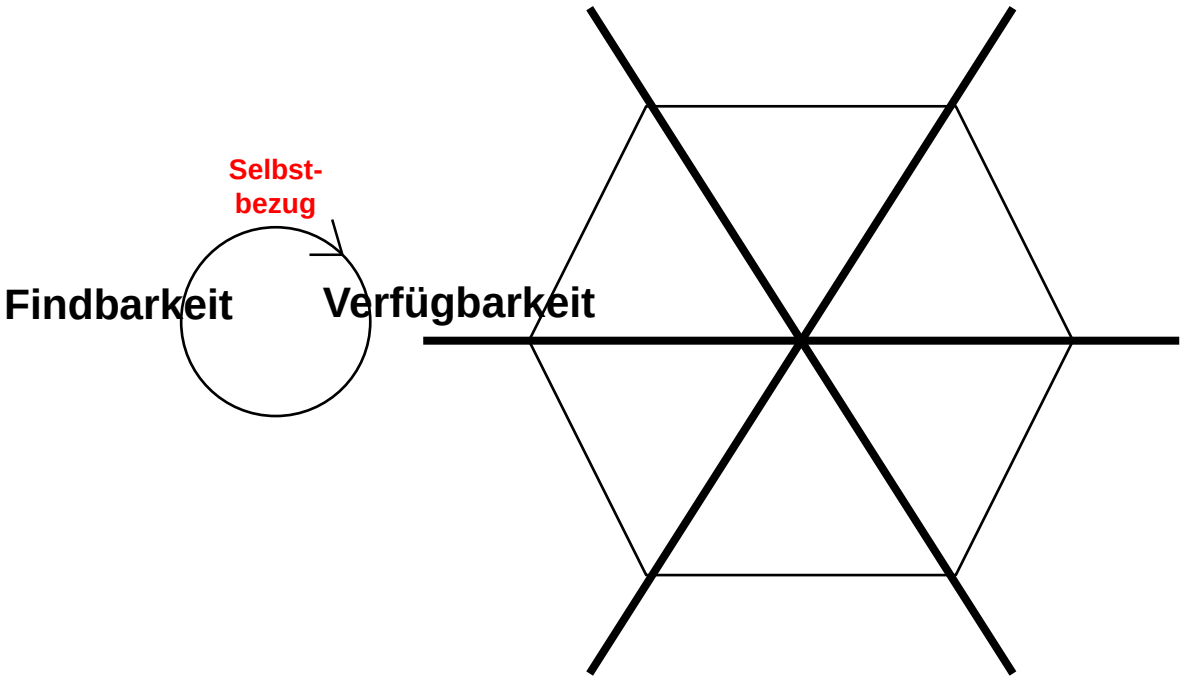
- Die Systeme sind jederzeit betriebsbereit und auf die Ressourcen (z.B. Daten, Funktionen) kann wie vorgesehen zugegriffen werden.
- Wichtig in diesem Zusammenhang ist es, dass die Verfügbarkeit selbst auch praktisch (tatsächlich) gesichert ist.
  „Die Verfügbarkeit muss tatsächlich verfügbar sein“
  Dies führt zum Begriff der Auffindbarkeit.
- Maßzahl für Verfügbarkeit: 99,x %

Beispiel und Umsetzung

- Sicherheitskopien, hochverfügbare Systeme, redundante Auslegung, redundante Weg, vernetzte Kommunikationsstrukturen
- Directory für Auffindbarkeit

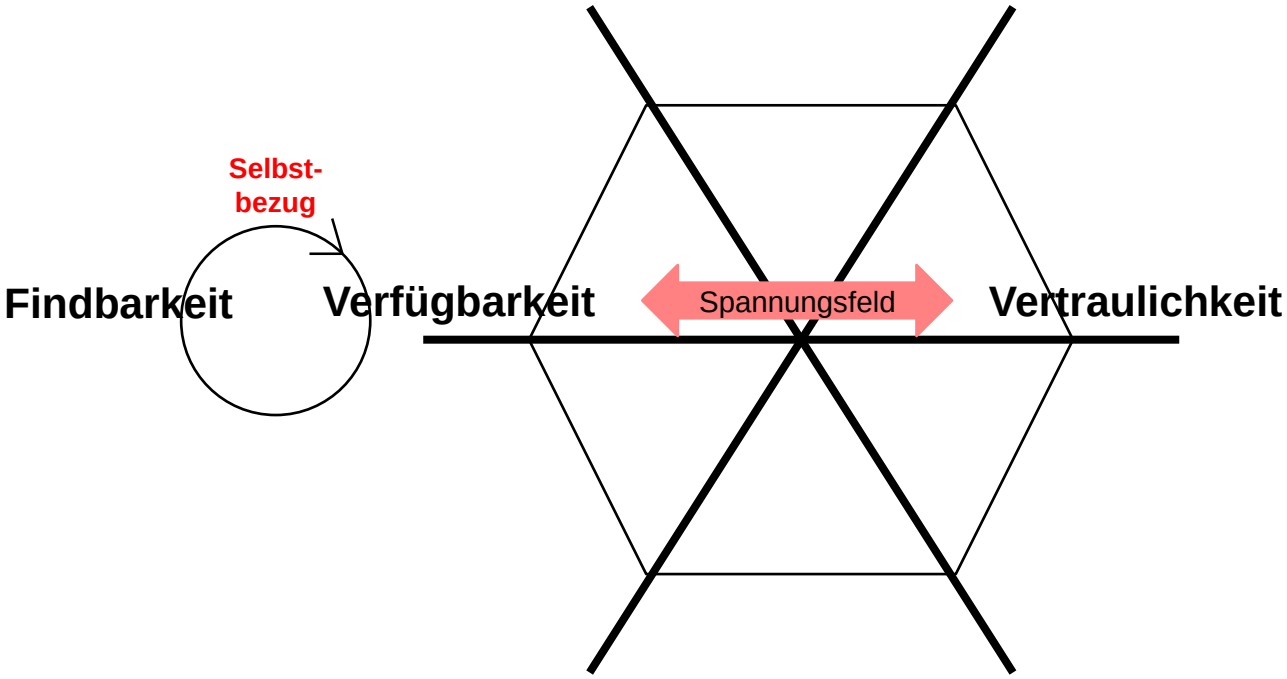
Quelle: Bedner, Mark / Ackermann, Tobias, 2010: **Schutzziele der IT-Sicherheit**, in: DuD- Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5: 323-328

Struktur der Schutzziele nach Martin Rost / Kirsten Bock



Rost M., Bock K.: *Privacy By Design und die Neuen Schutzziele*; in: DuD, Jg. 35., Heft 1, S. 30-35, Januar 2011
Rost M., Pfitzmann Andreas: *Datenschutz-Schutzziele - revisited*; in: DuD, Jg. 33., Heft 6, S. 353-358, Juli 2009

Struktur der Schutzziele nach Martin Rost / Kirsten Bock



Rost M., Bock K.: *Privacy By Design und die Neuen Schutzziele*; in: DuD, Jg. 35., Heft 1, S. 30-35, Januar 2011
Rost M., Pfitzmann Andreas: *Datenschutz-Schutzziele - revisited*; in: DuD, Jg. 33., Heft 6, S. 353-358, Juli 2009

Vertraulichkeit (confidentiality)

Definition

Schutz vor unbefugter Preisgabe von Informationen.

Information in Systemen und Netzen dürfen nur Befugten in der zulässigen Weise zugänglich sein (und keine unbeteiligten Dritten).

Beispiel

- **Verschlüsselung der E-Mail.**

Umsetzung

- **Verschlüsselungstechniken**
- **Zugriffsschutz**
- **Natürlich auch banales Abschließen der Räume**

Quelle: Bedner, Mark / Ackermann, Tobias, 2010: Schutzziele der IT-Sicherheit, in: DuD- Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5: 323-328

Verdecktheit (covertness, obscurity)

Definition

Die Vertraulichkeit selbst soll vertraulich behandelt werden („*Selbstbezug*“). Die vertrauliche Information selbst soll versteckt werden.

Es soll also eine verdeckte Übertragung von vertraulichen Daten stattfinden.

Beispiel

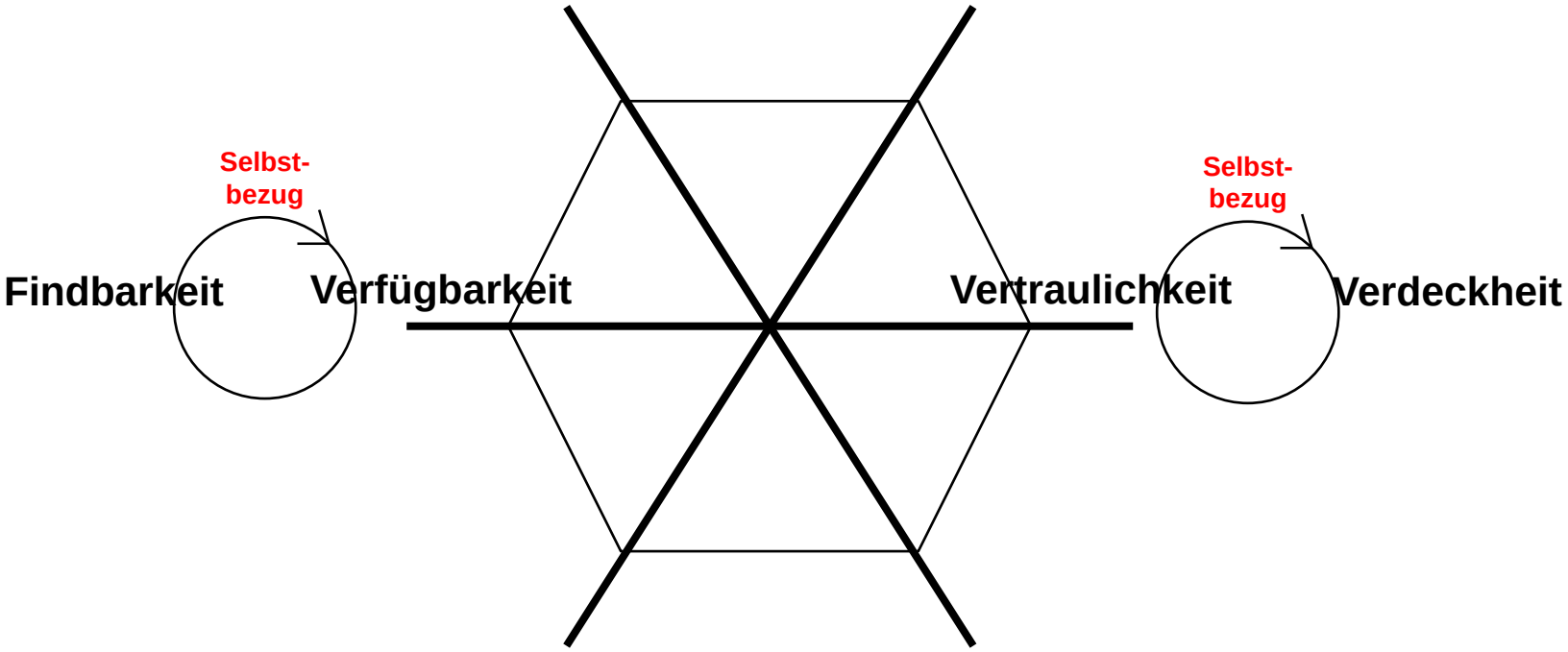
- **Steganografie**

Umsetzung

- **Verstecken eines Truecrypt Containers**
- **Tarnen und Täuschen (Artikel iX *08/2013,* http://heise.de/-1919755)**

Quelle: A. Pfitzmann, A. Schill und A. Westfeld, Mehrseitige Sicherheit in offenen Netzen, Vieweg Verlagsgesellschaft, 2000

Struktur der Schutzziele nach Martin Rost / Kirsten Bock



Rost M., Bock K.: *Privacy By Design und die Neuen Schutzziele*; in: DuD, Jg. 35., Heft 1, S. 30-35, Januar 2011
Rost M., Pfitzmann Andreas: *Datenschutz-Schutzziele - revisited*; in: DuD, Jg. 33., Heft 6, S. 353-358, Juli 2009

Integrität

Definition

Datenintegrität bedeutet die Vollständigkeit und Korrektheit der Daten. Vollständig heißt, dass alle Teile der Information verfügbar sind, korrekt heißt, dass die Daten den bezeichneten Sachverhalt unverfälscht wiedergeben.

Systemintegrität bedeutet die korrekte Funktionsweise des Systems. Normales versus anormales Verhalten.

Zeitliche Integrität bedeutet die genaue Einhaltung einer gewissen zeitlichen Abfolge (Börsenkurssystem)

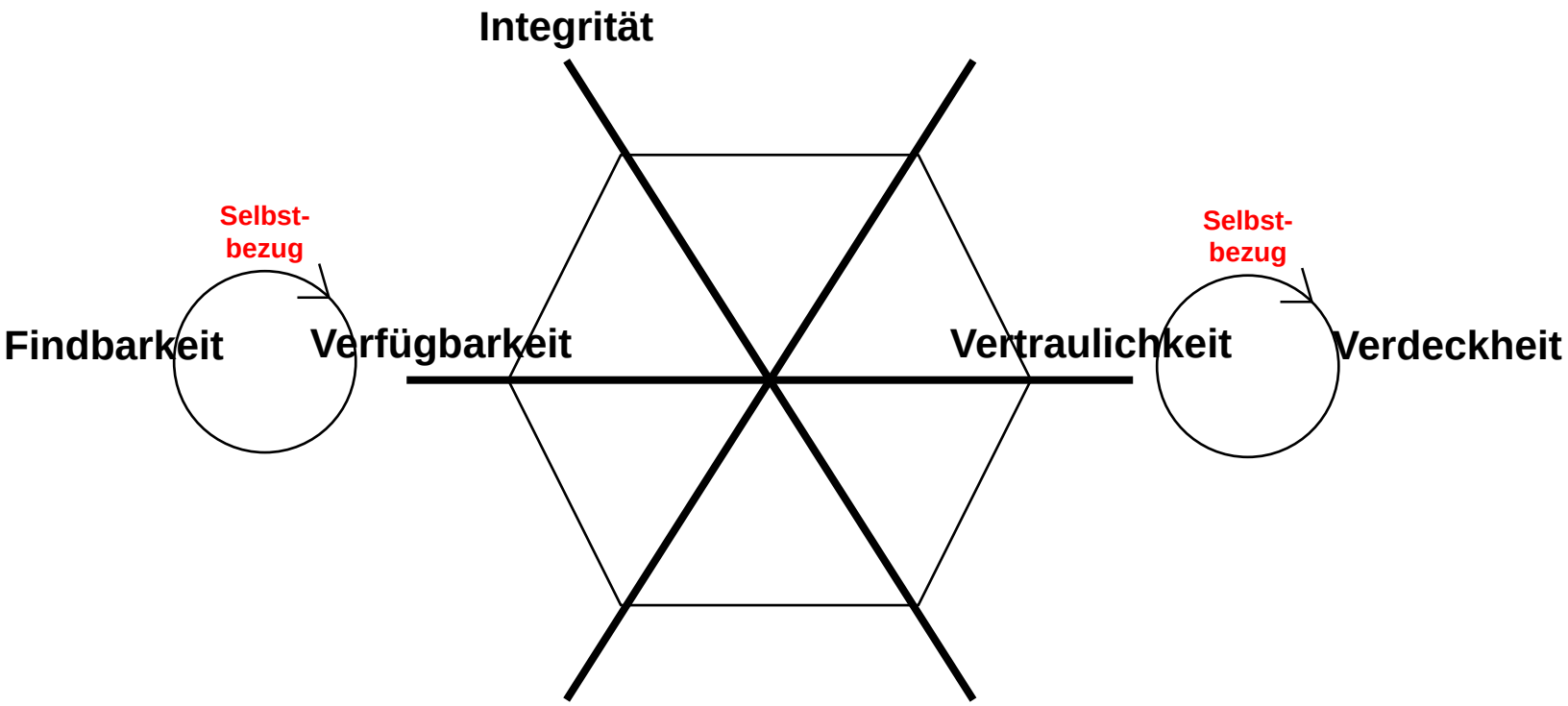
Manipulationen dürfen nicht unbemerkt bleiben.

Beispiel + Umsetzung

- **Hashfunktion (Datenintegrität)**
- **Zeitstempel (Zeitintegrität)**

Quelle: Bedner, Mark / Ackermann, Tobias, 2010: **Schutzziele der IT-Sicherheit**, in: DuD- Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5: 323-328

Struktur der Schutzziele nach Martin Rost / Kirsten Bock



Rost M., Bock K.: *Privacy By Design und die Neuen Schutzziele*; in: DuD, Jg. 35., Heft 1, S. 30-35, Januar 2011
Rost M., Pfitzmann Andreas: *Datenschutz-Schutzziele - revisited*; in: DuD, Jg. 33., Heft 6, S. 353-358, Juli 2009

Umfeldschutzziel (bzgl. Integrität): Zurechenbarkeit

Integrität bezieht sich auf den (technischen) Schutz von Inhalten (Inhaltsschutzziel). Entfalten die (technischen) Schutzziele im (menschlichen) Umfeld eine Wirkung, so kommt man zu Umfeldschutzzielen.

Die Integrität der Kommunikation soll überprüfbar werden. Hierzu müssen die Kommunikations- und Informationsteile aktiven Elementen (Personen, Rollen, Systemen) eindeutig zugerechnet werden können.

Definition

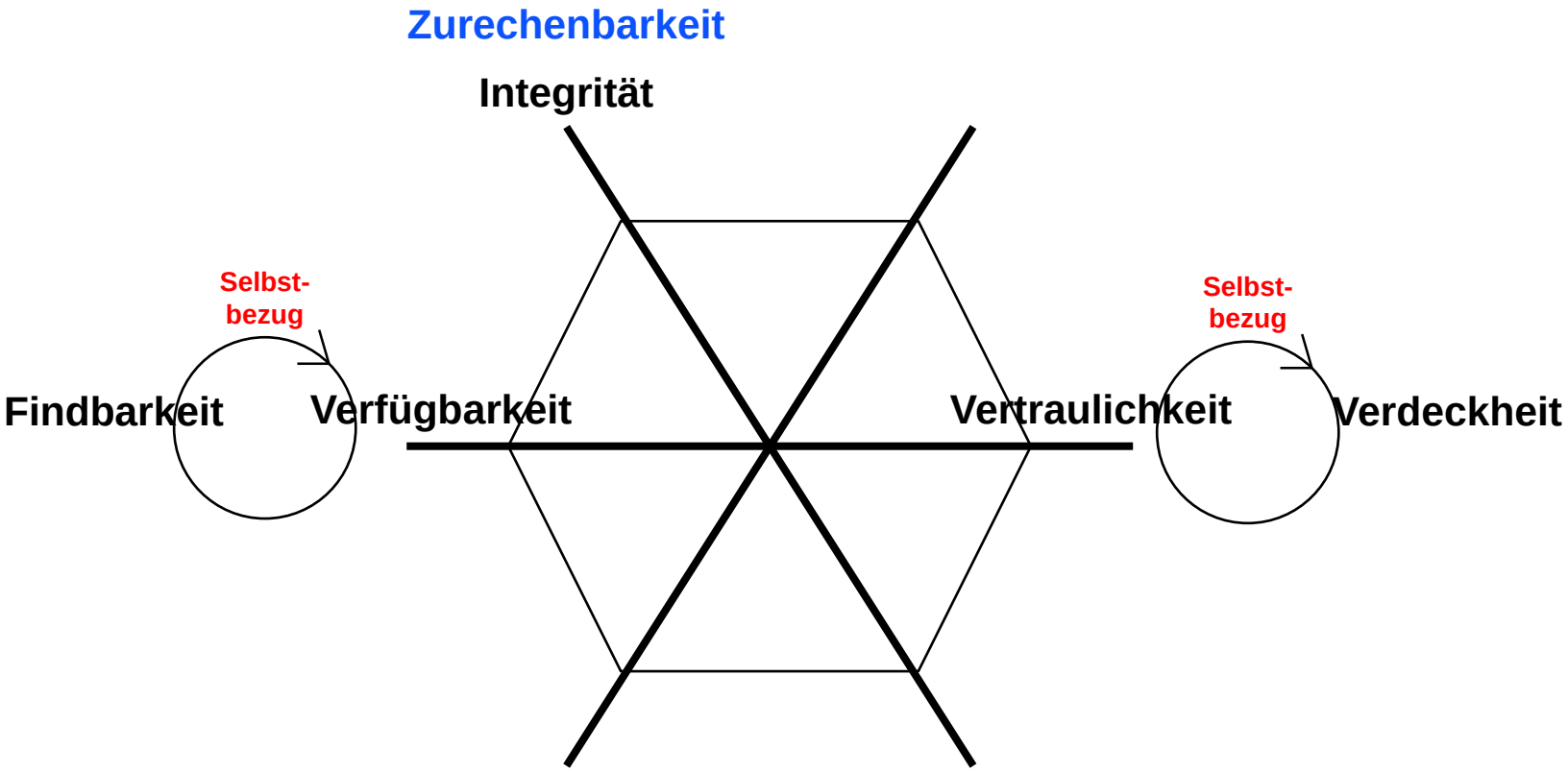
- **Aktionen (z.B. Senden, Empfangen) sowie Informationen können einer auslösenden Instanz (Person oder System) zugeordnet werden.**
- **Sie wird auch als Nachweisbarkeit (detectability), Unleugbarkeit oder Nicht-Abstreitbarkeit (nonrepudiation) bezeichnet.**

Beispiel + Umsetzung

- **Protokollierung**
- **Digitale Signatur.**
- **Änderungen an einem IT-System müssen einem Admin zugeordnet werden können.**

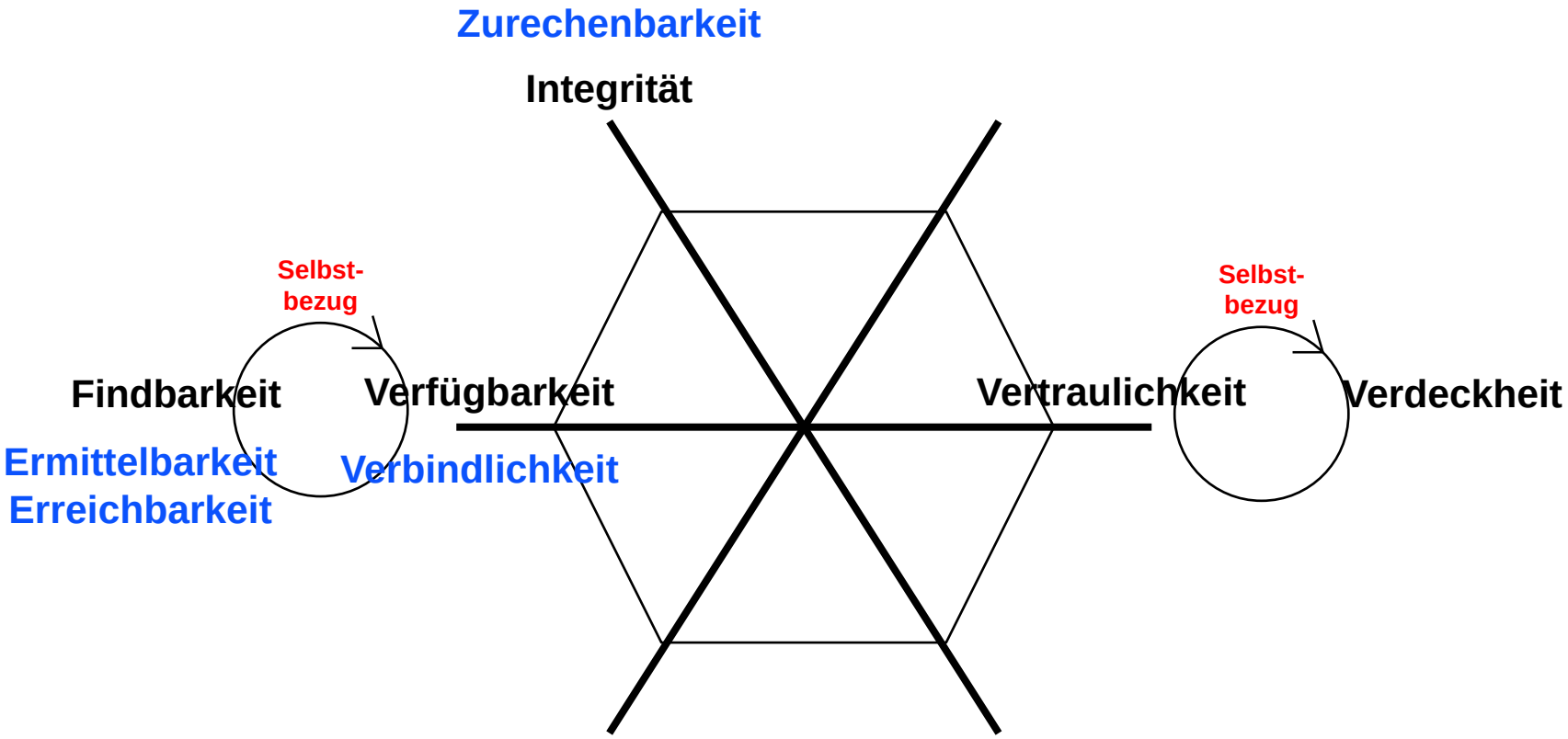
Quelle: Bedner, Mark / Ackermann, Tobias, 2010: **Schutzziele der IT-Sicherheit**, in: DuD- Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5: 323-328

Umfeldschutzziel (bzgl. Integrität): Zurechenbarkeit



Rost M., Bock K.: *Privacy By Design und die Neuen Schutzziele*; in: DuD, Jg. 35., Heft 1, S. 30-35, Januar 2011
Rost M., Pfitzmann Andreas: *Datenschutz-Schutzziele - revisited*; in: DuD, Jg. 33., Heft 6, S. 353-358, Juli 2009

Umfeldschutzziele (bzgl. Verfügbarkeit und Findbarkeit)



Rost M., Bock K.: *Privacy By Design und die Neuen Schutzziele*; in: DuD, Jg. 35., Heft 1, S. 30-35, Januar 2011
Rost M., Pfitzmann Andreas: *Datenschutz-Schutzziele - revisited*; in: DuD, Jg. 33., Heft 6, S. 353-358, Juli 2009

Umfeldschutzziel (bzgl. Vertraulichkeit): Anonymität

Definition

Nutzer können Ressourcen und Dienste benutzen, ohne ihre Identität in ihrem Umfeld zu offenbaren.

Selbst der Kommunikationspartner erfährt nicht die Identität.

Vollständige Anonymität, wenn bei Aktionen auch keine Pseudonyme bekannt werden.

Beispiel + Umsetzung

- **TOR**

Quelle: A. Pfitzmann, A. Schill und A. Westfeld, Mehrseitige Sicherheit in offenen Netzen, Vieweg Verlagsgesellschaft, 2000

Umfeldschutzziele (bzgl. Verdeckheit): Unbeobachtbarkeit

Definition

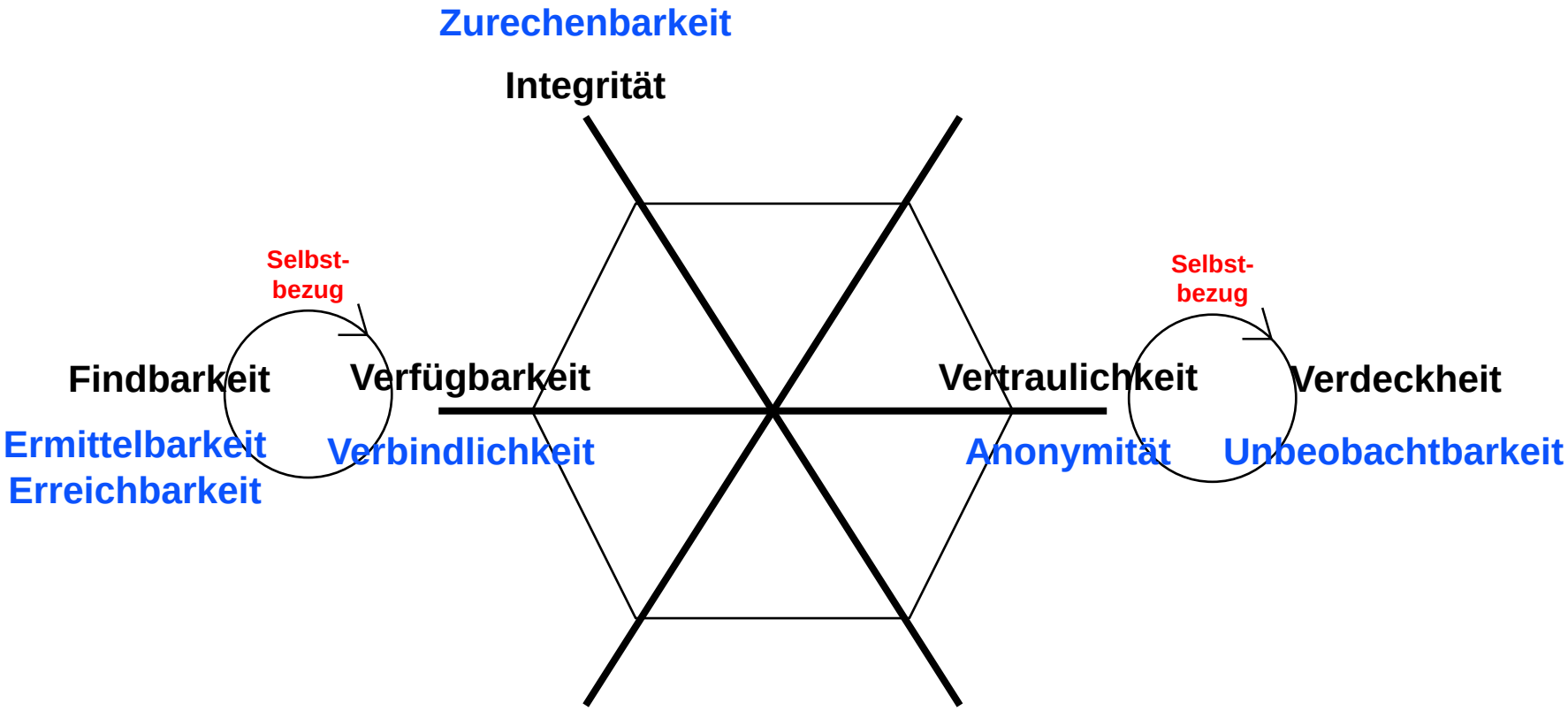
- **Nutzer können Ressourcen und Dienste benutzen, ohne dass andere dies beobachten können. Anonymität wird anonym ausgeführt.**
- **Dritte können weder das Senden noch den Erhalt von Nachrichten beobachten.**
- **Niemand außer den Kommunikationspartnern kann die Existenz einer Kommunikation erkennen.“**

Beispiel + Umsetzung

- **Geheimdienste**

Quelle: Bedner, Mark / Ackermann, Tobias, 2010: **Schutzziele der IT-Sicherheit**, in: DuD- Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5: 323-328

Umfeldschutzziel bzgl. Vertraulichkeit und Verdeckheit



Rost M., Bock K.: *Privacy By Design und die Neuen Schutzziele*; in: DuD, Jg. 35., Heft 1, S. 30-35, Januar 2011
Rost M., Pfitzmann Andreas: *Datenschutz-Schutzziele - revisited*; in: DuD, Jg. 33., Heft 6, S. 353-358, Juli 2009

Unverkettbarkeit

Definition

Mehrere kommunikative Ereignisse (etwa bei aufeinander folgende Abrufe von Informationen auf verschiedenen Webservern im Internet), sollen nicht miteinander in Verbindung gebracht werden können.

Daten sollen nur für den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können.

„Gegen“-Beispiele

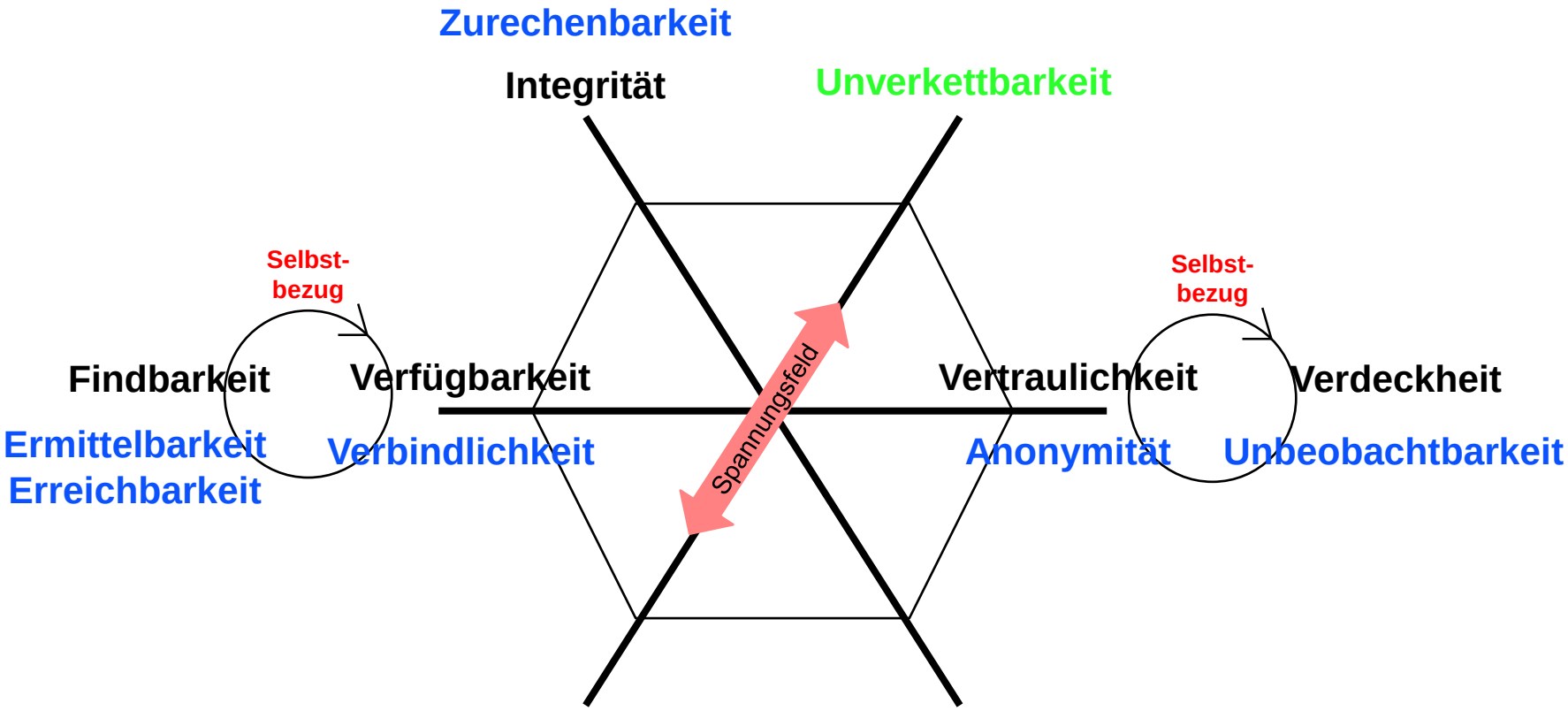
- **Cookies**
- **HTTP-Referrer**

Umsetzung

- **Prinzipien der Zweckbindung / Zwecktrennung (technisch und organisatorisch)**
- **Mix-Kanäle,** die die Zuordnung eines Pakets zu einem Nutzer verschleiern, indem sie nicht direkt adressiert vom Sender zum Empfänger, sondern „zwischenadressiert“ und verschlüsselt über mehrere Zwischenstationen übertragen werden („TOR-Netz“)

Quelle: Bedner, Mark / Ackermann, Tobias, 2010: **Schutzziele der IT-Sicherheit**, in: DuD- Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5: 323-328

Struktur der Schutzziele nach Martin Rost / Kirsten Bock



Rost M., Bock K.: *Privacy By Design und die Neuen Schutzziele*; in: DuD, Jg. 35., Heft 1, S. 30-35, Januar 2011
Rost M., Pfitzmann Andreas: *Datenschutz-Schutzziele - revisited*; in: DuD, Jg. 33., Heft 6, S. 353-358, Juli 2009

neue Schutzziele

Transparenz (transparency)

Definition

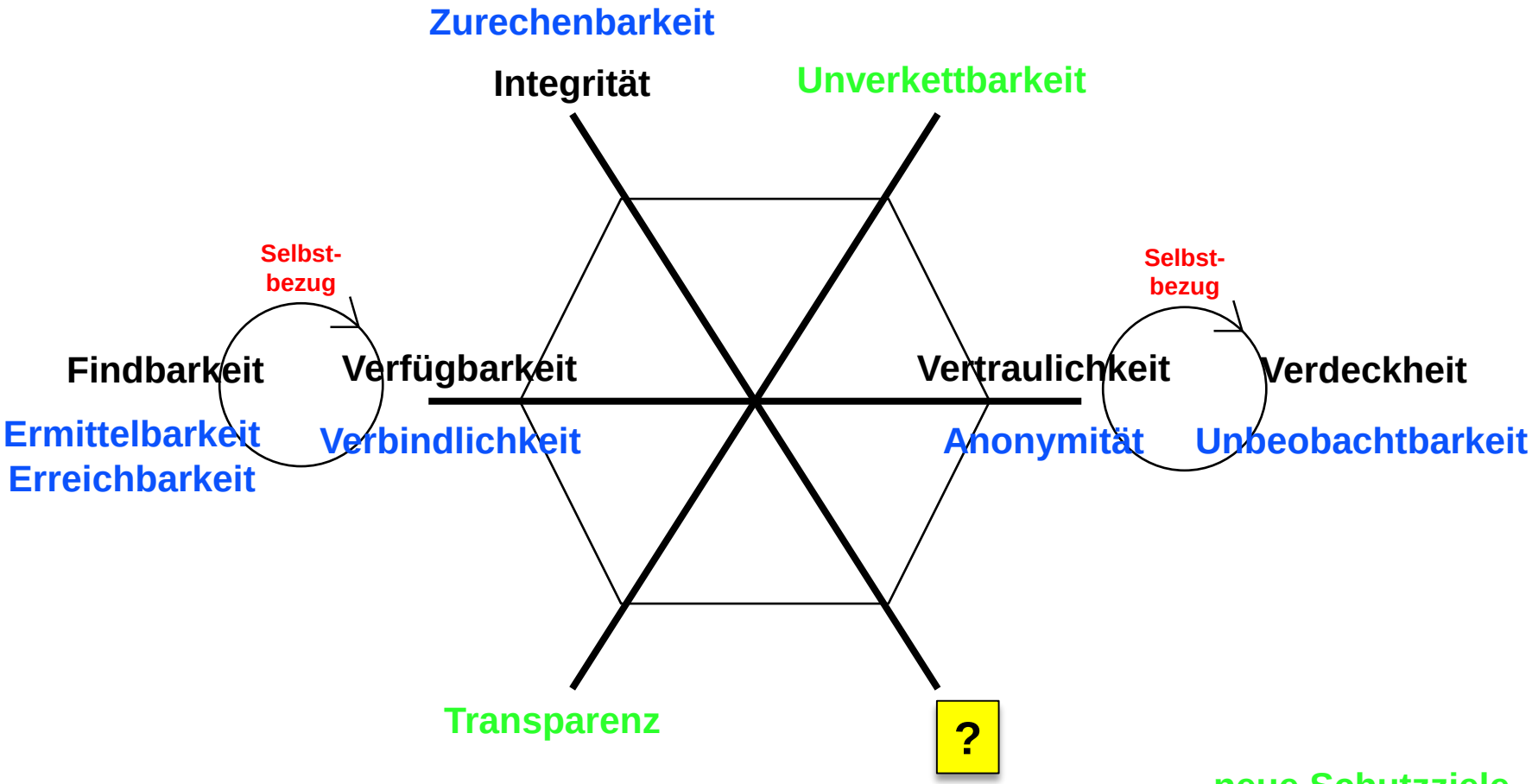
- **Der technische Aufbau von Systemen und Systemverbunden soll – soweit wie möglich – durchschaubar sein. Funktions- und Arbeitsweise sowie der Datenfluss nachvollziehbar, kontrollierbar und verständlich sein (Gegenteil einer „Blackbox“).**
- **Kommunikation in vernetzten Systmen soll einfach überprüft, nachvollzogen und kontrolliert werden können.**

Beispiel und Umsetzung

- **Open Source Software**
- **Protokollierung von Ereignissen, Web-Logs, Netzverkehr**
- **Werbenetzwerke**
- **„Google-Cloud“**
- **Facebook / WhatsApp**

Quelle: Bedner, Mark / Ackermann, Tobias, 2010: **Schutzziele der IT-Sicherheit**, in: DuD- Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5: 323-328

Struktur der Schutzziele nach Martin Rost / Kirsten Bock



Rost M., Bock K.: *Privacy By Design und die Neuen Schutzziele*; in: DuD, Jg. 35., Heft 1, S. 30-35, Januar 2011
Rost M., Pfitzmann Andreas: *Datenschutz-Schutzziele - revisited*; in: DuD, Jg. 33., Heft 6, S. 353-358, Juli 2009

Intervenierbarkeit

Definition

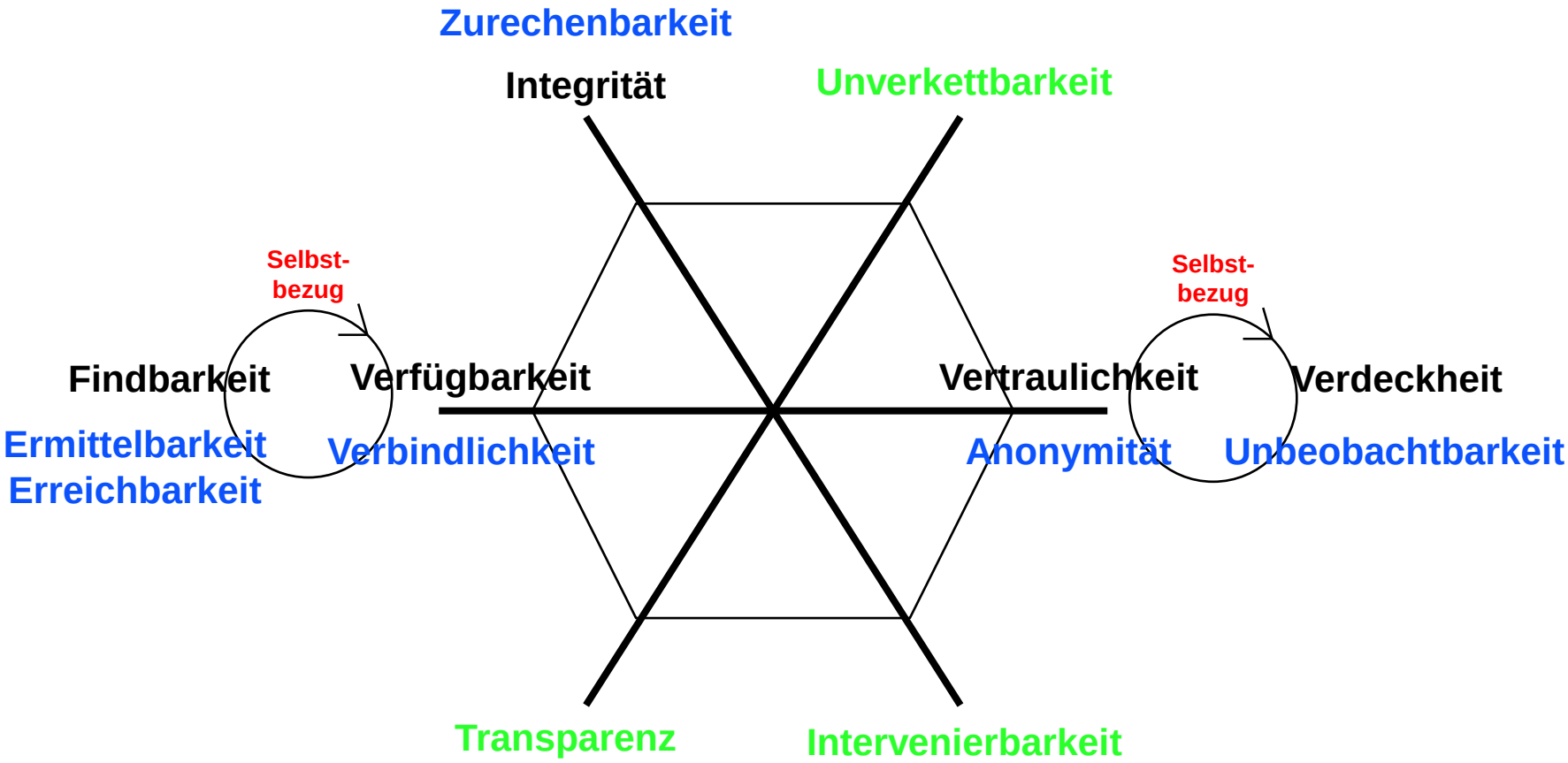
Der Benutzer hat die Möglichkeit auf verschiedenen Ebenen in das System einzugreifen, Änderungen vorzunehmen, Rechte wahrzunehmen.

Beispiel + Umsetzung

- **Datenfelder für freie Eingaben**
- **Rufnummernunterdrückung**
- **Deaktivierung von Funktionen**
- **Löschen von Profilen**

Quelle: Bedner, Mark / Ackermann, Tobias, 2010: **Schutzziele der IT-Sicherheit**, in: DuD- Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5: 323-328

Struktur der Schutzziele nach Martin Rost / Kirsten Bock



neue Schutzziele

Rost M., Bock K.: *Privacy By Design und die Neuen Schutzziele*; in: DuD, Jg. 35., Heft 1, S. 30-35, Januar 2011
Rost M., Pfitzmann Andreas: *Datenschutz-Schutzziele - revisited*; in: DuD, Jg. 33., Heft 6, S. 353-358, Juli 2009

Glaubhafte Abstreitbarkeit (plausible deniability)

Definition

Es soll glaubhaft möglich sein, einen technischen Sachverhalt abzustreiten.

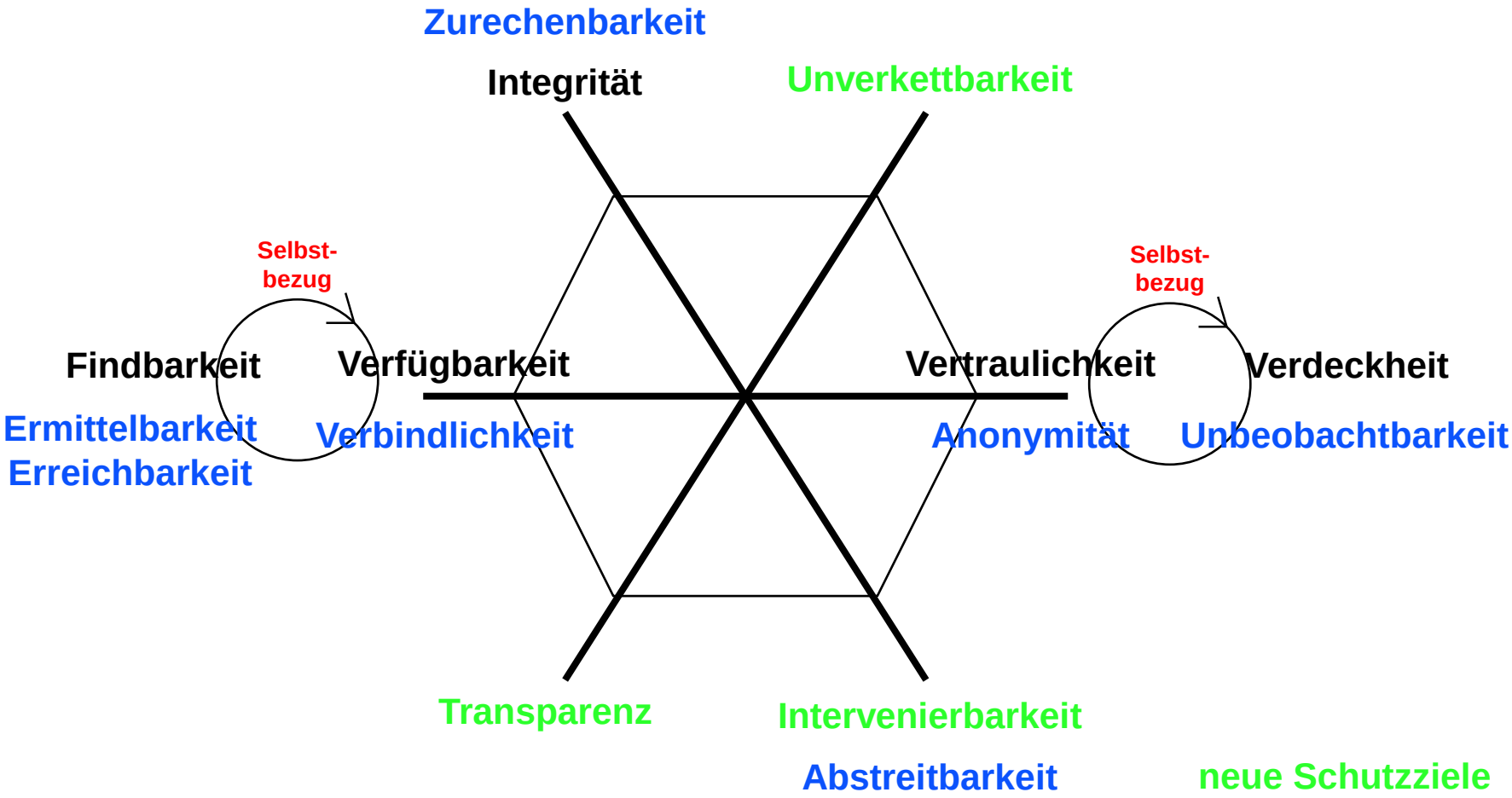
Im Zusammenhang hierzu stehen die Begriffe *Kontingenz* („Es ist anders, als es scheint“) und *Eingreifbarkeit*

Beispiel und Umsetzung

- **Truecrypt: Nachweis, dass überhaupt eine Verschlüsselung stattgefunden hat.**

Quelle: Bedner, Mark / Ackermann, Tobias, 2010: **Schutzziele der IT-Sicherheit**, in: DuD- Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5: 323-328

Umfeldschutzziele (bzgl. Intervenierbarkeit): Abstreitbarkeit



Rost M., Bock K.: *Privacy By Design und die Neuen Schutzziele*; in: DuD, Jg. 35., Heft 1, S. 30-35, Januar 2011
Rost M., Pfitzmann Andreas: *Datenschutz-Schutzziele - revisited*; in: DuD, Jg. 33., Heft 6, S. 353-358, Juli 2009

Umsetzung der Schutzziele

	Daten	Systeme
Verfügbarkeit **Findbarkeit** **Ermittelbarkeit** **Verbindlichkeit**	D 1.1 Einschränkung von Lösch-/Veränderungsrechten D 1.2 Schutz vor Schadsoftware D 1.3 Backup der Daten	S 1.1: Schutz vor Schadsoftware S 1.2: Backup von Konfigurationen und Software S 1.3: Hardwareredundanz S 1.4: Ausweichräume, und -Netze
Vertraulichkeit **Verdecktheit** **Anonymität** **Unbeobachtbarkeit**	D 2.1: Einschränkung von Leserechten (für Datenverarbeiter, ggf. durch den Nutzer selbst) D 2.2: Protokollierung lesender Zugriffe D 2.3: Verschlüsselung der Daten D 2.4: Ende-zu-Ende-Verschlüsselung	S 2.1: Einschränkung von lesenden Zugriffsrechten auf IT-Systeme (z. B. Netztrennung durch Sicherheitsgateways) S 2.2: Verschlüsselung auf Systemebene (Festplatten, Datenbank)
Integrität **Zurechenbarkeit**	D 3.1: Einschränkung von Schreib- und Änderungsrechten D 3.2: Protokollierung von schreibenden/ändernden Zugriffen D 3.3: Protokollierung geänderter Daten D 3.4: Nachberichtigung D 3.5: technische Integritätskontrollen (Signaturen/Hashes)	S 3.1: Einschränkung von schreibenden Zugriffen/Konfigurationmöglichkeiten auf IT-Systeme (z. B. Netztrennung durch Sicherheitsgateways) S 3.2 Schutz vor Schadsoftware S 3.3: Regelmäßige Integritätsprüfungen/Audits

aus: Probst Thomas: Generische Schutzmaßnahmen für Datenschutz-Schutzziele; in: DuD, Jg. 36, Heft 6, S. 439-444, Juni 2012

Umsetzung der Schutzziele

Nicht-Verkettbarkeit	D 4.1: Löschen, nach Wegfall der Erforderlichkeit; ggf. „Wipen“ D 4.2 Einschränkung von Verarbeitungs- / Nutzungs- / Übermittlungsrechten für einzelne Daten D 4.3: Kennzeichnung der Zwecke auf Ebene der Daten D 4.4: Einschränkung von identifizierenden Daten; Pseudonymisierung D 4.5: Anonymisierung von Daten	S 4.1: Kennzeichnung der Zwecke auf Ebene des Systeme S 4.2: Trennung von Datenbeständen S 4.3: Einschränkungen von Verarbeitungs-, Nutzungs- und Übermittlungsmöglichkeiten (Funktionalitätseinschränkung) S 4.4: Trennung auf Systemebene (Software, Hardware; Mandantenfähigkeit) S 4.5: Physikalische Trennung und unabhängige RZ-Betreiber
Transparenz	D 5.1: Dokumentation der Datenfelder einschließlich Erforderlichkeit D 5.2: Protokollierung von Datenverarbeitungen mit Schutzbedarf zunehmender Detaillierungsgrad und Speicherdauer D 5.3: Integritätsschutz der Protokolle (separater Protokollierungsserver)	S 5.1: Dokumentation der Systeme (Hardware, Software, Algorithmen) S 5.2: Protokollierung von Konfigurationsänderungen S 5.3: zunehmende Kontrolldichte bei höherem Schutzbedarfen; automatisiertes Monitoring
Intervenierbarkeit Kontingenz / Abstreitbarkeit	D 6.1: Schaffung notwendiger Datenfelder (z. B. für Gegendarstellungen) und Kennzeichnungen	S 6.1: Funktionalitäten in den Systemen für die Bearbeitung von Sperrungen, Widersprüchen, Beauskunftungen S 6.2: Funktionalitäten in den Systemen für die Umsetzung von weiteren Rechten Betroffener (z. B. Rufnummerunterdrückung, Pseudonyme Nutzungsmöglichkeit, etc.) S 6.3: Funktionalitäten für Betroffene, einzelne Betroffenenrechte direkt wahrzunehmen (z.B. Auskunftsportal, „Datenbrief“, Zusendung von Protokollen, eigene Änderungsmöglichkeiten) S 6.4: Steuerungsmöglichkeiten für einzelne Funktionen („Overrride“) bei automatisierten Einzelentscheidungen S 6.5: Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem

aus: Probst Thomas: Generische Schutzmaßnahmen für Datenschutz-Schutzziele; in: DuD, Jg. 36, Heft 6, S. 439-444, Juni 2012

Pseudonymität

Weitere Begriffe

Definition

Das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen (Alias) zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Schutz vor namentlicher Identifizierung.

Bezug zu einer bestimmten Person wird jedoch nicht endgültig aufgehoben, insbesondere wird die Zurechenbarkeit von Handlungen sichergestellt.

Beispiel + Umsetzung

- **Nutzername in einem Internetforum.**
- **Rollenpseudonyme (Admin, Prüfungsausschussvorsitzender).**

Quelle: Bedner, Mark / Ackermann, Tobias, 2010: **Schutzziele der IT-Sicherheit**, in: DuD- Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5: 323-328

Nicht-Verfolgbarkeit (untraceability)

Weitere Begriffe

Definition

- **Bezeichnet die Unmöglichkeit Handlungen oder Kommunikationsinhalte einer ganz bestimmten identifizierbaren Person nachverfolgen zu können.**
- **Hängt eng mit der Unverkettbarkeit und der Zurechenbarkeit.**

Beispiel + Umsetzung

- **Bezahlung mit Geldkarte.**

Quelle: Bedner, Mark / Ackermann, Tobias, 2010: **Schutzziele der IT-Sicherheit**, in: DuD- Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5: 323-328

Authentizität (authenticity)

Weitere Begriffe

Definition

- **Authentizität stellt durch geeignete Kontrollmaßnahmen sicher, dass Date… und Informationen wirklich aus der angegebenen Quelle stammen.**
- **Diese Identifikationsmöglichkeit muss über die Dauer einer Kommunikationsbeziehung erhalten bleiben.**
- **Bei der Authentisierung beweist der Benutzer dem System, dass er derjenige ist, für den er sich ausgibt (durch Abgleich von Credentials).**
  Auch umgekehrte/beidseitige Richtung möglich.

Beispiel und Umsetzung

- **Einloggen in ein System**
- **Zertifikat für eine Website**

Quelle: Bedner, Mark / Ackermann, Tobias, 2010: **Schutzziele der IT-Sicherheit**, in: DuD- Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5: 323-328

Beherrschbarkeit (controllability)

Weitere Begriffe

Definition

- **Beherrschbarkeit bedeutet, dass das IT-System kein „Eigenleben“ entwick und keine nichttolerierbaren Nebenwirkungen auftreten.**

Beispiel und Umsetzung

- **Falschalarm (als Gegenbeispiel)**

Quelle: Bedner, Mark / Ackermann, Tobias, 2010: **Schutzziele der IT-Sicherheit**, in: DuD- Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5: 323-328

Revisionsfähigkeit (reviewability)

Weitere Begriffe

Definition

- **Unterfall der Transparenz: Nachprüfbarkeit und Nachvollziehbarkeit**
- **Revisionsfähigkeit ist im Zusammenhang mit Verwaltungsvorschriften (z.B. im Umgang mit personenbezogenen Daten) von Bedeutung**

Beispiel und Umsetzung

- Protokollierung und Dokumentation von Handlungen

Quelle: Bedner, Mark / Ackermann, Tobias, 2010: **Schutzziele der IT-Sicherheit**, in: DuD- Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5: 323-328

Weitere Begriffe

Finalität

Definition

- **Wird vor allem in Bezug auf Zahlung verwendet:**
  Wenn eine Zahlungstransaktion angestoßen worden ist, so soll auch die effektive Durchführung des Zahlungsvorgangs sichergestellt sein (Schutz vor Zahlungsausfällen)

Beispiel

- **Eigenschaft elektronischer Zahlungssysteme**
- **Bestellung in einem Online-Shop → Bei Drücken des Button „Zahlung“ soll diese auch sichergestellt sein.**

Nicht-Vermehrbarkeit (non-propagation)

Weitere Begriffe

Definition

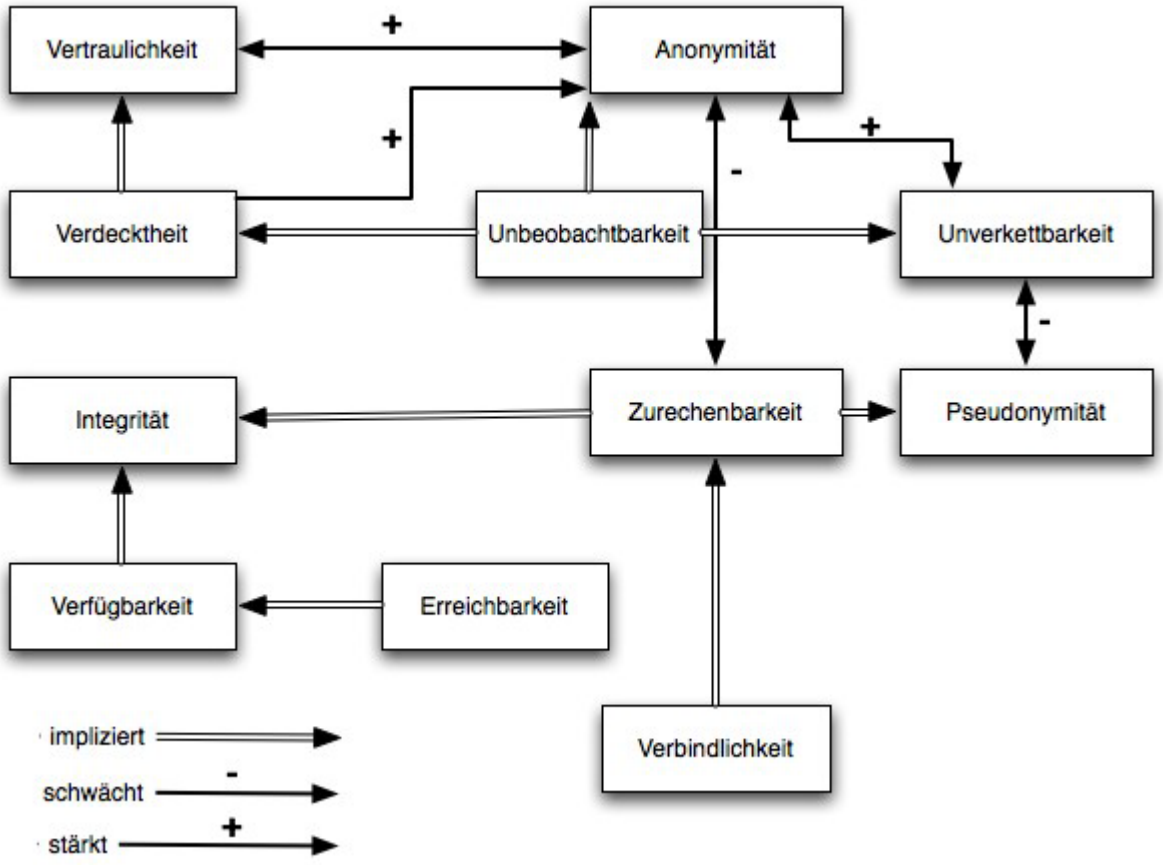
Informationen können von Unberechtigten nicht kopiert oder im Rahmen von„Replay-Angriffen“ nicht unerkannt wiederholt werden können.

Gegen-Beispiel

- **Wiederholung einer finanziellen Transaktion**

Quelle: Bedner, Mark / Ackermann, Tobias, 2010: **Schutzziele der IT-Sicherheit**, in: DuD- Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5: 323-328

Wechselwirkungen zwischen Schutzzielen



Quelle: A. Pfitzmann, A. Schill und A. Westfeld, Mehrseitige Sicherheit in offenen Netzen, Vieweg Verlagsgesellschaft, 2000

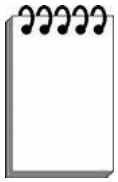
Privacy by Design (PbD)

Dr. Ann Cavoukian, Datenschutzbeauftragte der kanadischen Provinz Ontario, gilt seit Jahren als die treibende Kraft hinter PbD.

http://www.privacybydesign.ca/index.php/about-pbd/

Die 7 Grundprinzipien:

1. **Proaktiv, nicht reaktiv;**
2. **Datenschutz als Standardeinstellung**
3. **Der Datenschutz ist in das Design eingebettet**
4. **Volle Funktionalität – eine Positivsumme, keine Nullsummenspiel**
5. **Durchgängige Sicherheit - Schutz während des gesamten Lebenszyklus**
6. **Sichtbarkeit und Transparenz – Für Offenheit sorgen**
7. **Die Wahrung der Privatsphäre der Nutzer – Für eine nutzerzentrierte Gestaltung sorgen.**



Literatur

- Bedner, Mark / Ackermann, Tobias: *Schutzziele der IT-Sicherheit*, in: DuD-Datenschutz und Datensicherheit, 34. Jahrgang, Heft 5, S. 323-328, 2010
- Probst Thomas: Generische Schutzmaßnahmen für Datenschutz-Schutzziele; in: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6, S. 439-444, Juni 2012
- Rost, M. / Bock, K.: *Privacy By Design und die Neuen Schutzziele*; in: DuD - Datenschutz und Datensicherheit, 35. Jahrgang, Heft 1, S. 30-35, Januar 2011
- Rost, Martin; Pfitzmann, Andreas, 2009: *Datenschutz-Schutzziele - revisited*; in: DuD - Datenschutz und Datensicherheit, 33. Jahrgang, Heft 6, Juli 2009: 353-358, Juli 2009