Grundlagen des Datenschutzes und der IT-Sicherheit (Teil 2b)

Vorlesung im Sommersemester 2012

an der Universität Ulm

von Bernhard C. Witt

2. Grundlagen der IT-Sicherheit

Grundlagen des Datenschutzes		Grundlagen der IT-Sicherheit	
✓	Geschichte des Datenschutzes	✓	Anforderungen zur IT-Sicherheit
✓	Datenschutzrechtliche Prinzipien	➔	Mehrseitige IT-Sicherheit
✓	Technischer Datenschutz		Risiko-Management
✓	Kundendatenschutz		Konzeption von IT-Sicherheit

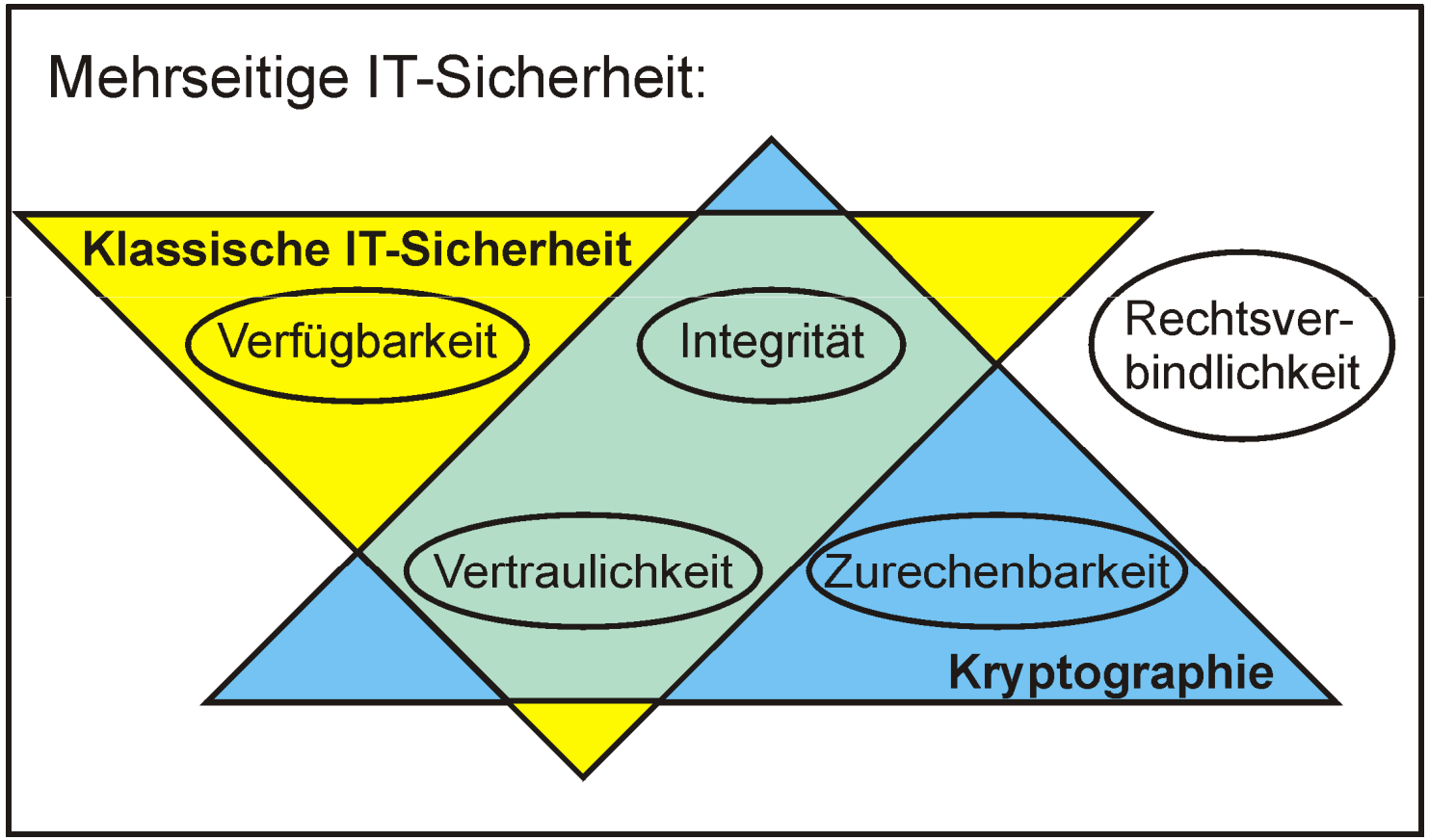
Mehrseitige IT-Sicherheit:

- Kennzeichen mehrseitiger IT-Sicherheit
- Ziele mehrseitiger IT-Sicherheit
  - Verfügbarkeit
  - Integrität
  - Vertraulichkeit
  - Zurechenbarkeit
  - Rechtsverbindlichkeit

Mehrseitige IT-Sicherheit (1)

- 1997: „Duale“ bzw. „Mehrseitige“ IT-Sicherheit entwickelt vom Ladenburger Kolleg „Sicherheit in der Kommunikationstechnik“
- Erweiterung der klassischen Sicherheitsziele, die der Verlässlichkeit der IT-Systeme dienen, um Komponenten zur Beherrschbarkeit der IT-Systeme (→ Integration der Betroffenensicht) → komplementäre Sicht
- **Verlässlichkeit** = keine unzulässige Beeinträchtigung der IT-Systeme, Daten bzw. Funktionen/Prozessen im Bestand, ihrer Nutzung oder ihrer Verfügbarkeit
  → Sicherheit der Systeme
- **Beherrschbarkeit** = keine unzulässige Beeinträchtigung von Rechten oder schutzwürdigen Belangen der Betroffenen durch Vorhandensein oder Nutzung von IT-Systemen
  → Sicherheit vor den Systemen

Mehrseitige IT-Sicherheit (2)



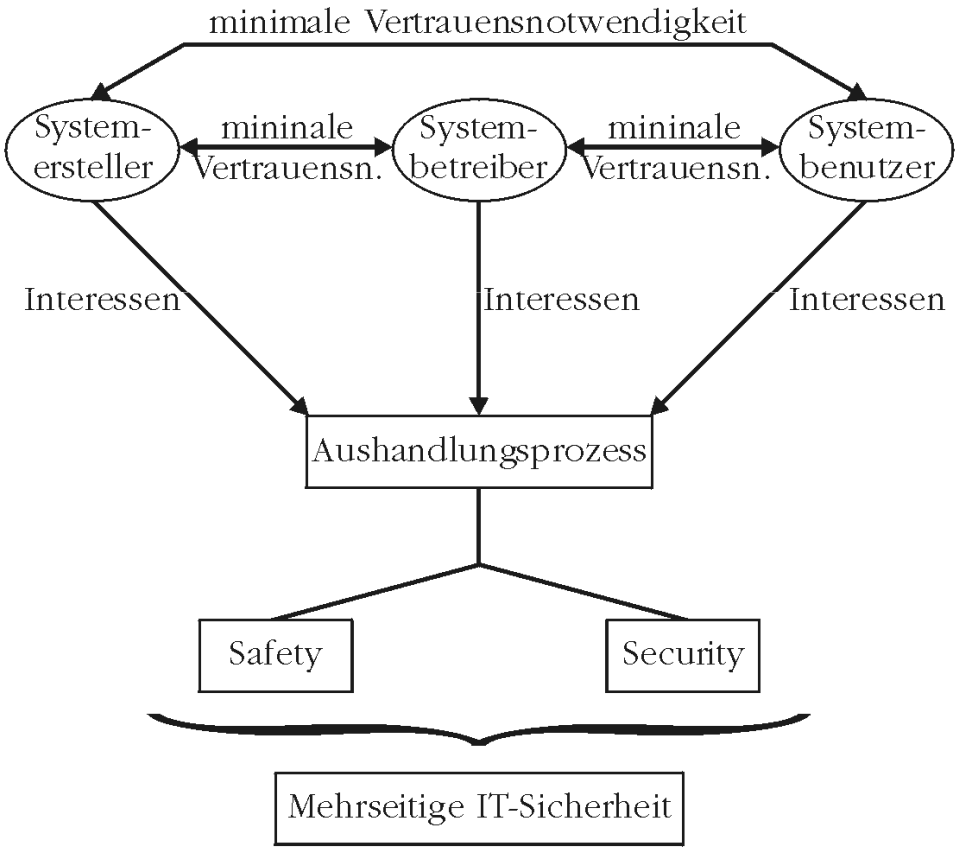
Mehrseitige IT-Sicherheit (3)

Definition 11: Mehrseitige IT-Sicherheit

Schutz von Hardware, Software und Daten vor Gefährdungen vereinbarter Verfügbarkeit, Integrität, Vertraulichkeit, Zurechenbarkeit und Rechtsverbindlichkeit

- Mehrseitige IT-Sicherheit erfordert die Einbeziehung der Schutzinteressen aller Beteiligten:
  - → Formulierung der spezifischen Sicherheitsinteressen
  - → Erkennen der zu lösenden Schutzkonflikte
  - → Aushandlung zur Auflösung dieser Konflikte
  - → Durchsetzung eigener Sicherheitsinteressen (Kompromiss)
- **Grundsatz**: Sicherheit mit minimalen Annahmen über andere (d.h.: möglichst wenig Vertrauen in andere setzen müssen)

Mehrseitige IT-Sicherheit (4)



Festgestellte Schadensfälle

Schäden durch	2004	2006	2008	2010
Unfälle (menschl. bzw. techn. Versagen)	73%	70%	64%	63%
Angriffe (ungezielt bzw. gezielt)	60%	43%	36%	40%

Quelle: <kes>-Sicherheitsstudien

- mehr Schäden durch Unfälle (→ Safety) zu verzeichnen als durch Angriffe (→ Security)
- (mehrseitige) IT-Sicherheit hat beides zu berücksichtigen
- Ursachenermittlung ergibt differenziertes Bild (Mehrfachnennungen waren möglich; bei <kes> in einer Tabelle aufgelistet)

Ursachen von Schadensfällen durch unabsichtliche Ereignisse

Ursachen unabs. Gefahr	2000	2002	2004	2006	2008	2010
Fehler eigener Mitarbeiter	52%	30%	51%	49%	36%	36%
Fehler durch Externe	6%	9%	15%	30%	16%	13%
höhere Gewalt	5%	3%	8%	12%	4%	12%
Software-bedingte Defekte	30%	19%	43%	46%	26%	32%
Hardware-bedingte Defekte	23%	15%	38%	45%	34%	30%
Dokumentations-bed. Defekte	11%	3%	17%	20%	15%	20%

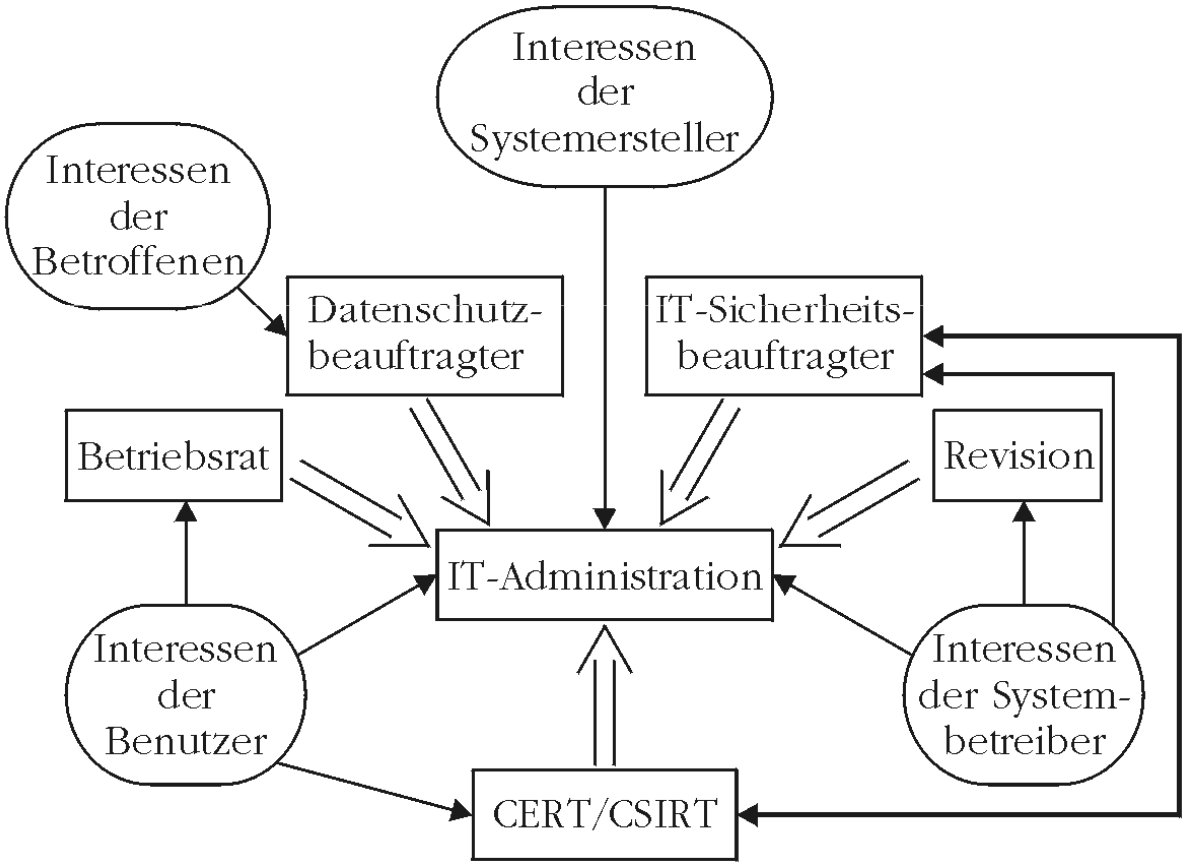
Quelle: <kes>-Sicherheitsstudien

Ursachen von Schadensfällen durch Angriffe

Formen erlittener Angriffe	**2000**	**2002**	**2004**	**2006**	**2008**	**2010**
Malware (Vir., Würm., Troj.Pf.)	29%	25%	54%	35%	21%	27%
unbefugte Kenntnisnahme	11%	6%	9%	12%	8%	13%
Hacking	-----	8%	9%	12%	11%	8%
Manipulation z. Bereicherung	2%	2%	8%	11%	8%	11%
Sabotage (inkl. DoS-Attacken)	2%	2%	8%	10%	6%	5%

Quelle: <kes>-Sicherheitsstudien

Akteure zur IT-Sicherheit



Ziele mehrseitiger IT-Sicherheit (1)

Definition 12: Verfügbarkeit (availability)

Gewährleistung, dass das IT-System (für befugte Nutzer) zugänglich und funktionsfähig ist

- → **ISO/IEC 27000**: property of being accessible and usable upon demand by an authorized entity
- → Prozessausführung in vorgesehener Weise zum geplanten Zeitpunkt im vorgegebenen Zeitrahmen
- → Sicherung vor Ausfällen und ungewolltem Verlust
- → betrifft auch die Vollständigkeit des Datenbestands (Nutzdaten, Passwortdaten, Konfigurationsdaten & Protokolldaten)

Berechnung der Verfügbarkeit (1)

$$\text{Verfügbarkeit einer IT-Komponente} = \frac{(\text{vereinbarte Servicezeit} - \text{Ausfallzeit})}{\text{vereinbarte Servicezeit}} \text{ [in \%]}$$

$$\text{Verfügbarkeit eines Dienstes} = \frac{\text{MTBF}}{(\text{MTBF} + \text{MTTR})}$$

Hinweis:

- MTBF = "mean time between failures" (= Gesamtbetriebszeit / Gesamtzahl aufgetretener Fehler); MTTR = "mean time to repair“ (= Gesamtreparaturzeit / Gesamtzahl aufgetretener Fehler)
- bei der vereinbarten Servicezeit (wie auch der Gesamtbetriebszeit) werden vereinbarte Wartungszeiten nicht berücksichtigt, da Systemausfälle in diesem Zeitraum ausdrücklich durch die getroffene Vereinbarung abgedeckt sind (= „geplante Nichtverfügbarkeit“)

Berechnung der Verfügbarkeit (2)

Berücksichtigung **technischer Redundanzen** (parallele Systeme) durch:

$$\text{Verfügbarkeit}_{\text{baugleich}} = 1 - (1 - \text{Verfügbarkeit}_{\text{normal}})^{\text{Anzahl}}$$

$$\text{Verfügbarkeit}_{\text{bauungleich}} = 1 - \Pi\ (1 - \text{Verfügbarkeit}_{\text{normal}} \text{ der Komponente i})$$

- besonders kritische IT-Systeme können durch technische Redundanz eine deutlich höhere Verfügbarkeit erhalten (Parallelität statt Seriellität!)
- die Angabe von Verfügbarkeiten ist vor allem im Rahmen von **Service Level Agreements** (SLAs) wichtig; Ausfallzeiten (durch unbeabsichtigte Ereignisse & Angriffe) sind teuer
- bei Auftreten von Ausfallzeiten hängt einiges davon ab, welche „Reaktionszeiten“ (bis wann wird auf die Meldung reagiert?) und „Problembeseitigungszeiten“ (bis wann ist das gemeldete Problem behoben?) mit einem entsprechenden Serviceunternehmen vereinbart wurden

Berechnung der Verfügbarkeit (3)

Berücksichtigung **Gesamtverfügbarkeit** durch:

Verfügbarkeit IT-Verbund = Π (Verfügbarkeit aller IT-Komponenten)

- Die Einzelverfügbarkeiten werden also miteinander multipliziert
- Je komplexer ein IT-Verbund also ist, desto ausfallanfälliger ist er insgesamt, wenn er keinerlei Redundanzen aufweist
- Im Zuge einer Parallel-Schaltung von IT-Systemen wird die Nicht-Verfügbarkeit eines IT-Systems ggf. durch eine vorhandene Verfügbarkeit eines anderen IT-Systems ausgeglichen (vorausgesetzt, das redundante IT-System ist tatsächlich aktiver Teil des Clusters und nicht nur als Cold-Stand-by konzipiert)
- Bei Hochverfügbarkeit muss Redundanz standort-übergreifend realisiert sein

Gründe für Ausfallzeiten

hinsichtlich <u>unbeabsichtigter</u> Ereignisse:

- zu 39 % **Hardware**-Fehler
  (davon 51 % Plattenspeicher)
- zu 31 % Fehler & Abstürze in **Software**-Programmen
  (davon 62 % Betriebssystem)
- zu 18 % **Bedienungsfehler**
- zu 12 % **externe Fehlerquellen** wie Stromausfall & Wasser-schaden

  Quelle: Jochen Sommer: IT-Servicemanagemet mit ITIL und MOF, 2004

→ leider keine absolute Angabe der durchschnittlichen Ausfallzeit & keine Angabe zu angriffsbedingten Ausfallzeiten

Ausfall der Verfügbarkeit durch Angriffe

Dauer von Ausfallzeiten:

- zu 32,5 % 0 h
- zu 27,8 % < 4 h
- zu 13,4 % [4 .. 8] h
- zu 8,6 % (8 .. 24] h
- zu 5,3 % (1 .. 3] d
- zu 2,3 % > 3 d
- zu 10,2 % kein Kommentar

  Quelle: InformationWeek „IT-Security 2004“

→ im Schnitt ca. **6 h Ausfallzeit durch** erfolgreiche **Angriffe** auf die Verfügbarkeit von Server, Anwendungen und Netzwerken

Dauer von Ausfallzeiten:

- 17 h Virus-/Wurm-Infektion
- 2 h Hoax
- 9 h Fehlalarm
- 130 h gezielter Angriff

  Quelle: <kes>-Sicherheitsstudie 2010

→ Ausfallzeiten bei konkret eingetretenen **Einzelfällen**

→ Gezielte Angriffe (targetted attacks) besonders aufwändig bei Wiederherstellung der Verfügbarkeit

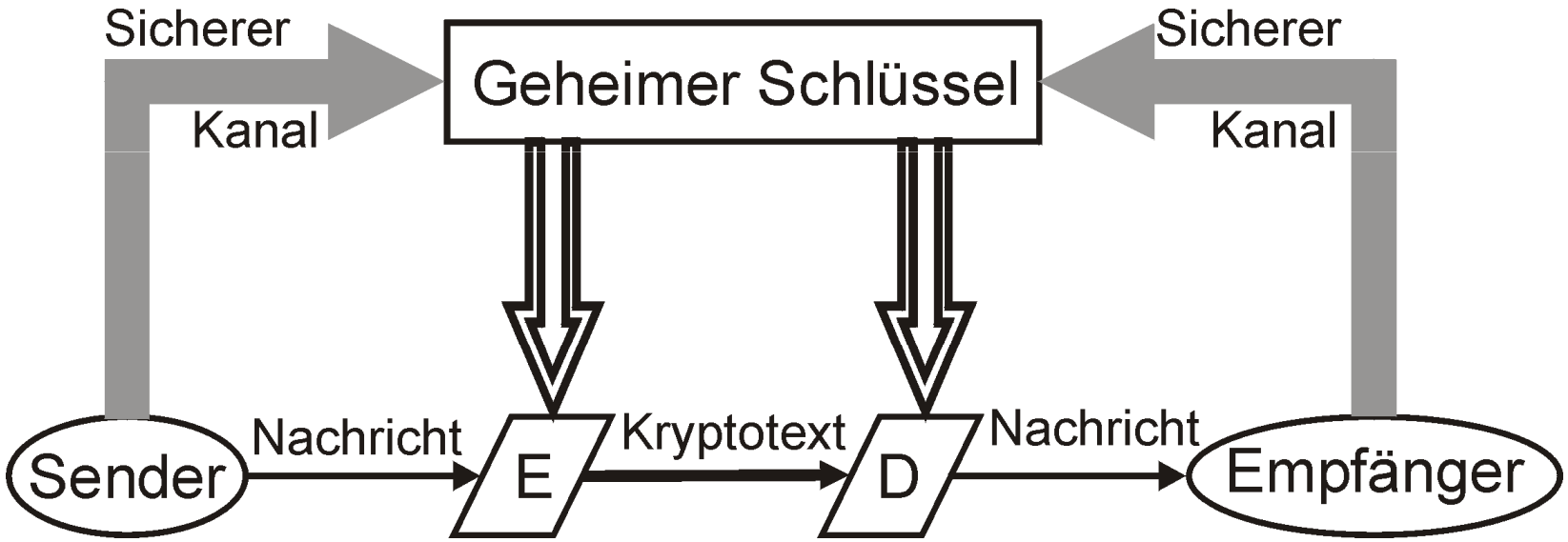
Ziele mehrseitiger IT-Sicherheit (2)

Definition 13: Vertraulichkeit (confidentiality)

Gewährleistung, dass die Daten des IT-Systems nur durch befugte Nutzer interpretiert werden

- → **ISO/IEC 27000**: property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- → kein unbefugter Informationsgewinn
- → Daten für Unbefugte nicht zugänglich (auch nicht über verdeckte Kanäle)
- → ergänzt durch Anonymität/Pseudonymität, Unbeobachtbarkeit & Verdecktheit aus Kommunikationstechnik

Symmetrische Verschlüsselung

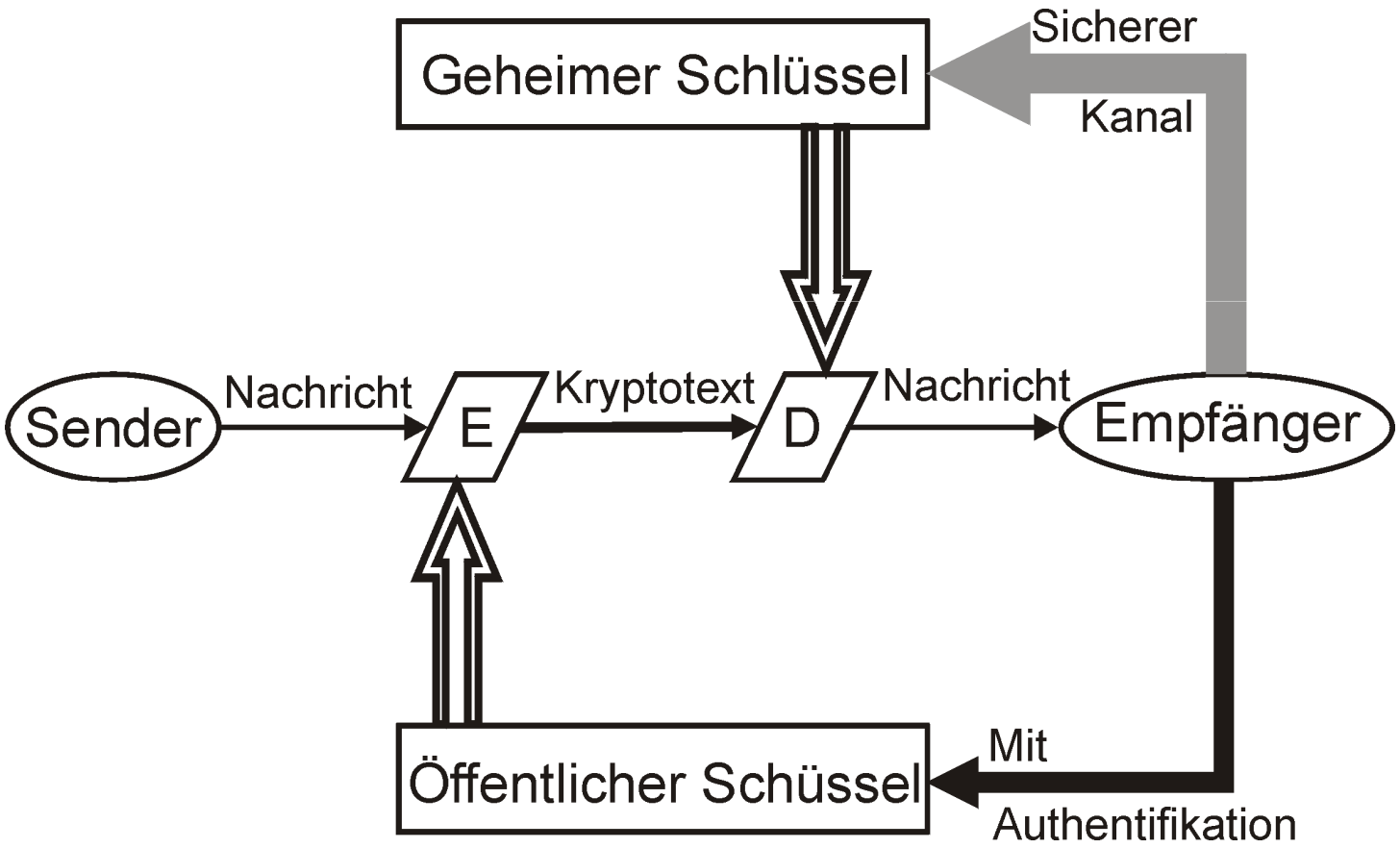


Beispiel: Symmetrische Verschlüsselung

Sender:					
Klartext:	1	0	1	1	
+ Schlüssel:	1	1	0	1	[XOR]
= Chiffre:	0	1	1	0	

Empfänger:					
Chiffre:	0	1	1	0	
- Schlüssel:	1	1	0	1	[XOR]
= Klartext:	1	0	1	1	

Asymmetrische Verschlüsselung



Beispiel: Asymmetrische Verschlüsselung (1)

Verfahren nach Rivest, Shamir und Adleman (RSA):

Ausgangspunkt für Empfänger (!):

- wähle zwei Primzahlen p + q; z.B. p=3 und q=7
- berechne das Produkt dieser Primzahlen und dessen Eulerschen Funktionswert;
  $n=p*q=3*7=21$ und $\varphi(n)=(p-1)*(q-1)=2*6=12$
- wähle zufällig den geheimen Dechiffrierschlüssel d, für den gilt: $ggT(d, \varphi(n))=1$; z.B. d=5
- berechne den zu d gehörenden öffentlichen Chiffrierschlüssel e, für den gilt: $d*e \equiv 1 \bmod \varphi(n)$; $5*e \equiv 1 \bmod 12 \rightarrow e=17$ ($5*17=85=7*12+1$); Anm: empfohlen sind e=3, e=17, e=65537
- veröffentliche n und e

Beispiel: Asymmetrische Verschlüsselung (2)

Sender: (e=17, n=21)			
Klartext:	10	11	
Chiffre:	19	2	$c_i=(m_i)^e \bmod n$

Empfänger: (d=5, n=21)			
Chiffre:	19	2	
Klartext:	10	11	$m_i=(c_i)^d \bmod n$

Vergleich der Verschlüsselungen

Symmetrisch:

- Gängige Verfahren:
  one-time-pad, AES, DES, Triple-DES
- Typische Schlüssellänge:
  128 – 256 Bit-Schlüssel „auf absehbare Zeit“ sicher
- Performanz:
  mind. um Faktor 100 schneller als asymmetrisch
- Ziel:
  Sicherung d. **Vertraulichkeit**

Asymmetrisch:

- Gängige Verfahren:
  RSA, ElGamal
- Typische Schlüssellänge:
  1024 – 4096 Bit-Schlüssel (entspricht etwa 128 – 256 Primzahlen)
- Performanz:
  stark vereinfachter Schlüsselaustausch
- Ziel:
  Sicherung d. **Vertraulichkeit**

Zum Vergleich symmetrischer zu asymmetrischer Verschlüsselung

Gemäß Primzahlensatz gilt für die Primzahl-Anzahl:

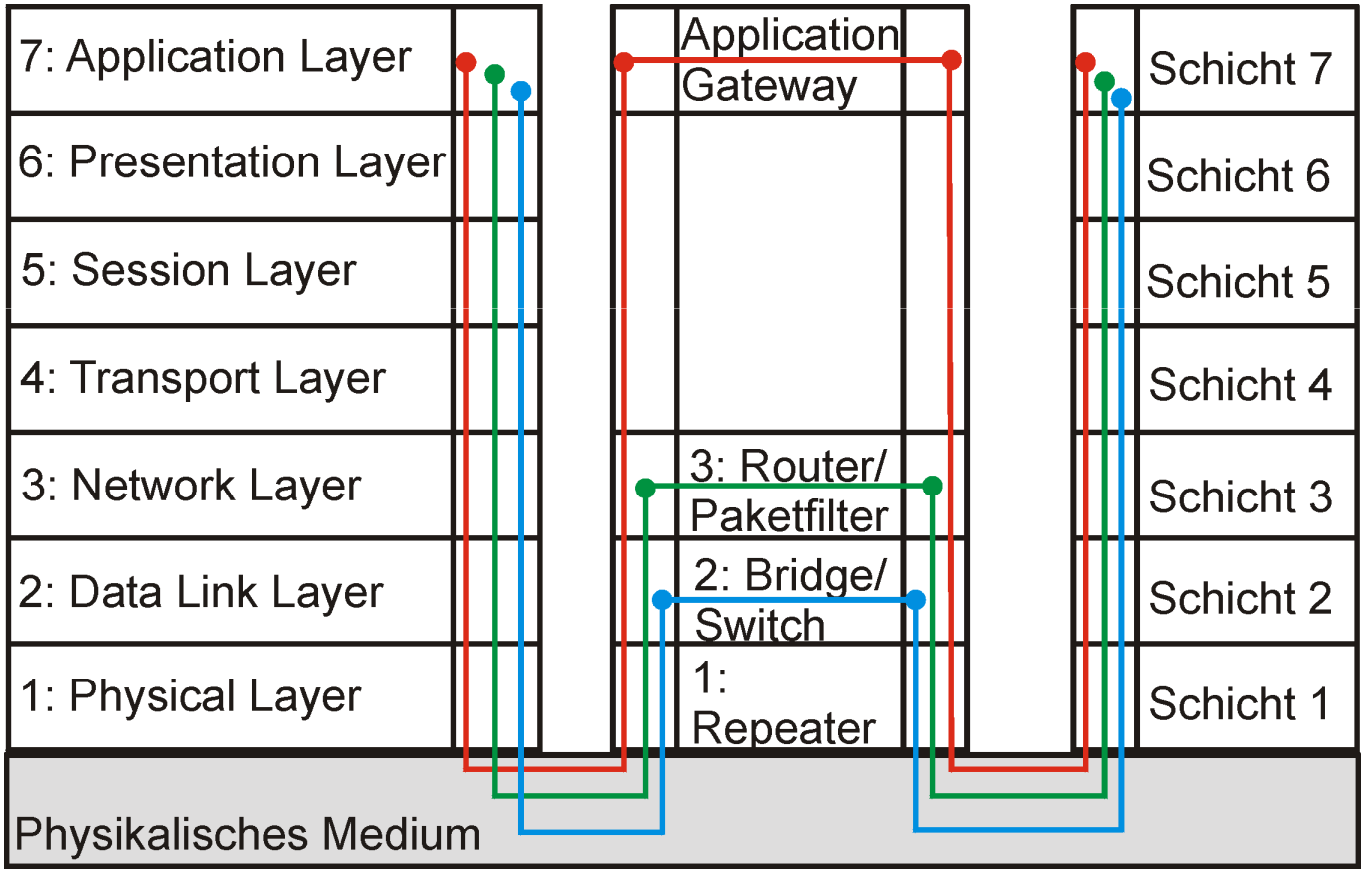
$(n/[\ln(n)+2]) < \pi(n) < (n/[\ln(n)-4])$

→ $\mathbf{\pi(n) \approx [n/\ln(n)]}$

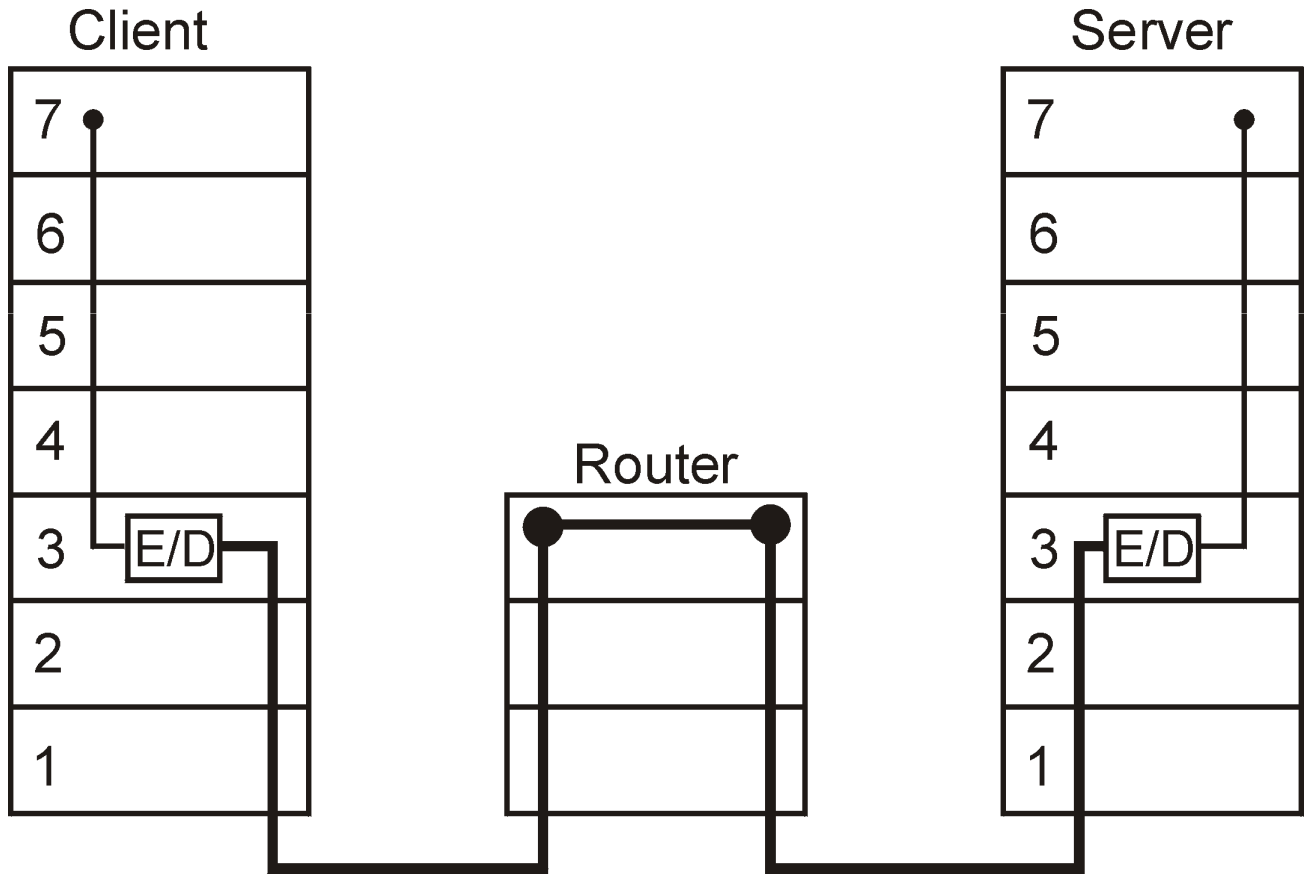
- im Intervall [1 .. 1024] → $\pi(n) \approx 148$ (Primzahlen)
- im Intervall [1 .. 2048] → $\pi(n) \approx 269$ (Primzahlen)
- im Intervall [1 .. 3072] → $\pi(n) \approx 382$ (Primzahlen)
- im Intervall [1 .. 4096] → $\pi(n) \approx 492$ (Primzahlen)

beim Vergleich mit Bits ist zu beachten, dass jedes Bit den Wert 0 oder 1 annehmen kann

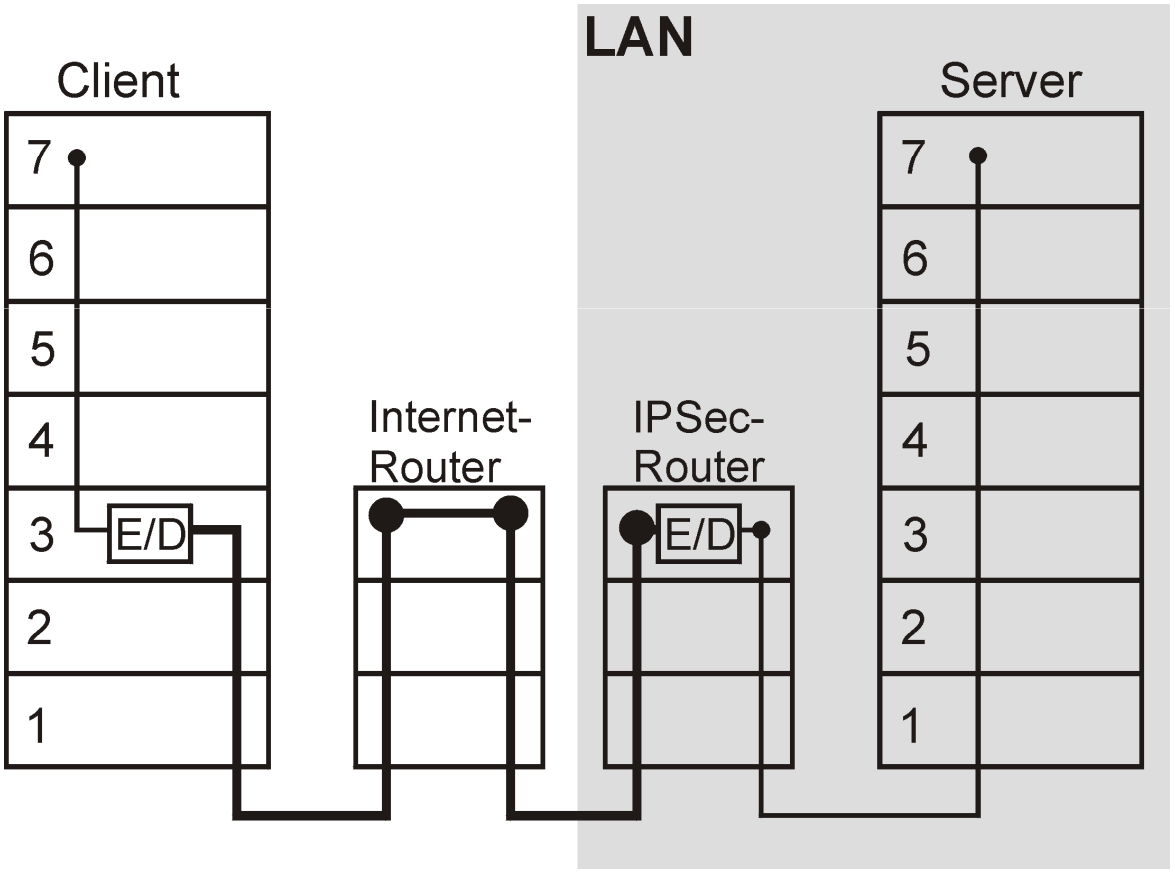
Kommunikationsbeziehungen beim ISO/OSI-Referenzmodell



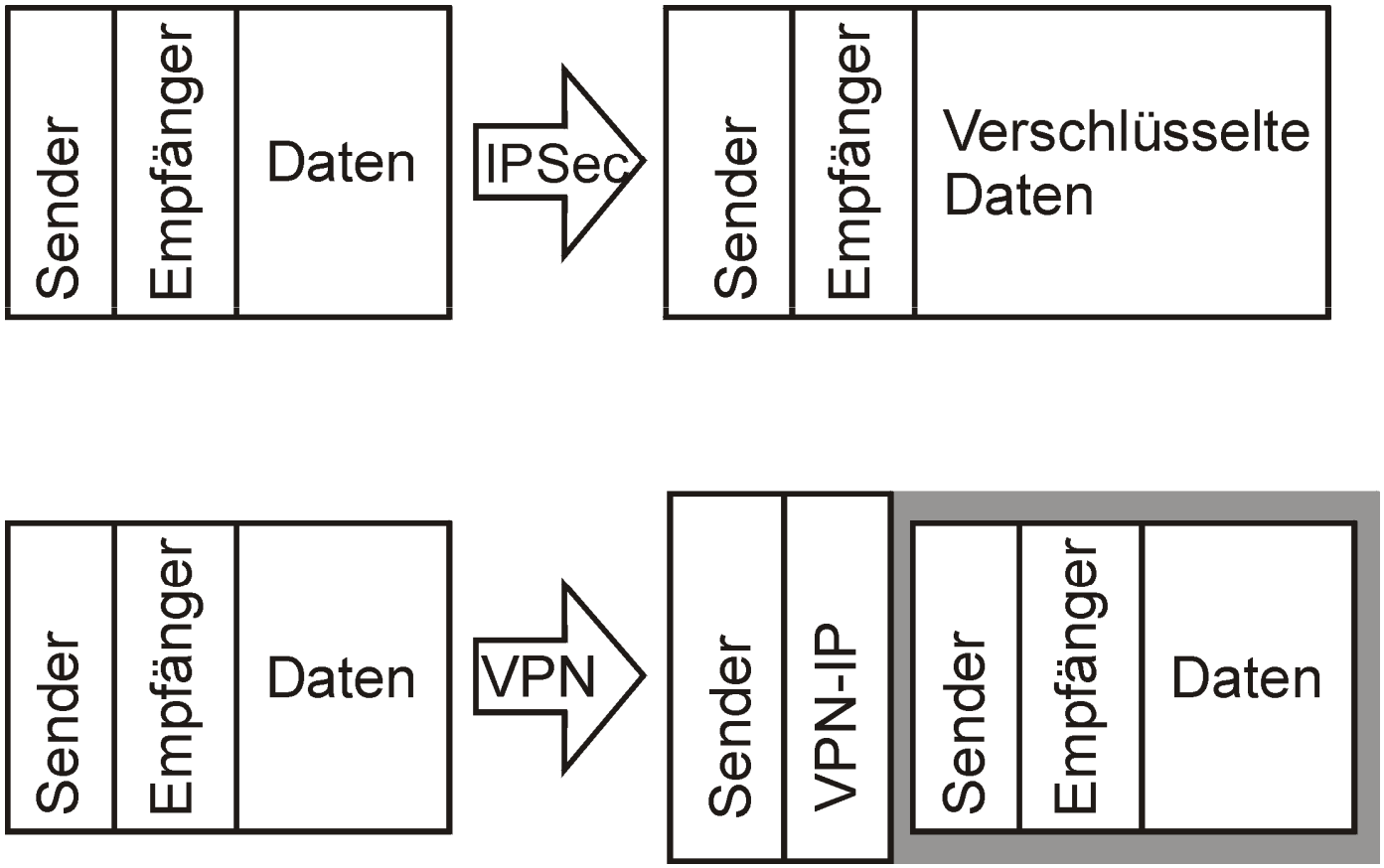
Kommunikation via IPSec: Ende-zu-Ende-Verschlüsselung



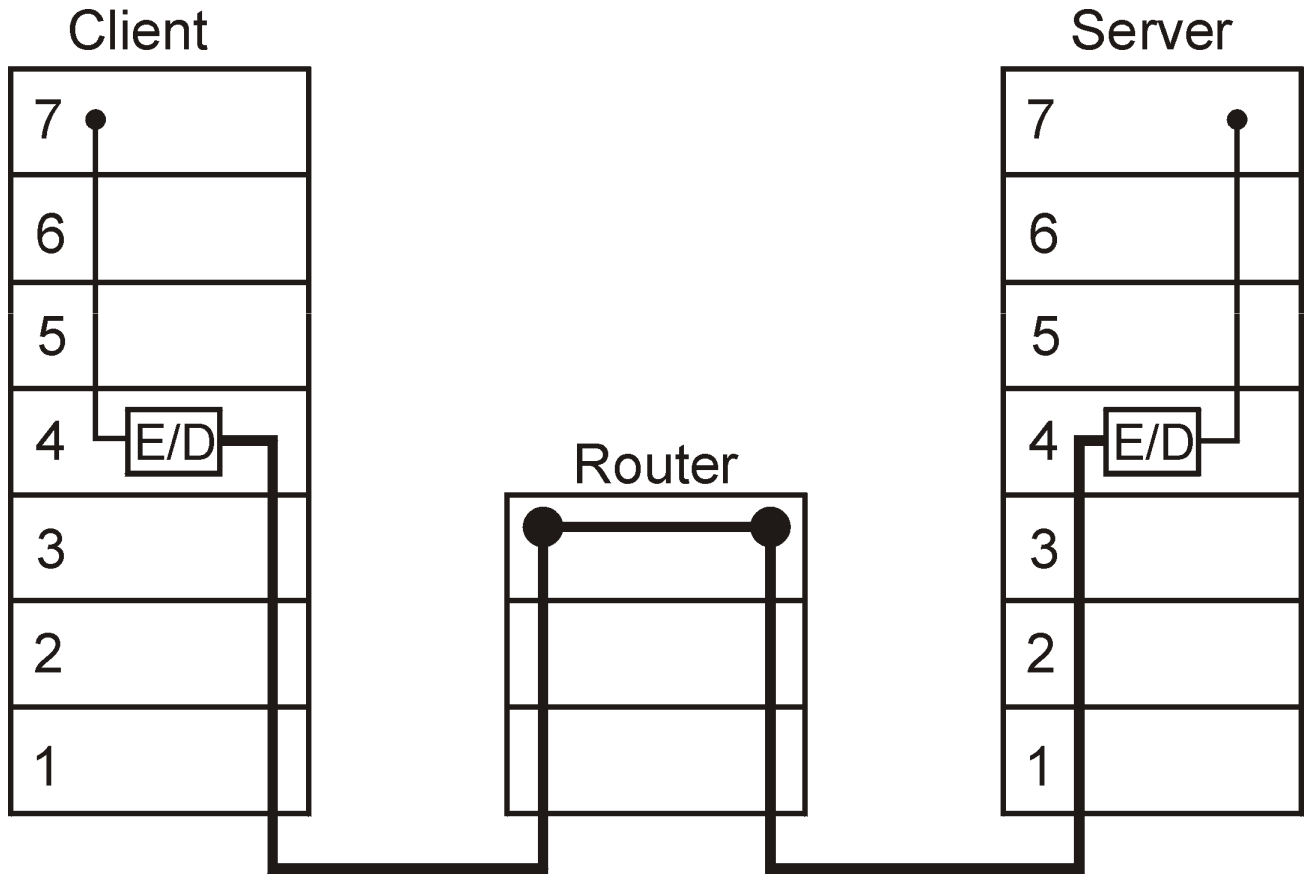
Kommunikation via VPN: Verbindungsverschlüsselung



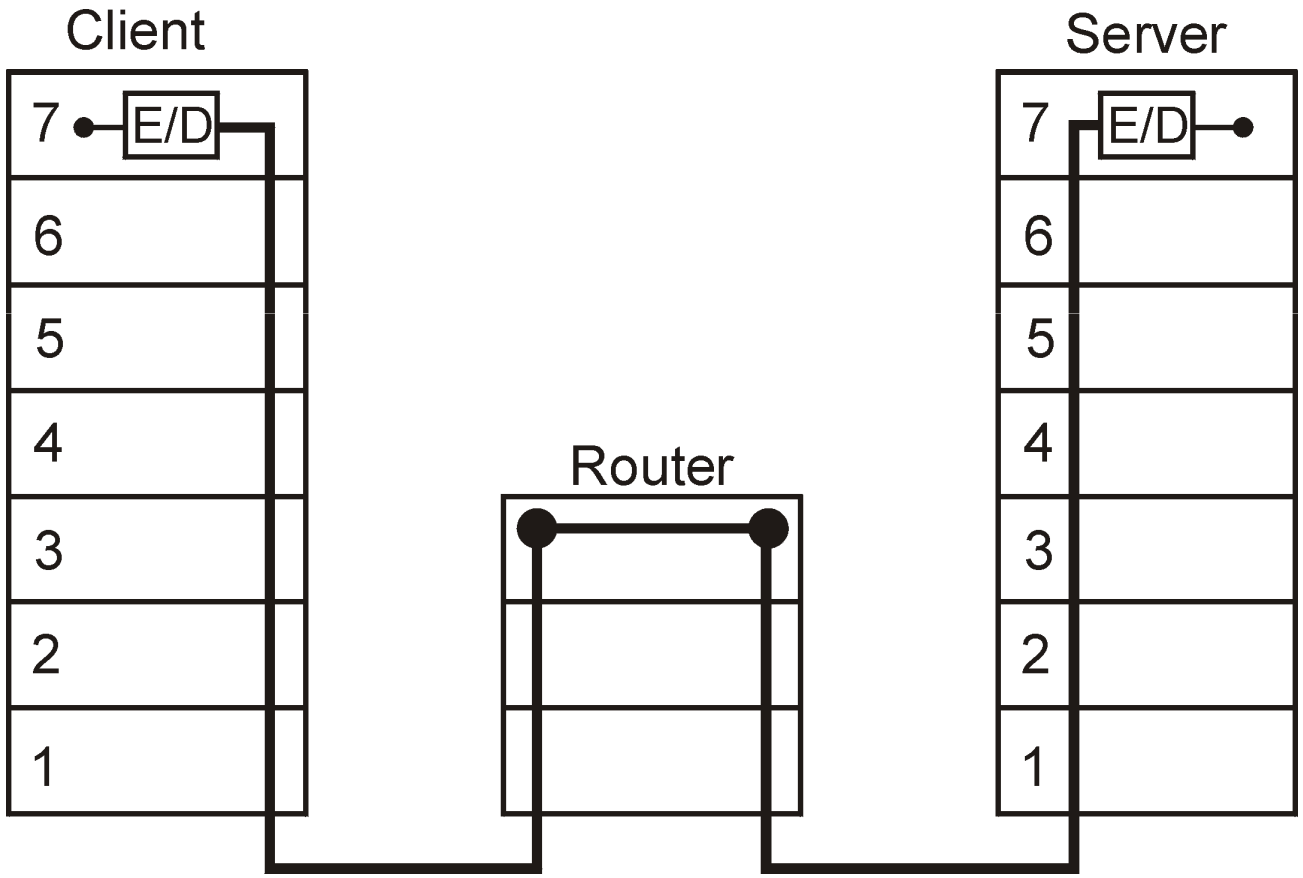
Unterschied zwischen IPSec & VPN



Kommunikation via SSL/TLS: Ende-zu-Ende-Verschlüsselung



Kommunikation via SSH: Ende-zu-Ende-Verschlüsselung



Verlust der Vertraulichkeit

unbefugte Zugriffsart	2006		2008		2010	
	bek.	verm.	bek.	verm.	bek.	verm.
Verlust mobiler IT-Systeme	27%	9%	14%	17%	12%	13%
Verlust von Speichermedien	7%	5%	10%	18%	8%	20%
Missbrauch durch Berechtigte	3%	15%	7%	18%	8%	18%
Social Engineering / Phishing	-----	-----	9%	17%	6%	29%
Online-Angriff	2%	4%	4%	7%	6%	6%
Einbruch in Gebäude	17%	1%	8%	7%	6%	5%
Abhören von Kommunikation	1%	8%	0%	8%	1%	8%

Quelle: <kes>-Sicherheitsstudien 2006 & 2008 & 2010

bek. = bekannt/sicher; verm. = vermutlich

Ziele mehrseitiger IT-Sicherheit (3)

Definition 14: Integrität (integrity)

Gewährleistung, dass die Daten des IT-Systems nur durch befugte Nutzer verändert werden

- → **ISO/IEC 27000**: property of protecting the accuracy and completeness of assets
- → Vorliegen korrekter (= originalgetreuer und unverfälschter) und aktueller Daten
- → Feststellbarkeit von Manipulationen (Datenqualität)
- → zielt auf die Vollständigkeit des Datenbestandes ab
- → Anforderungen an disaster recovery

Sicherung der Integrität

- Ein Nachweis von Integrität erfolgt z.B. mittels **Authentifizierungs-mechanismen**
- Ebenso im Einsatz vor allem zur Vermeidung ungewollter Manipulationen: **fehlerkorrigierender Code** & verschiedene **Fehlermeldeverfahren**
- Die Zuverlässigkeit von IT-Komponenten kann durch entsprechende Zertifikate (Common Criteria) nachgewiesen werden
- Protokollierungen erforderlich für Datenqualität
- Revisionssicherheit z.B. durch Abspeichern auf nur einmal beschreibbaren Datenträgern

Hinweis:

Authentisierung = Nachweis einer Identität

Authentifizierung = Überprüfung einer Identität

Autorisierung = Gewährung Zutritts-/Zugangs-/Zugriffsrechten für Identität

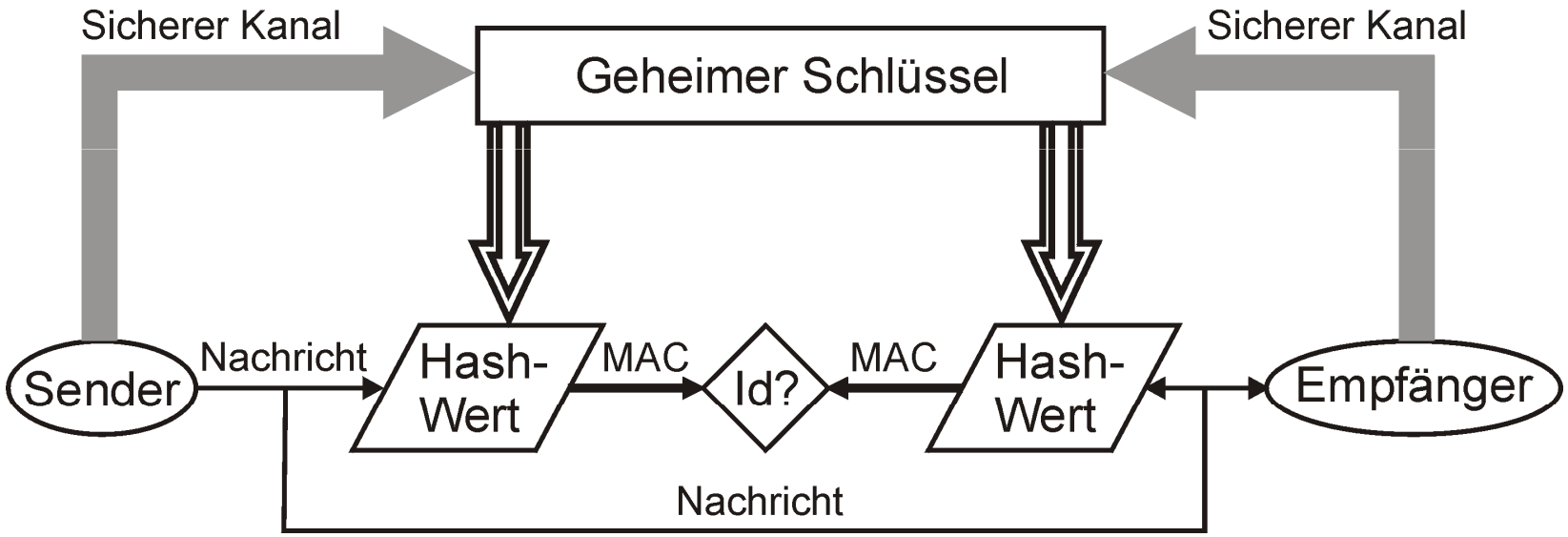
Ziele mehrseitiger IT-Sicherheit (4)

Definition 15: Zurechenbarkeit (accountability)

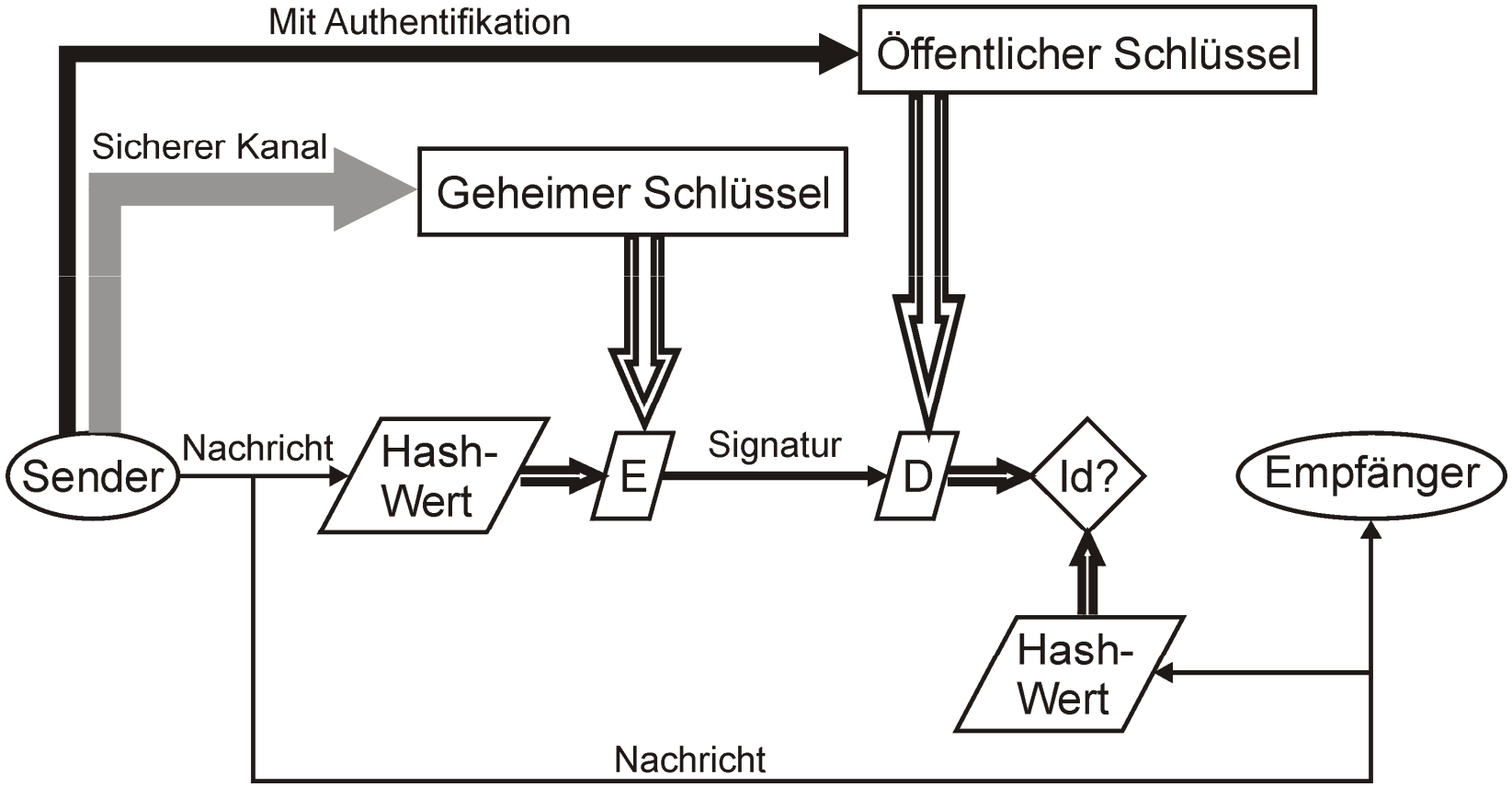
Gewährleistung, dass jederzeit festgestellt werden kann, welcher Nutzer einen Prozess ausgelöst hat

- → **ISO/IEC 27000**: responsibility of an entity for its actions and decisions
- → Verantwortlichkeit & Authentizität (Glaubwürdigkeit)
- → Diese Daten kommen vom Kommunikationspartner
- → Die Daten kommen von diesem Kommunikationspartner
- → Kern des Rechtemanagements

Symmetrische Authentifikation: Message Authentication Code



Asymmetrische Authentifikation: Digitale Signatur



Vergleich der Authentifikationen

Symmetrisch:

- Gängige Verfahren:
  SecurID, GSM-Authentikation
- Ziel:
  Sicherung d. **Integrität**
- Key-Recovery sinnvoll:
  Hinterlegung des Entschlüsselungsschlüssels zur Vorbeugung gegen Schlüsselverlust

Asymmetrisch:

- Gängige Verfahren:
  RSA, ElGamal, DSS, DSA
- Ziel:
  Sicherung d. **Integrität** und **Zurechenbarkeit**
- erfüllt Anforderungen zur fortgeschrittenen Signatur nach SigG, sofern geheimer Schlüssel unter alleiniger Kontrolle des Schlüsselinhabers (qualifizierte Signatur, wenn zertifiziert und mit sicherer Einheit erzeugt)

Ziele mehrseitiger IT-Sicherheit (5)

Definition 16: Rechtsverbindlichkeit (legal liability)

Gewährleistung, dass Daten und Vorgänge gegenüber Dritten jederzeit rechtskräftig nachgewiesen werden können

→ Transparenz (Nachvollziehbarkeit)

→ Reversibilität & Verhinderung falschen Abstreitens

→ Nachweis zugesicherter Eigenschaften (assurance)

→ Voraussetzung für Auditierbarkeit

→ Ausgleich für fehlenden klassischen Augenscheinbeweis