

LF4

Skript

Teil 1

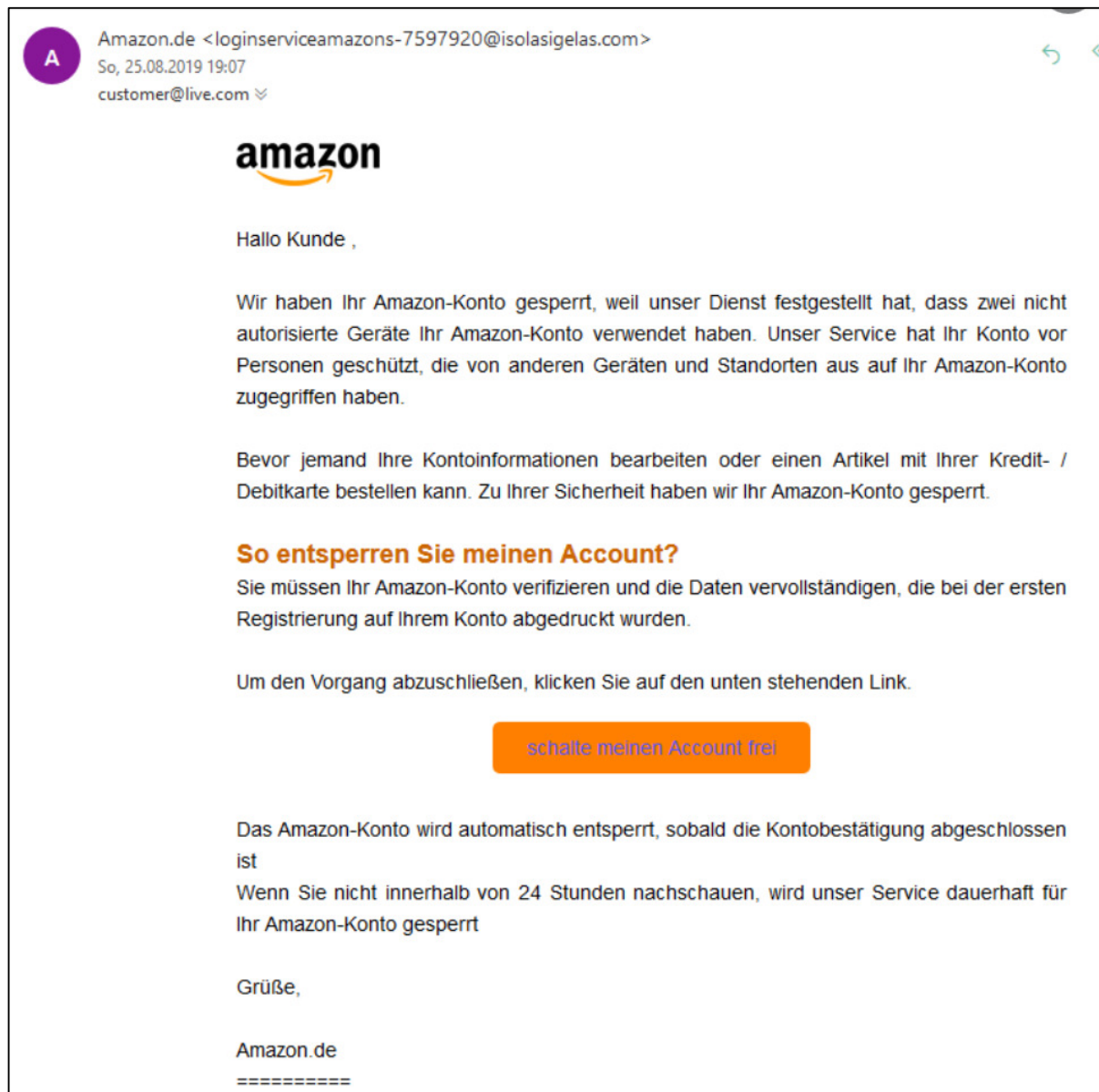
Test am Freitag 26.04.:

- Begriffe der Datensicherheit, Stichwort VIVA. Wie kann ich sie schützen/angreifen jeweils eine Maßnahme (BackUp für Verfügbarkeit etc.)
- CIA Dreieck, wird als Dreieck dargestellt weil wird als "Stellschraube" angesehen
- Datenschutz (nicht! Puzzle auf Seite 10 aber wo ist der Datenschutz geregelt etc.
Begriff unterschied zwischen persönlichen Daten und personenbezogenen Daten - Punkt 1.3 Seite 8
- Verschlüsselung alle drei Arten

Erstellt von: YN

Inhaltsverzeichnis

1. Grundlagen der Informationssicherheit
 - 1.1 Was ist Informationssicherheit?
 - 1.2 IT- Schutzziele der Informationssicherheit
 - 1.3 Datenschutz und Datensicherheit
 - 1.4 DSGVO (Datenschutzgrundverordnung)
2. Bedrohung der Informationssicherheit
 - 2.1 Die IT-Grundschatzkataloge
 - 2.1.1 Der Bausteinkatalog
 - 2.1.2 Der Gefährdungskatalog
 - 2.1.3 Der Maßnahmenkatalog
3. Maßnahmen zur Gewährleistung der Informationssicherheit
 - 3.1 Verschlüsselung
 - 3.1.1 Cäsar
 - 3.1.2 Enigma
 - 3.2 Aktuelle Verschlüsselungsverfahren
 - 3.2.1 Symmetrische Verschlüsselung
 - 3.2.2 Asymmetrische Verschlüsselung
 - 3.2.3 Hybride Verschlüsselung
 - 3.3 Digitale Signatur
 - 3.4 RAID
 - 3.5 Datensicherung (Backup und/oder Archivierung)
 - 3.5.1 Vollsicherung
 - 3.5.2 Inkrementelle Sicherung
 - 3.5.3 Differenzielle Sicherung



Skript_LF4.docx

Falscher Link

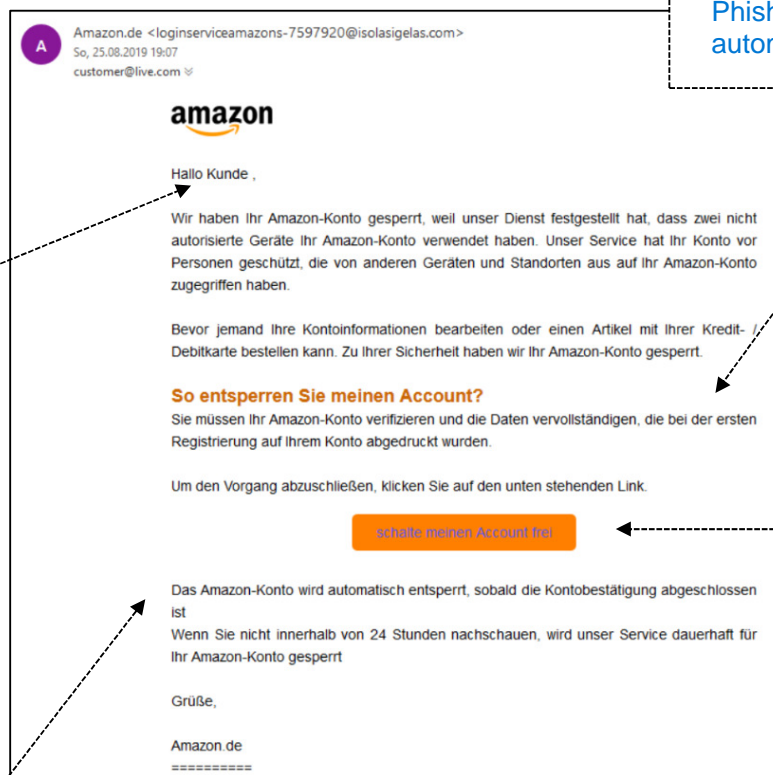
Den User einschränken und erstmal ohne Nachfrage Features sperren.

Schlechte Grammatik, viele Schreibfehler oder ganz andere Sprache. Viele Phishing E-Mails werden automatisch Übersetzt

Unpersönliche Anrede

Amazon wird nie nach Daten fragen die nichts mit der Website zu tun hat. Also Bankverbindung, Sozialversicherungsnummer etc.

Skript

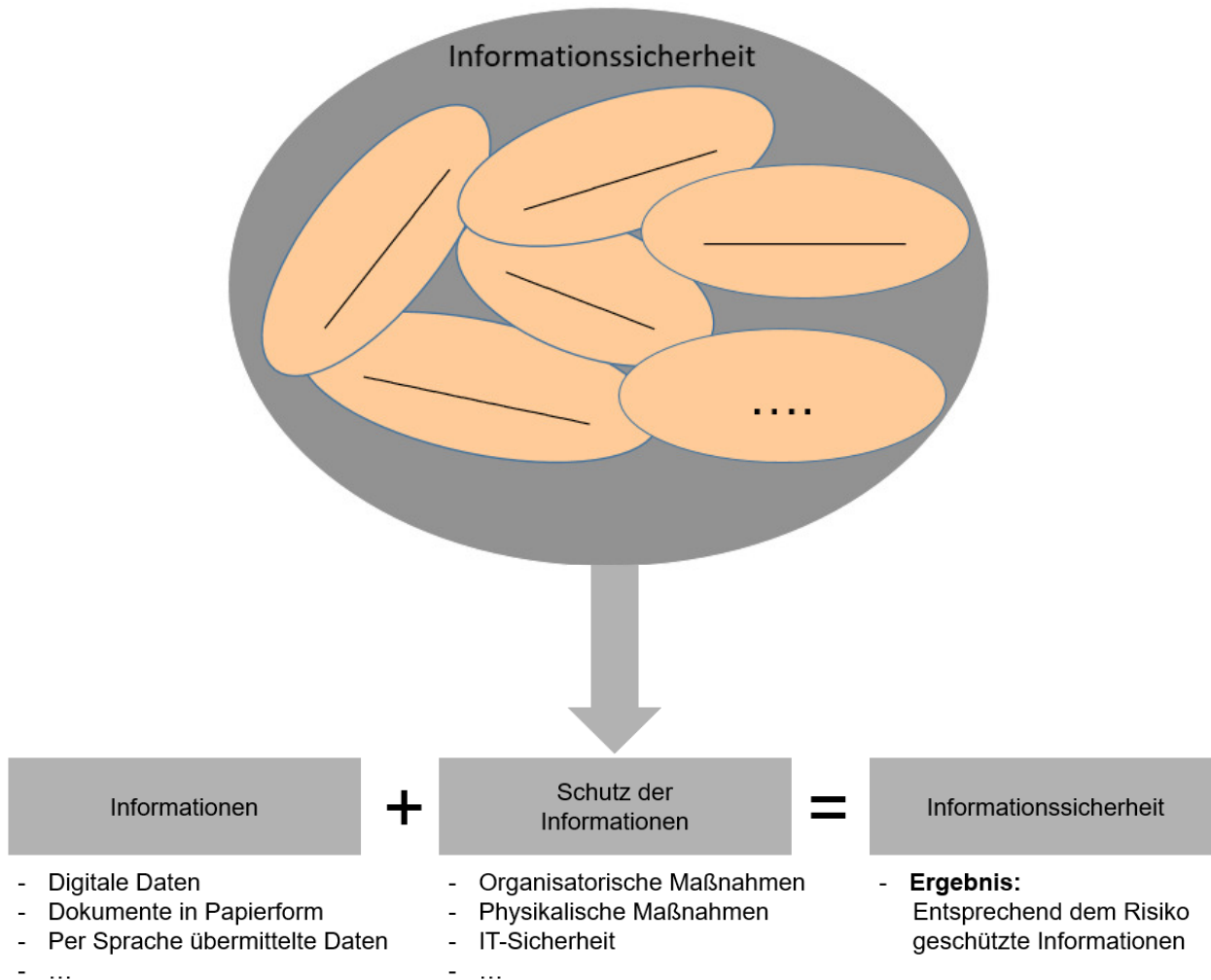


Fristdruck, Terminfrist

Login-Button wird angeboten. Normalerweise wird auf die Hauptseite verwiesen. Dort kann man sich gefahrlos einloggen.

1. Grundlagen der Informationssicherheit

1.1 Was ist Informationssicherheit?



Skript_LF4.docx

Unter dem Begriff „**Informationssicherheit**“ versteht man also alle Maßnahmen, welche folgendes leisten:

- Schutz vor Gefahren/Bedrohungen
- Vermeidung von Schäden
- Minimierung von Risiken

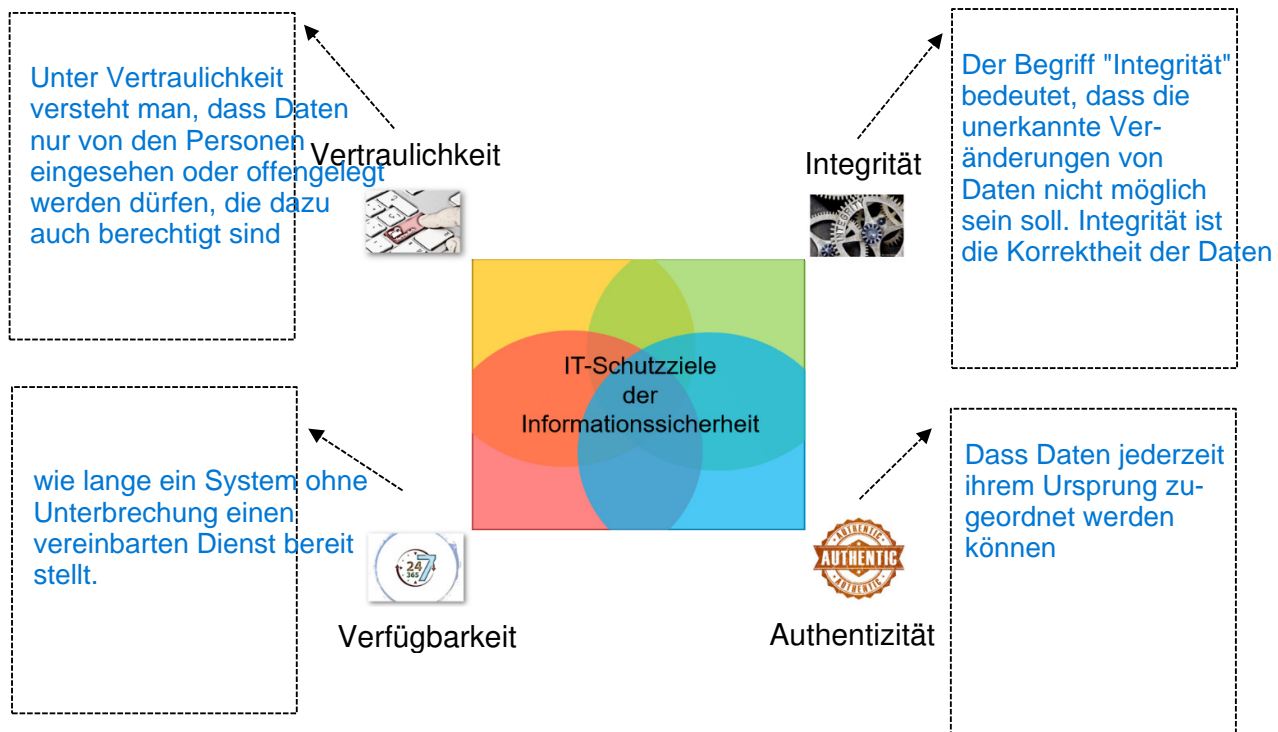
Die IT-Sicherheit umfasst die Sicherheit

- der IT-Systeme und der darin gespeicherten Daten

1.2 IT- Schutzziele der Informationssicherheit

Unter dem Begriff „**Informationssicherheit**“ versteht man also das Gewährleisten der **Schutzziele der Informationssicherheit** in technischen und nicht technischen Systemen.

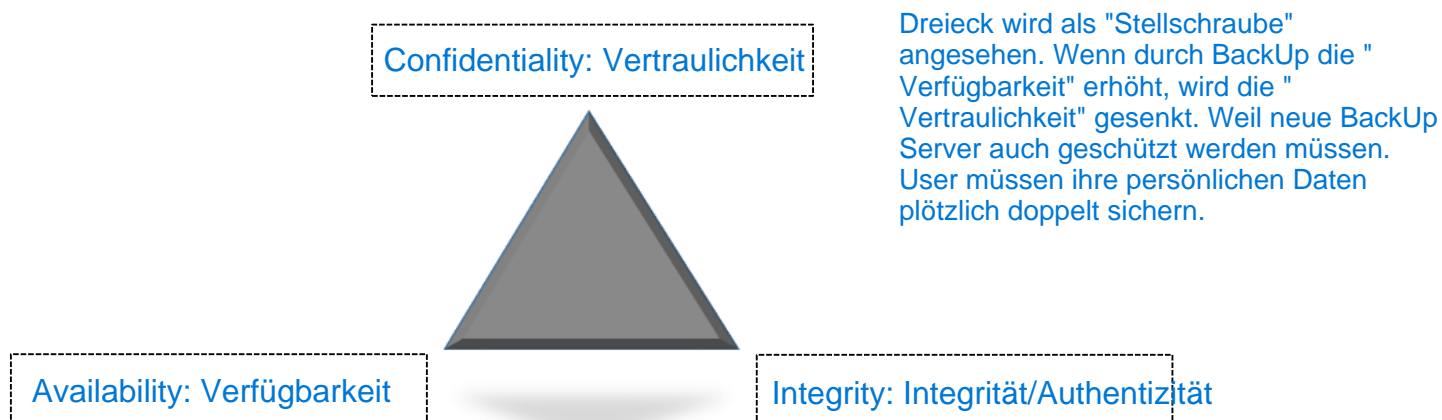
Schutzziele der Informationssicherheit sind **Vertraulichkeit, Verfügbarkeit, Integrität** und Authentizität (**wird der Integrität zugerechnet**).



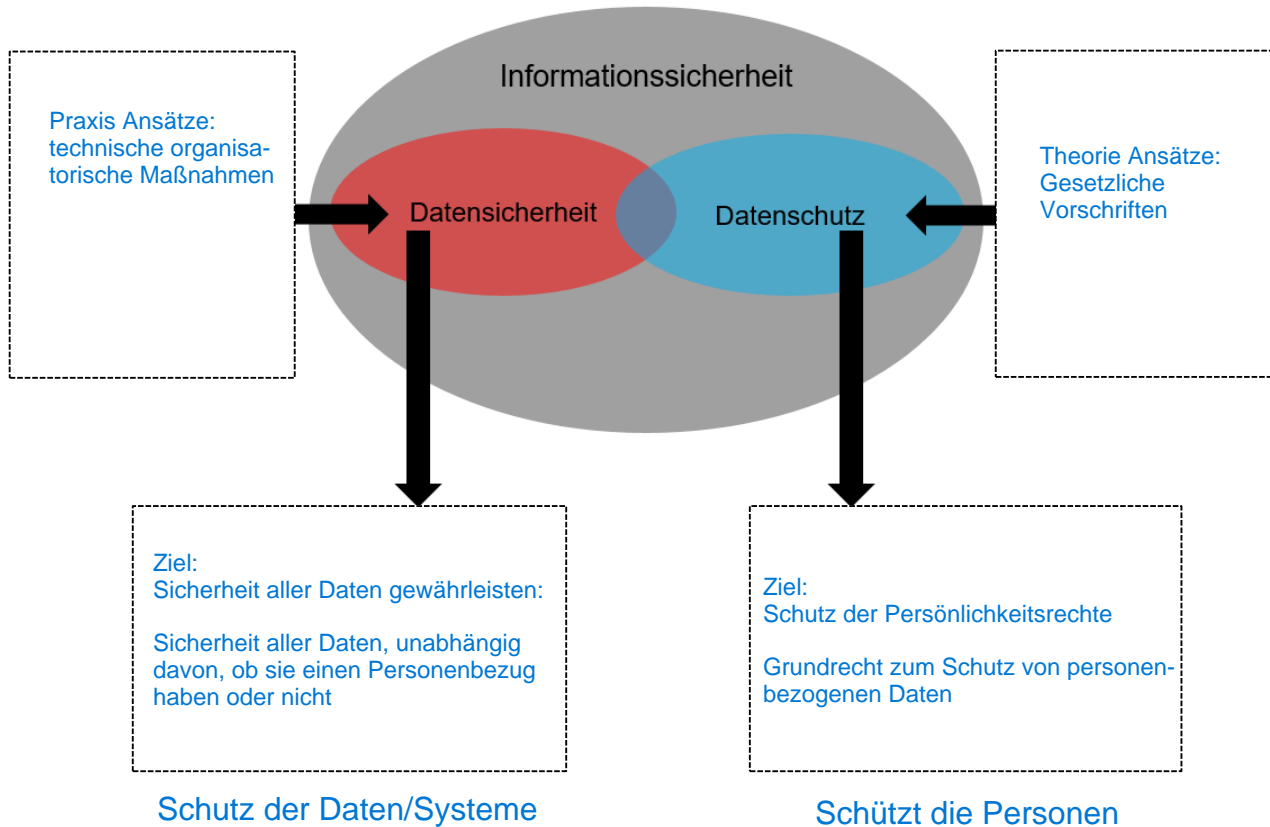
Diese Prinzipien werden auch im **CIA-Dreieck** (Confidentiality, Integrity und Availability) zusammengefasst.

Bei allen Bemühungen um Sicherheit darf man folgendes aber nicht vergessen: Werden Maßnahmen zur Erhöhung der Vertraulichkeit eingesetzt leidet darunter die Verfügbarkeit, erhöht man die Verfügbarkeit leidet darunter die Integrität usw.

Man kann diesen Zusammenhang in einem Dreieck darstellen mit den drei Kriterien Vertraulichkeit, Integrität und Verfügbarkeit als Eckpunkte und die Eigenschaften eines Systems oder die Anforderungen an ein System darin als Fläche eintragen.



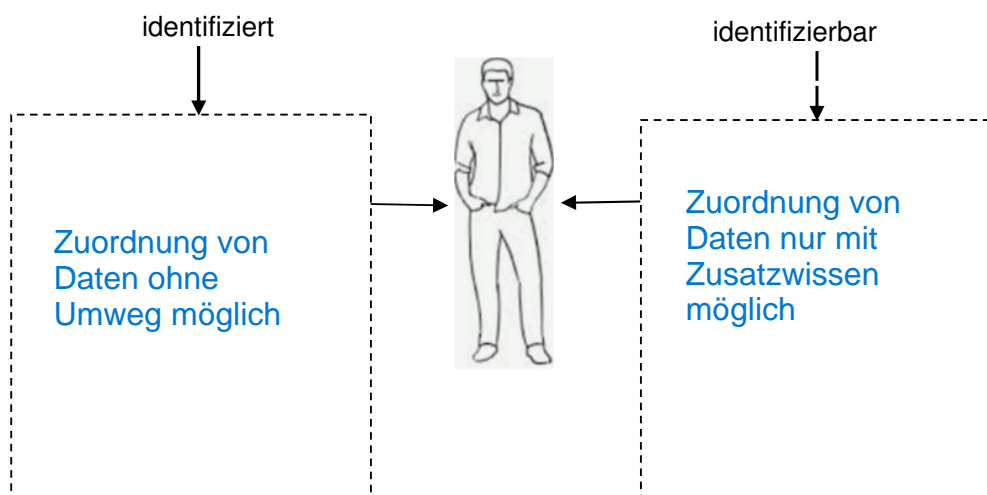
1.3 Datenschutz und Datensicherheit



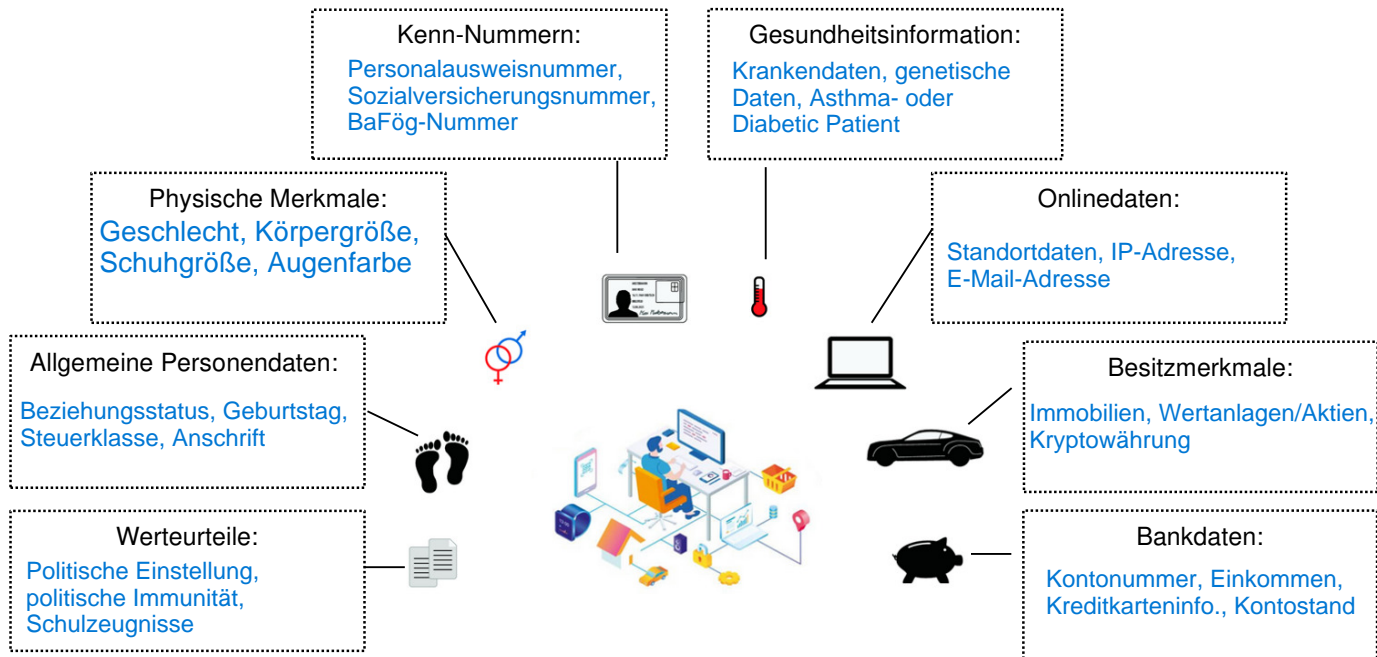
Skript_LF4.docx

Was sind personenbezogene Daten?

Gesetzlich definiert wird der Begriff **personenbezogene Daten** in **Artikel 4** der DSGVO als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen“.



Kategorien von personenbezogenen Daten:



1.4 DSGVO (Datenschutzgrundverordnung)

Ab dem 25. Mai 2018 gilt die Datenschutz-Grundverordnung (DSGVO) der EU.

Die **neue EU-Datenschutzverordnung** ist ein Regelwerk, welches die Handhabung und die Verarbeitung **personenbezogener Daten** innerhalb der europäischen Union vorschreibt.

Die **EU-Datenschutzgrundverordnung** soll einen grenzübergreifenden Datenschutz gewährleisten.

Ziele der DSGVO?

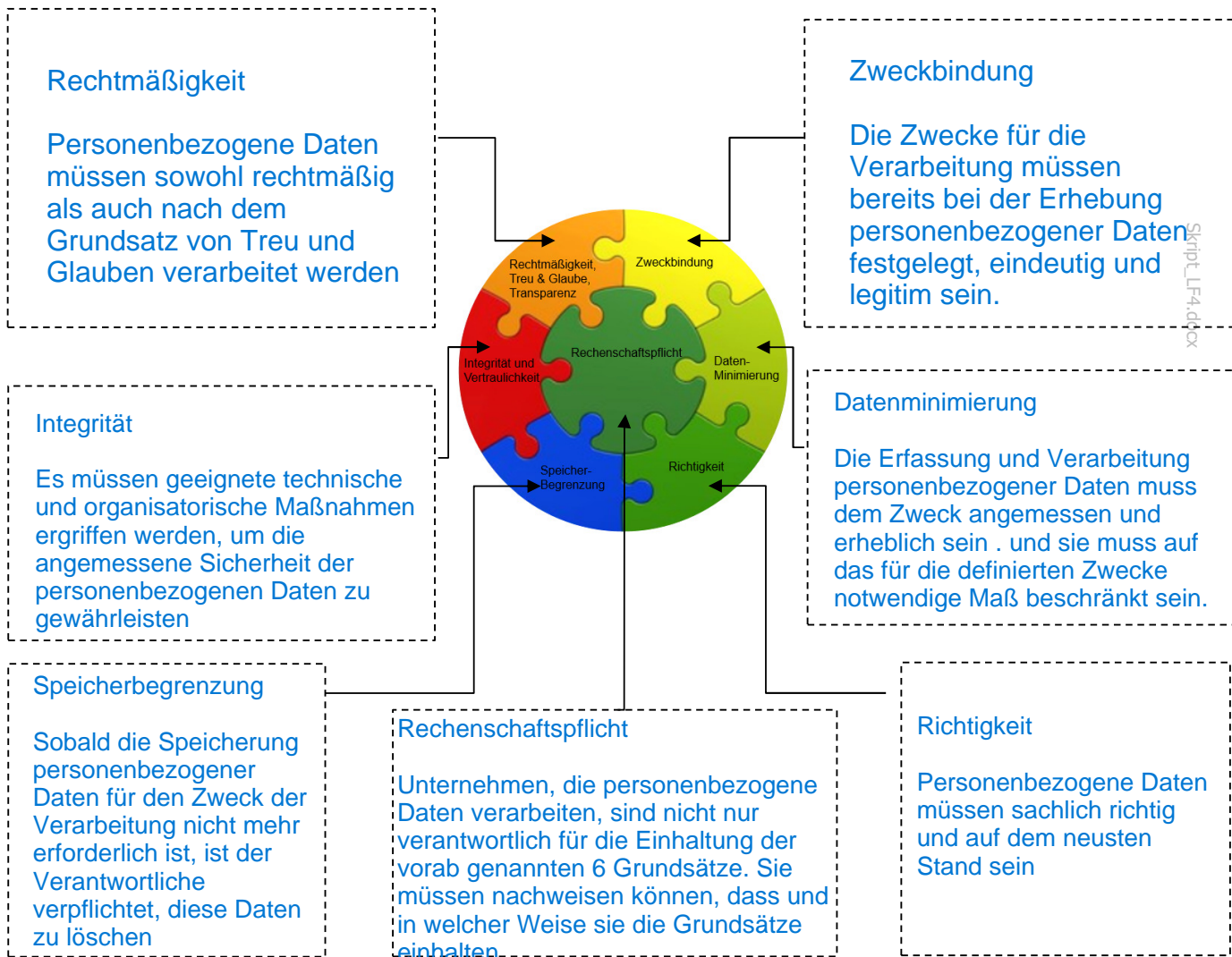


Für wen gilt die DSGVO?

Die DSGVO gilt für alle **Unternehmen, die personenbezogene Daten von EU-Bürgerinnen und Bürgern verarbeiten**. Dabei ist es irrelevant, wo sich der Daten-Verarbeiter geographisch befindet. Der Geltungsbereich der DSGVO umfasst also auch Unternehmen aus Nicht-EU-Ländern, sobald sie personenbezogene Daten von EU-Einwohnern verarbeiten

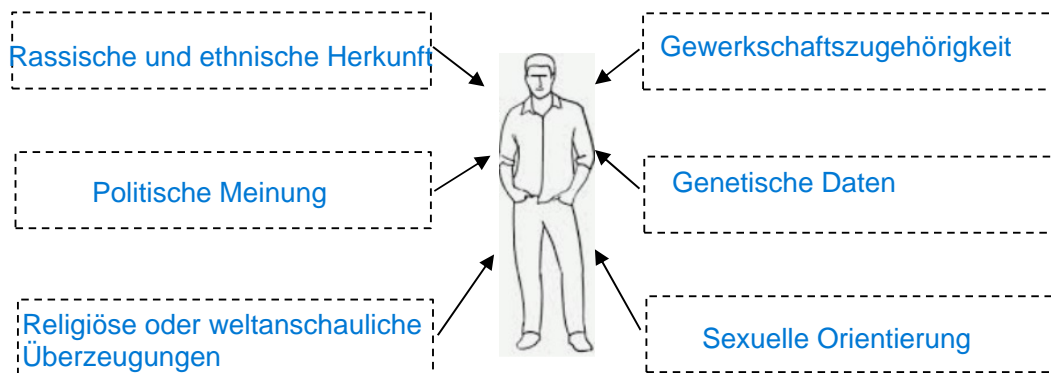
Was fordert die DSGVO für die Speicherung und Verarbeitung personenbezogener Daten?

Das **Fundament der DSGVO** bilden **7 Grundsätze** zur rechtskonformen **Verarbeitung** personenbezogener Daten. Diese Grundsätze sind in **Artikel 5** der DSGVO festgelegt:



Eine **besondere Datenkategorie** mit **grundsätzlichem Verarbeitungsverbot** wird in **§ 9** der DSGVO geregelt:

Diese Daten sind:

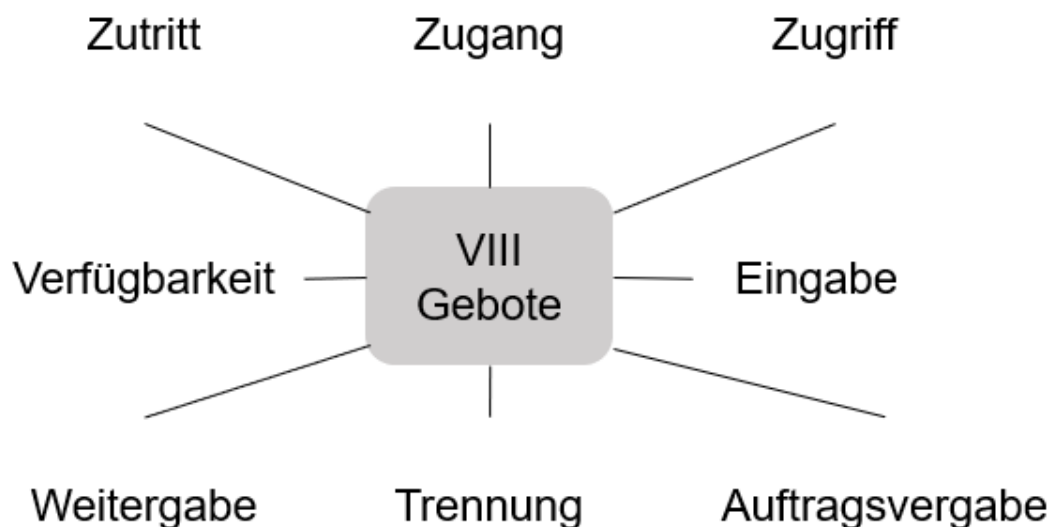


Ausnahmen des Verarbeitungsverbotes ist die Einwilligung des Betroffenen!

Technisch Organisatorische Maßnahmen (TOM) für den Datenschutz

Da die DSGVO bei der konkreten Definition der technisch organisatorischen Maßnahmen (TOM) für den Datenschutz eher vage bleibt, hilft ein Blick ins Bundesdatenschutzgesetz (BDSG).

Die Anlage zu § 9 Satz 1 des Bundesdatenschutzgesetzes (BDSG) enthält die folgenden 8 Regeln für die professionelle Datenverarbeitung in Organisationen, die auch als die **"8 Gebote des Datenschutzes"** bekannt sind:



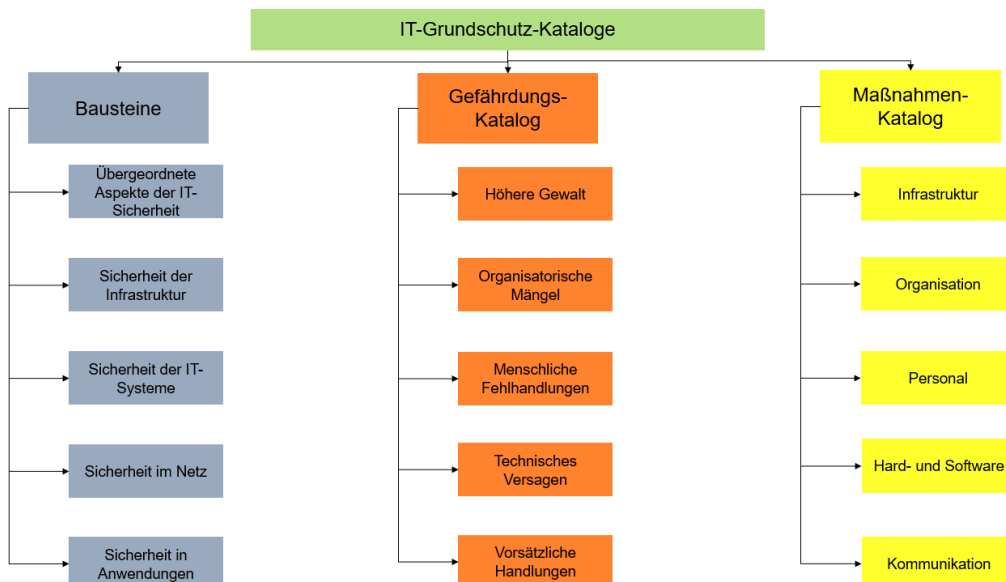
Zutritt	Unbefugten den Zutritt zu Anlagen verwehren
Zugang	Unbefugte daran hindern Systeme zu nutzen
Zugriff	Benutzer haben nur Zugriff auf Daten, wenn sie Berechtigung haben
Eingabe	Sicherstellen, dass im nach hinein nachvollzogen werden kann, wer welche Daten verändert hat (Logdatei)
Auftragsvergabe	Garantieren, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen verarbeitet werden
Trennung	Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden
Weitergabe	Sicherstellen, dass Daten bei Übertragung und Speicherung vollständig, zugriffssicher und nachvollziehbar übermittelt werden
Verfügbarkeit	Daten gegen zufällige Zerstörung oder Verlust geschützt sind

2. Bedrohung der Informationssicherheit

Aufgrund der vielseitigen Bedrohungen für IT-Systeme ist es wichtig, dass die Sicherheit nicht nur als einzelner Baustein angesehen wird, sondern vielmehr als ganzheitliche Aufgabe, die es zu bewältigen gilt. Aus diesem Grund hat das BSI (Bundesamt für Sicherheit in der Informationstechnik) eine Dokumentensammlung erstellt. Diese Dokumentensammlung sind die IT-Grundschutzkataloge. Unternehmen und Behörden können auf Grundlage der IT-Grundschutzkataloge ein Zertifikat nach dem IT-Grundschutz erlangen. Dieses Zertifikat zeichnet Unternehmen und Behörden für das Durchführen geeigneter Maßnahmen zur Absicherung ihrer IT-Systeme gegen IT-Sicherheitsbedrohungen aus.

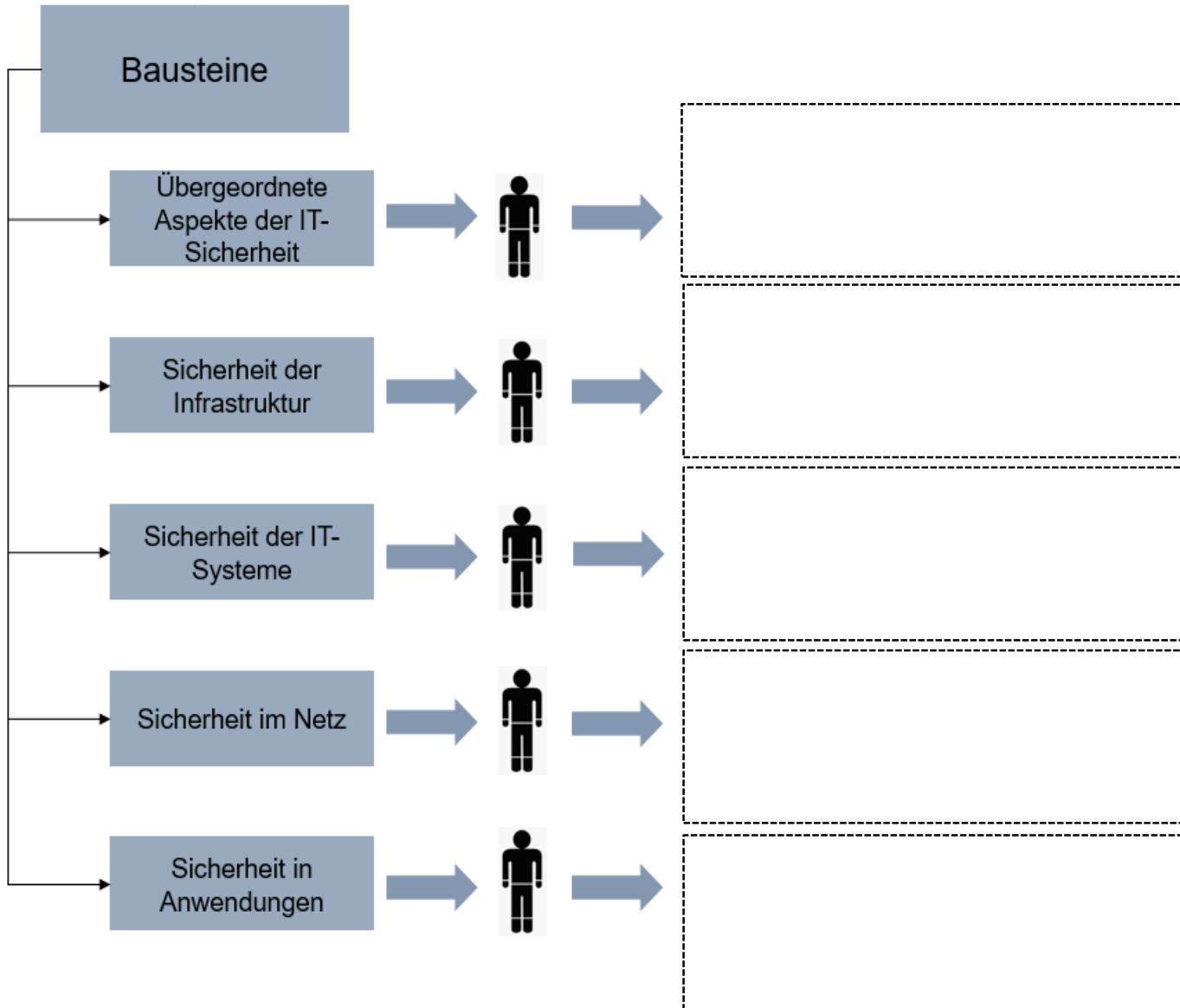
Skript_LF4.docx

2.1 Die IT-Grundschutzkataloge bestehen aus drei Hauptkapiteln:



2.1.1 Der Bausteinkatalog:

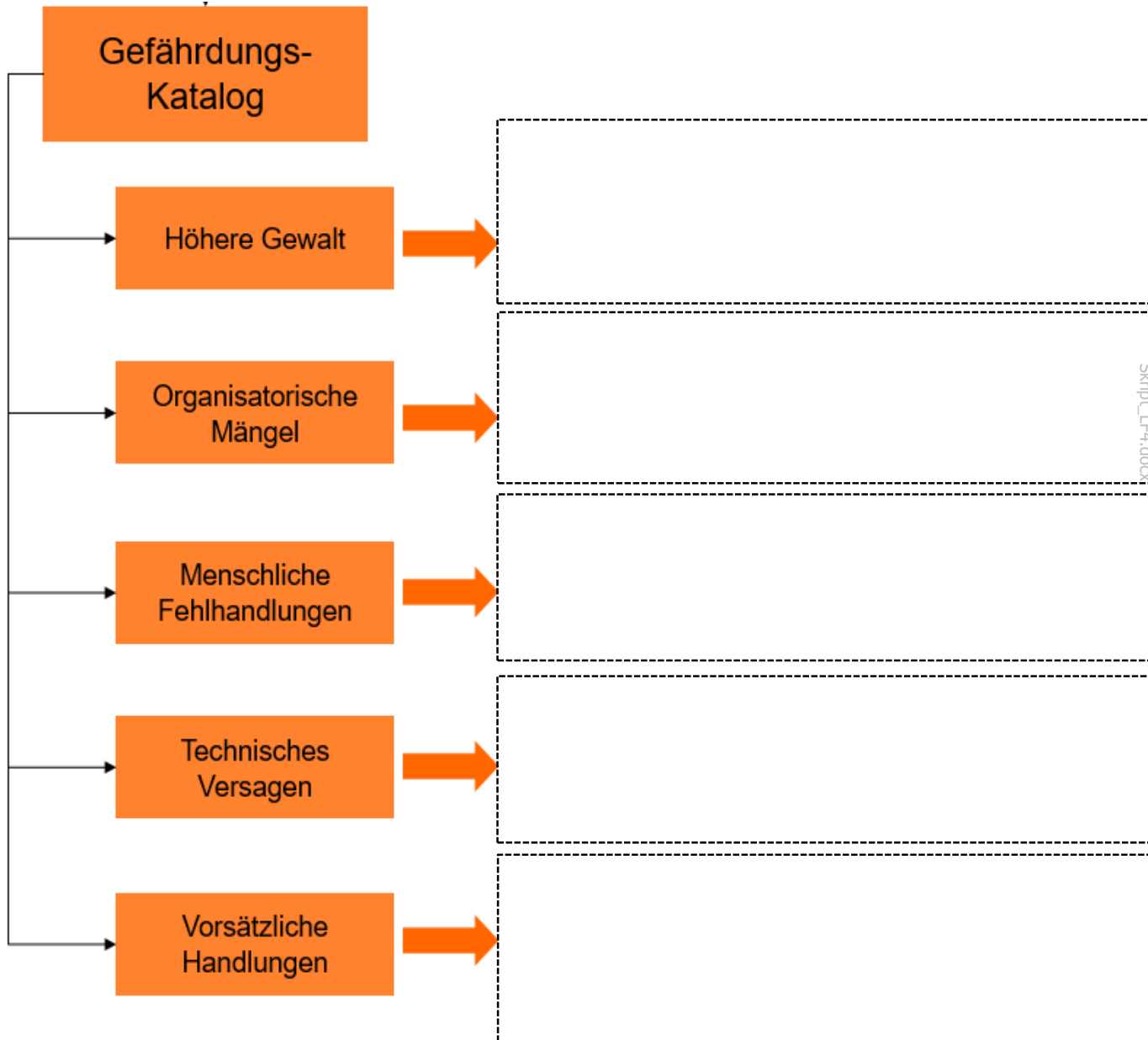
Der Bausteinkatalog ist das zentrale Element und folgt – wie auch die weiteren Kataloge – einem Schichtenmodell.



2.1.2 Der Gefährdungskatalog:

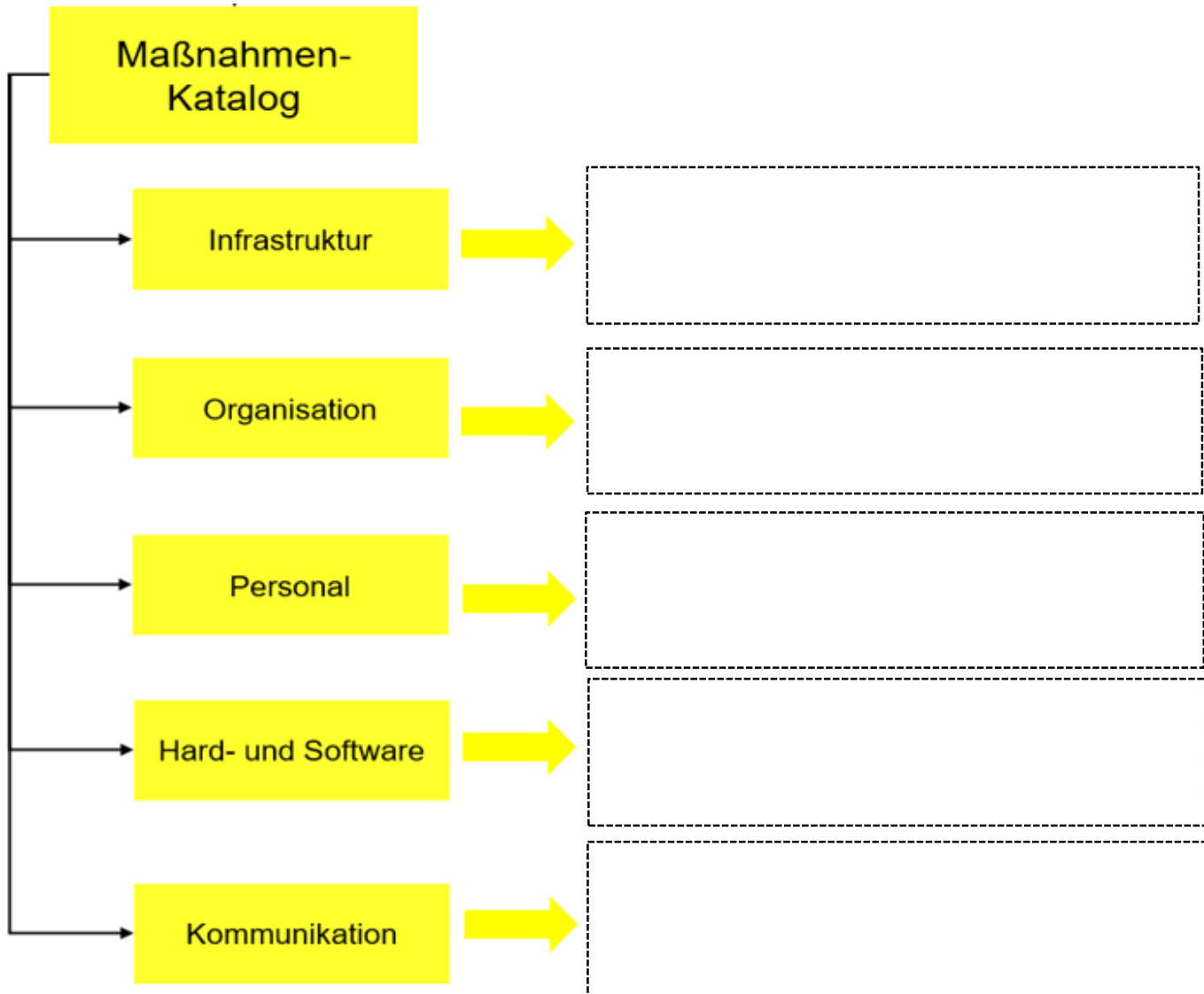
Der Gefährdungskatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) umfasst mehr als 700 verschiedene Bedrohungen. Die Bandbreite der möglichen Gefahren reicht von vorsätzlichen Handlungen, bis hin zu Risiken durch höhere Gewalt.

Der Gefährdungskatalog listet möglichen Gefährdungen für IT-Systeme auf. Dieser Gefährdungskatalog folgt dem allgemeinen Aufbau nach Schichten.



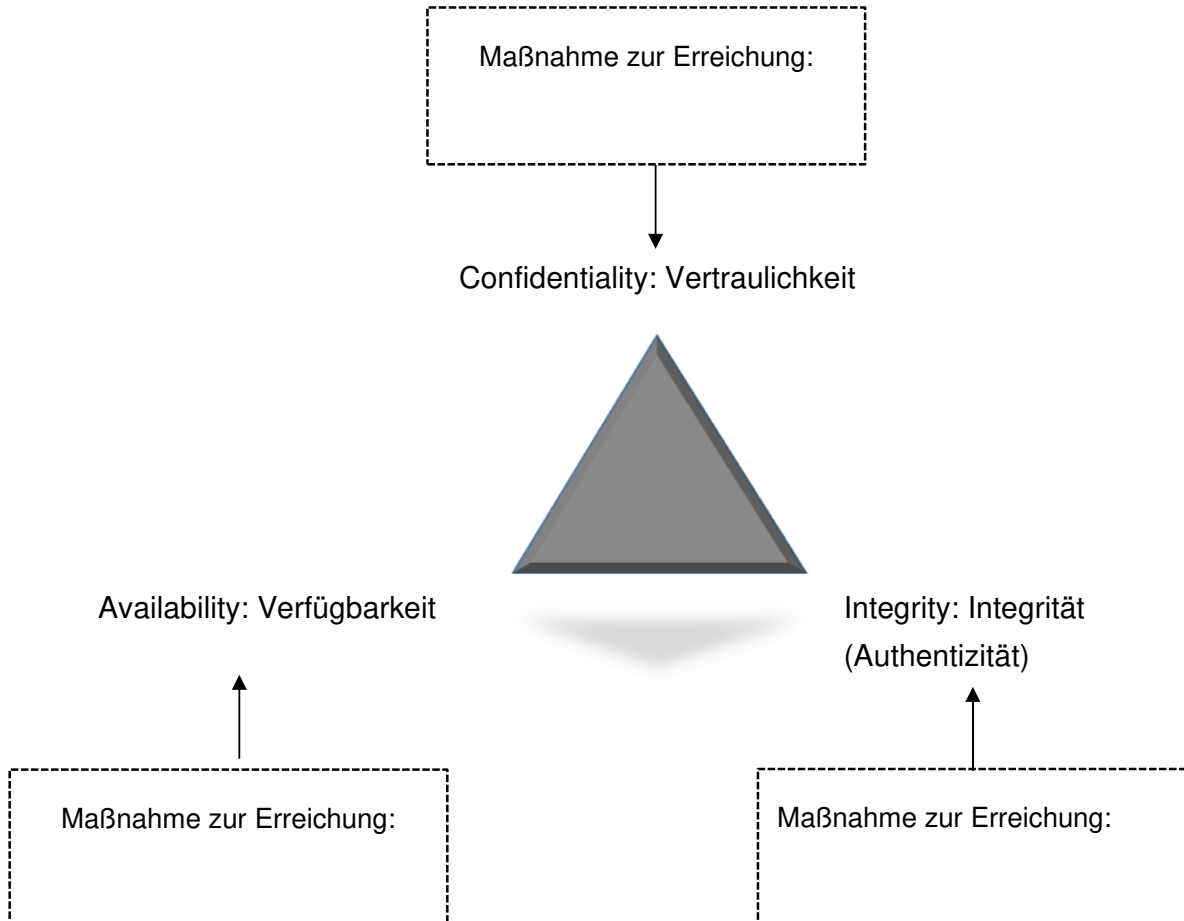
2.1.3 Der Maßnahmenkatalog:

Die zur Umsetzung des Grundschatzes notwendigen Maßnahmen sind in Maßnahmenkatalogen zusammengefasst. Hierbei werden auch Schichten zur Strukturierung der einzelnen Maßnahmengruppen genutzt.



3. Maßnahmen zur Gewährleistung der Informationssicherheit

Das Ziel der Maßnahmen zur Gewährleistung der Informationssicherheit ist es immer, die drei primären Schutzziele der Informationssicherheit Vertraulichkeit, Integrität (Authentizität) und Verfügbarkeit von Informationen aufrecht zu erhalten.



Skript_LF4.docx

3.1 Verschlüsselung

Historische Verschlüsselungstechniken

Verschlüsselung ist keine Erfindung des Computerzeitalters. Es wurden schon immer Wege gesucht, um eine vertrauliche Kommunikation zu ermöglichen, hauptsächlich um militärische Nachrichten vor dem unbefugten Mitlesen abzusichern.

Dazu einige Beispiele:

3.1.1 Cäsar



Die Cäsar-Verschlüsselung ist ein Verschlüsselungsverfahren, bei dem jeder Buchstabe auf einen anderen Buchstaben abgebildet wird. Handelt es sich um eine Verschiebung des Alphabets, muss lediglich der Verschiebungswert als „Schlüssel“ bekannt sein, damit die Nachricht entschlüsselt werden kann. Bei einem Verschiebungswert von 3 wird aus einem A ein D, B wird zu E, usw. Das Wort „WAHR“ lautet verschlüsselt ZDKU.

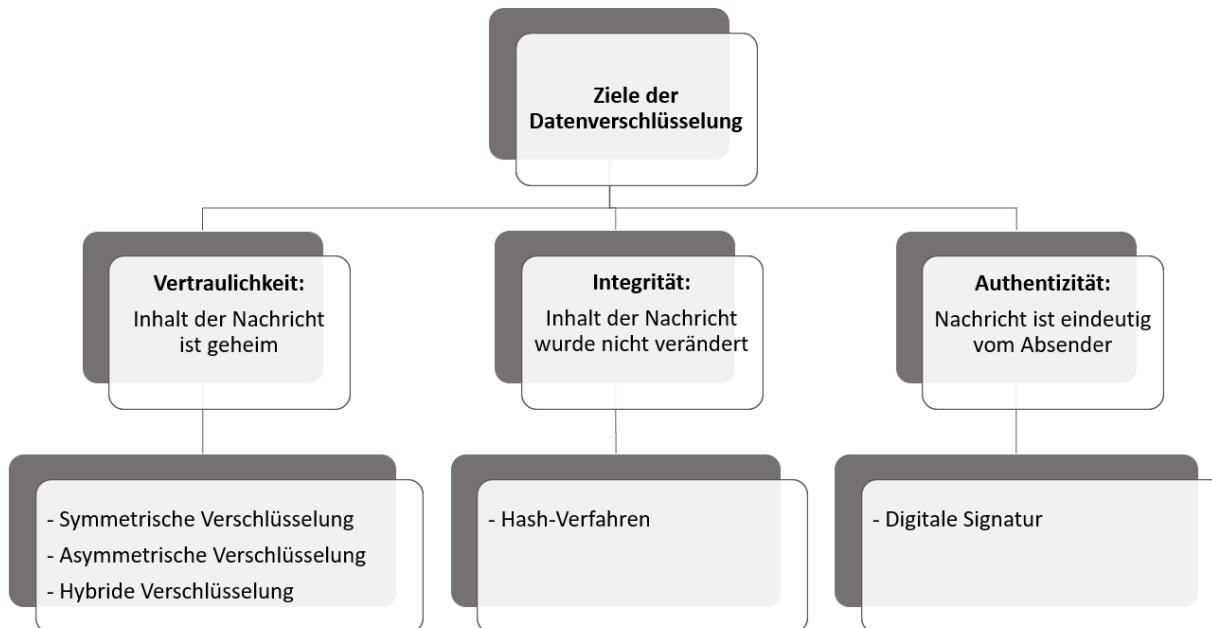
3.1.2 Enigma



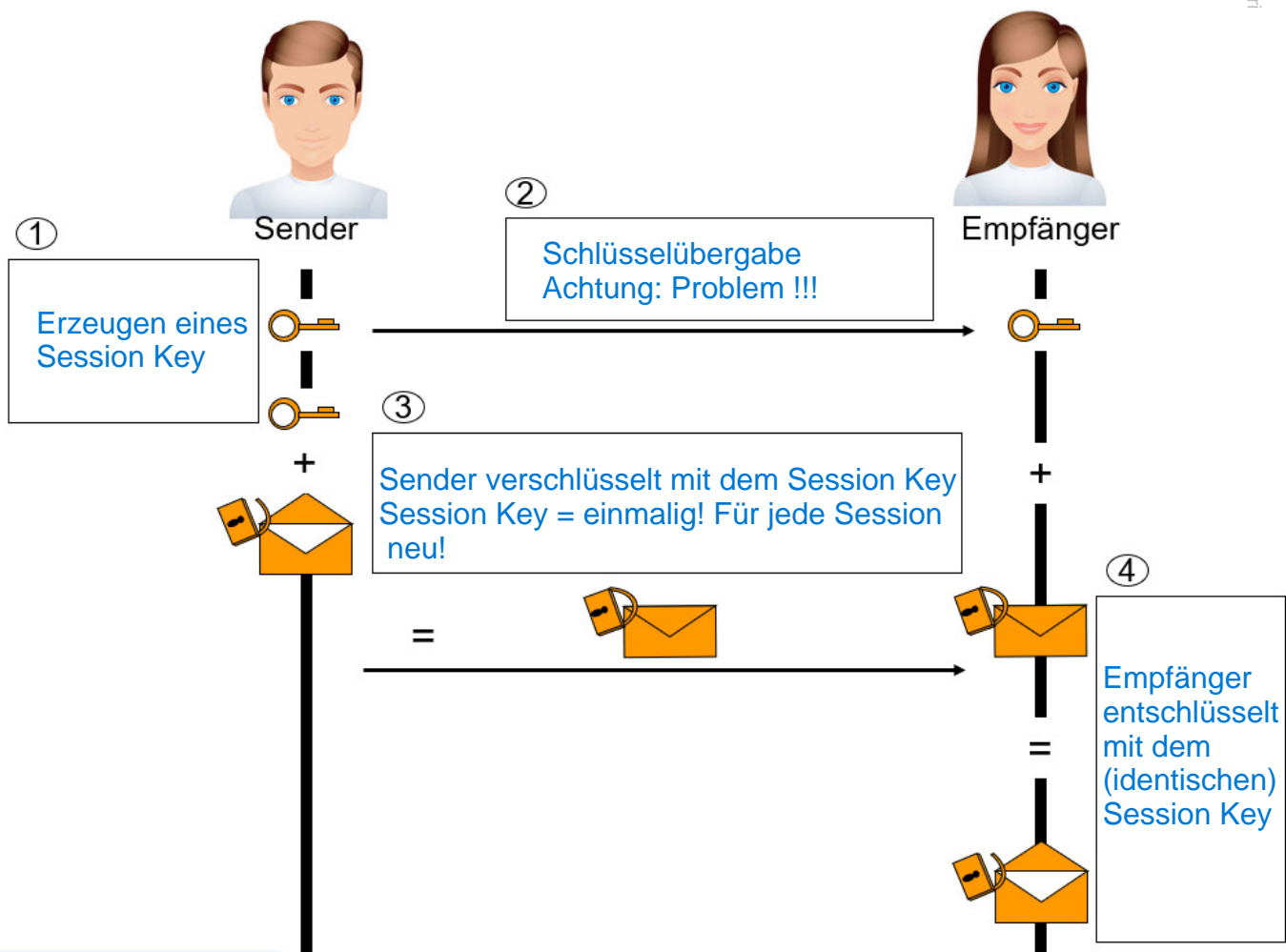
Die Enigma wurde vor allem bekannt, weil sie im zweiten Weltkrieg von der deutschen Wehrmacht zur Verschlüsselung des Nachrichtenverkehrs verwendet wurde. Sie sieht aus wie eine alte Schreibmaschine, besitzt aber drei bewegliche Walzen die miteinander verdrahtet sind. Der Schlüssel, der jedem Kommunikationspartner bekannt sein muss, setzt sich aus mehreren Faktoren zusammen, wie zum Beispiel der Auswahl der Walzen, der Reihenfolge der Montierung, der Verdrahtung oder auch der Grundstellung.

3.2 Aktuelle Verschlüsselungsverfahren

Ziele der Datenverschlüsselung (Kryptografie):



3.2.1 Symmetrische Verschlüsselung



Symmetrische Verschlüsselung ist ein Verfahren, bei dem jeweils derselbe Schlüssel für die Ver- und Entschlüsselung verwendet wird (z.B. DES, 3DES, IDEA, AES). ← häufig Angewendet!

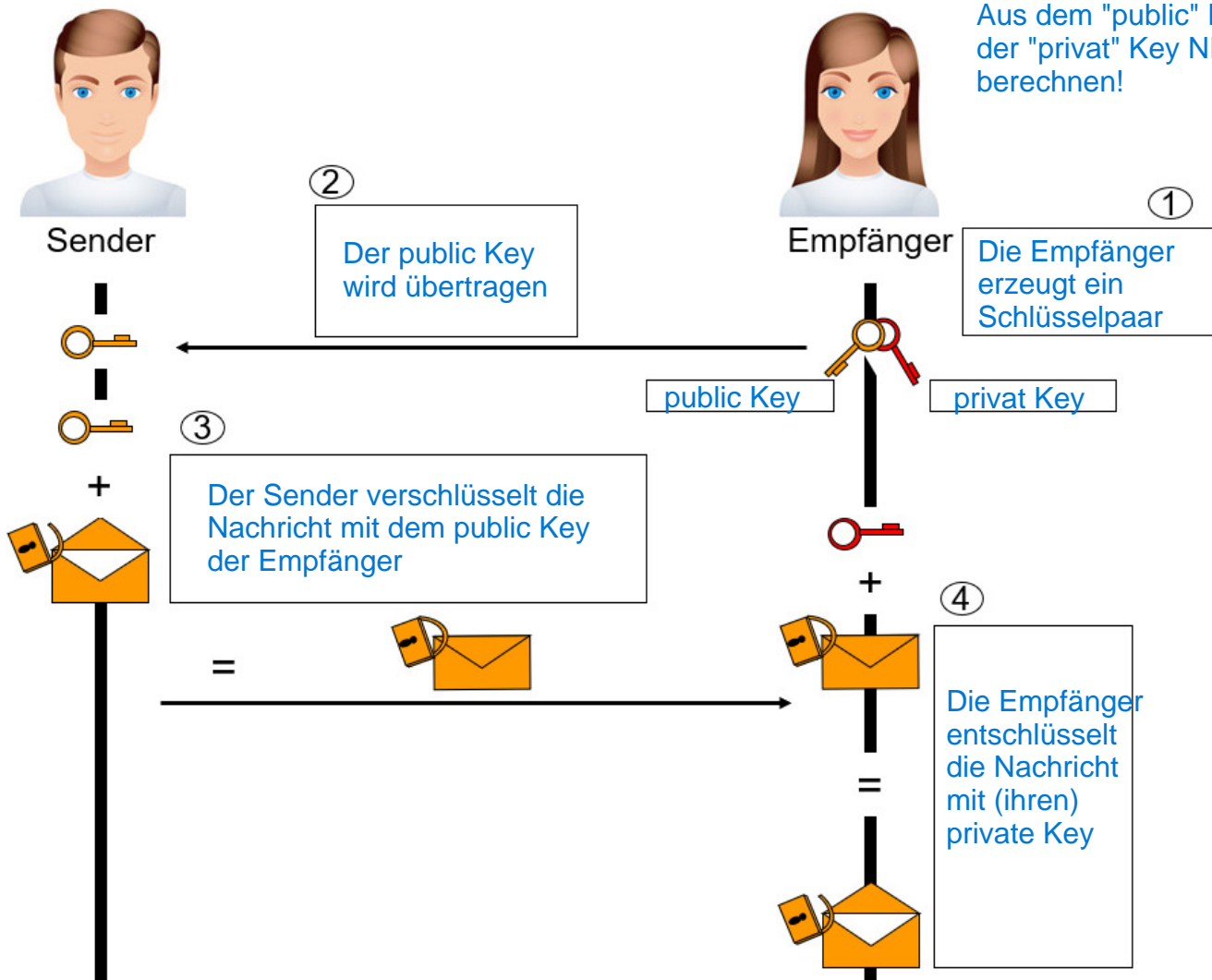
Einsatzgebiete:

- Pay-TV
- In Verbindung mit asymmetrischen Verfahren

3.2.2 Asymmetrische Verschlüsselung

Sender erzeugt (einmalig) ein Schlüsselpaar aus "privat" und "public" Key. Die Schlüssel stehen in einem mathematischen Zusammenhang: Was mit dem "public" Key verschlüsselt wurde, lässt sich nur mit dem "private" Key entschlüsseln (und umgekehrt)

Aus dem "public" Key lässt sich der "privat" Key NICHT berechnen!



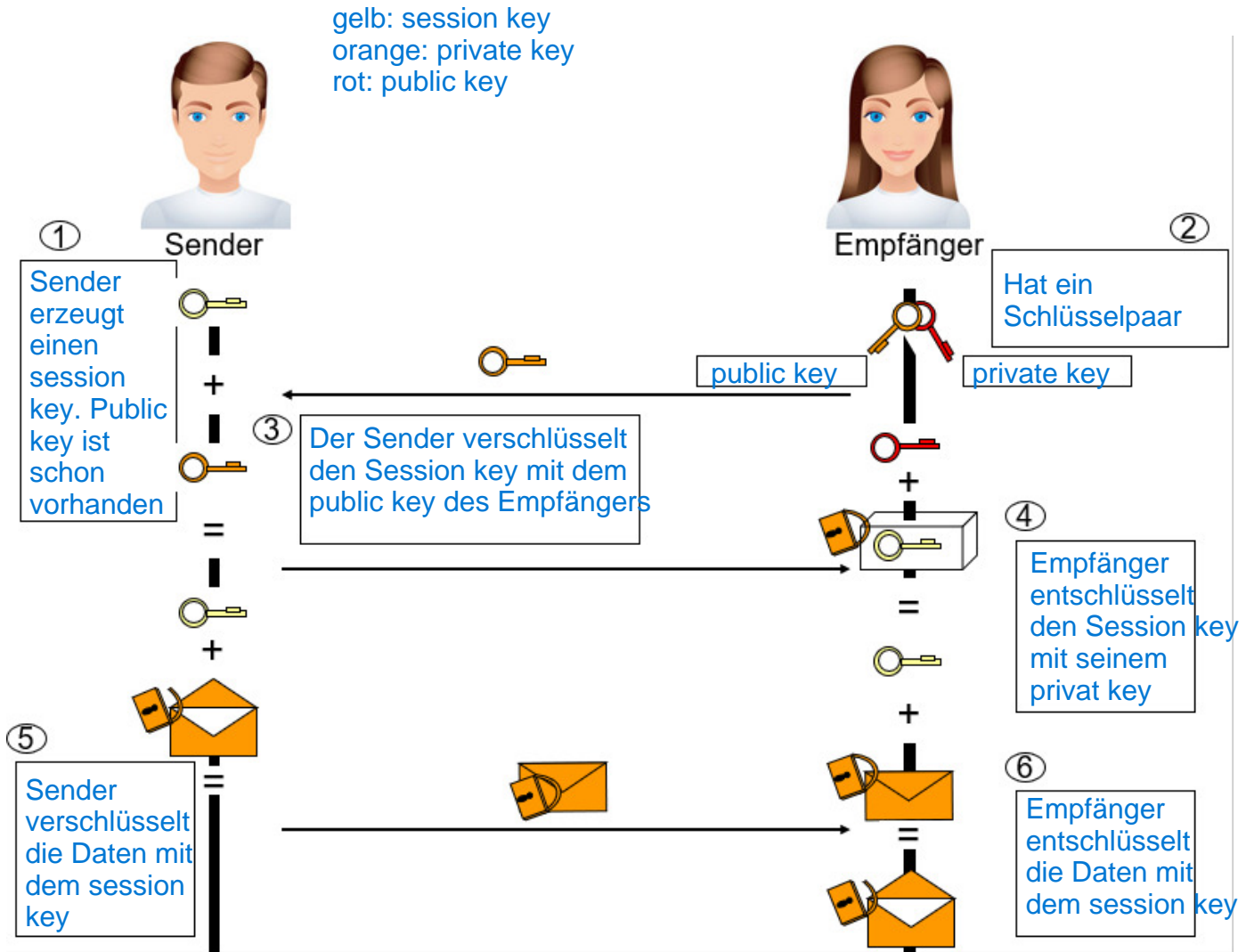
Diese sind Verschlüsselungsverfahren, bei denen sich die Schlüssel für Ver- und Entschlüsselung unterscheiden. Meist wird der öffentliche *Public Key* zum Verschlüsseln, der geheime *Private Key* zum Entschlüsseln verwendet (z.B. RSA).

Einsatzgebiete:

- E-Mail-Verkehr
- https
- SSL

3.2.3 Hybride Verschlüsselung

Die hybride Verschlüsselung kombiniert die symmetrische und die asymmetrische Verschlüsselung und vermeidet jeweils deren Nachteile. Die zu übertragende Nachricht wird symmetrisch verschlüsselt. Der dafür nötige Schlüssel wird vorher asymmetrisch verschlüsselt übertragen. (z.B. SSH, HTTPS, SSL/TLS).



Vergleich von symmetrischer und asymmetrischer Verschlüsselung

	Symmetrische Verschlüsselung	Asymmetrische Verschlüsselung
Vorteile	- sehr performant (weil Schlüssel kürzer ist)	- Problem der Schlüsselübertragung ist gelöst
Nachteile	- Problem der Schlüsselübermittlung	- sehr rechenaufwändig, zeitaufwändig faktor 1.000 - 10.000 mal langsamer als symmetrisch

Schlüsselraum:

Von der Länge des Schlüssels, also der Zahl der Bitstellen ergibt sich die Menge der Möglichkeiten, aus denen ein Schlüssel ausgewählt werden kann. Diese Menge nennt man *Schlüsselraum*.

Um eine hohe Sicherheit zu gewährleisten, sollte der Schlüsselraum möglichst groß gewählt werden.

Beispiel: Mit einer Schlüssellänge von 40 Bit erhält man $2^{40} = 1,1 \times 10^{12}$ Möglichkeiten. Mit leistungsstarken Prozessoren oder durch den Zusammenschluss vieler Rechner (z.B. Cloud, Cluster) lassen sich mehr als 10¹¹ Schlüssel pro Sekunde testen. Alle Möglichkeiten bei 40 Bit Schlüssellänge auszuprobieren, würde dann lediglich 11 Sekunden dauern.

Aufgaben:

- 1.) Geben Sie die üblichen Schlüssellängen bei den unten angegebenen Verschlüsselungsverfahren an.

Symmetrische Verfahren		Asymmetrische Verfahren	
DES (Data Encryption Standard)		RSA (Rivest-Shamir-Adleman)	
3DES			
IDEA (International Data Encryption Algorithm)			
AES (Advanced Encryption Standard)			

- 2.) Ein Verschlüsselungsverfahren benutzt eine Schlüssellänge von 64 Bit.

- a) Wie lange bräuchte man maximal mit einem leistungsstarken Rechner, das 10^{11} Schlüssel pro Sekunde testen kann, um das System zu knacken?

- b) Ein 64-Bit-Schlüssel wird von einem Rechner in 60 Minuten entschlüsselt. Durch die Verwendung eines 78-Bit-Schlüssels soll die Zeit zur Entschlüsselung bei gleicher Rechenleistung auf mehrere Wochen erhöht werden. Ermitteln Sie die Entschlüsselungszeit in Wochen. Der Rechenweg ist anzugeben.

- 3.) Um wie viel Bit muss die Schlüssellänge mindestens erhöht werden, wenn die maximale Entschlüsselungszeit mindestens um den Faktor 100 verlängert werden soll?

Skript_LF4.docx

3.3 Digitale Signatur

Mit fortschreitender Digitalisierung wird es immer wichtiger, Daten sicher zu transportieren und Unterschriften digital abzubilden – und dass bei hoher Rechtsgültigkeit. Ob beim elektronischen Geschäftsverkehr mit Kunden oder Partnern, in der Behördenkommunikation oder bei internen Abläufen: Für sensible Dokumente und Daten ist zu gewährleisten, dass

- der Absender der Daten *authentisch* ist und
- die digital verschickten Daten nicht verändert wurden und damit unverfälscht sind (= *Integrität* der Daten).

Mit der elektronischen Unterschrift sind diese Anforderungen erfüllt.

Was leistet eine digitale Signatur?

Eine elektronische Signatur stellt das elektronische Äquivalent zur handschriftlichen Unterschrift dar, d.h., sie kann dazu benutzt werden, um:

- die Unverfälschtheit eines elektronischen Dokumentes sicher zu überprüfen
⇒ **Integrität**
- den Unterzeichner eines elektronischen Dokumentes sicher zu identifizieren
⇒ **Identität (Authentizität)**

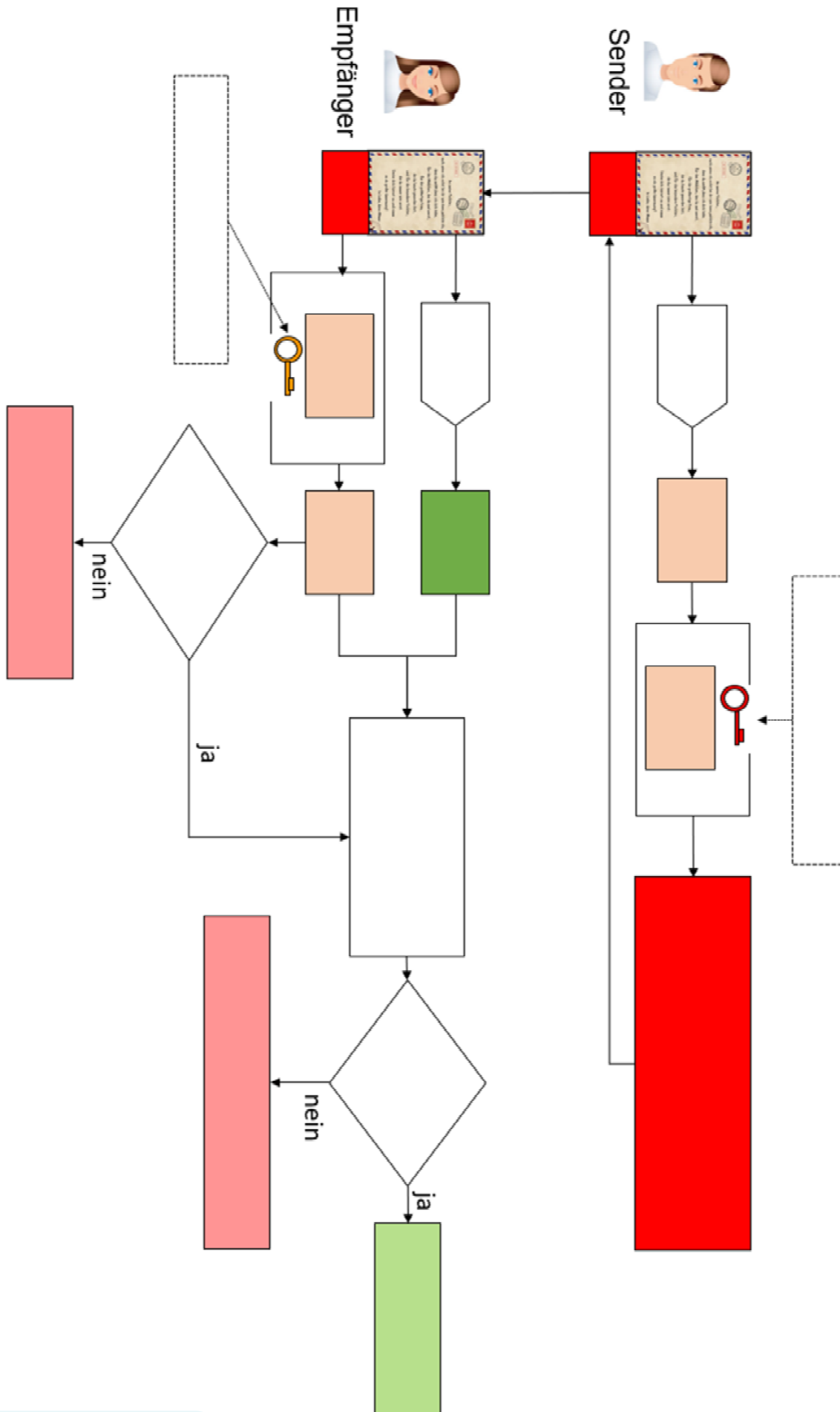
Die Überprüfung der Integrität des Dokumentes und die Identität des Absenders erfolgt mittels Hashing.

Als Hashing bzw. Hashfunktion wird ein Algorithmus bezeichnet, der eine digitale Eingabe beliebiger Länge auf eine immer gleiche, eindeutige Ausgabe fester Länge abbildet.

Bekannte Hash-Verfahren: MD5, SHA-1 oder SHA-256.

In den nachfolgenden Beispielen wurde das Hashverfahren SHA-1 verwendet. Hier sieht man vor allem zwei wichtige Merkmale sehr deutlich, nämlich dass die Länge der Hashes immer gleich ist und dass nur kleine Änderungen an der Eingabe zu einem völlig neuen Hash führen:

Eingabe	SHA-1 Ausgabe
Hallo	59d9a6df06b9f610f7db8e036896ed03662d168f
hallo	fd4cef7a4e607f1fcc920ad6329a6df2df99a4e8
Hello	f7ff9e8b7bb2e09b70935a5d785e0cc5d9d0abf0



Skript_LF4.docx

Aufgaben:

1.) Für den E-Mail-Verkehr werden folgende drei IT-Sicherheitsziele gefordert. Nennen Sie jeweils ein geeignetes Verfahren, um die folgenden Forderungen zu erfüllen.

a.) Vertraulichkeit der E-Mail:

b.) Authentizität der E-Mail:

c.) Integrität der E-Mail:

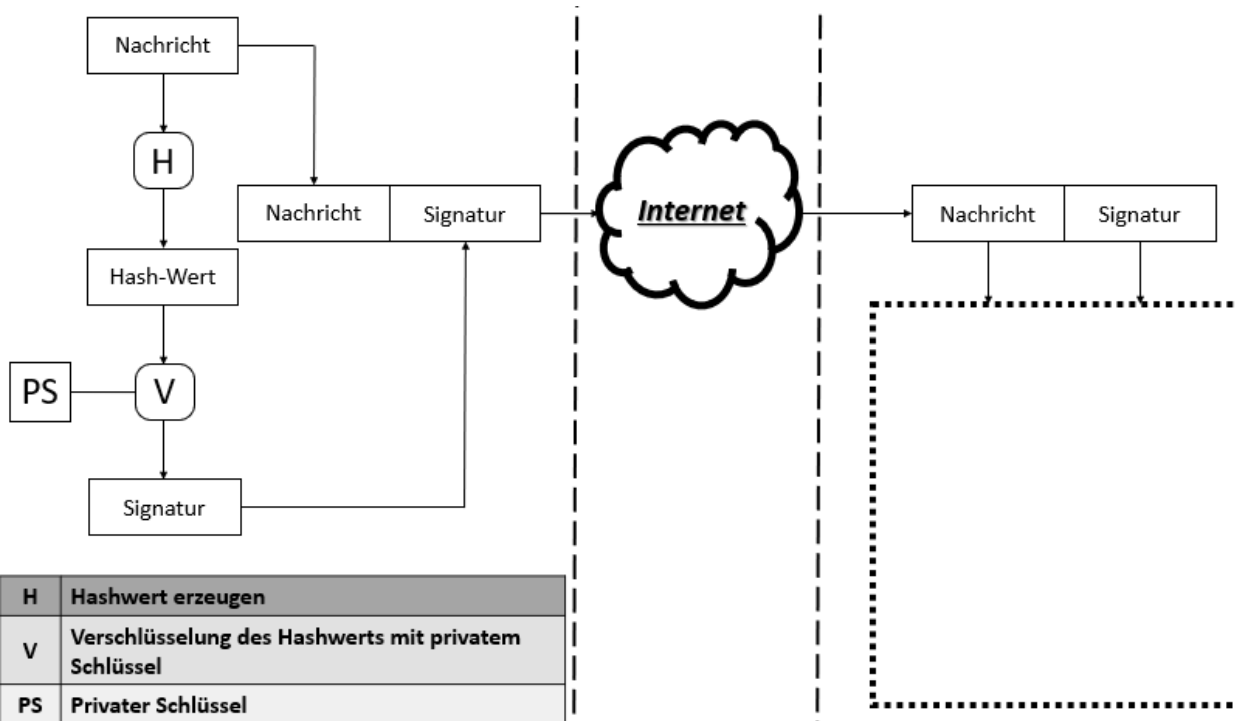
2.) Ausgehende E-Mails werden digital signiert. Sie sollen das Verfahren der asymmetrischen digitalen Signatur anhand einer Grafik darstellen. Vervollständigen Sie die folgende Grafik, indem Sie die Verifizierung (Prüfung der Signatur) auf Empfängerseite ergänzen.

Sender

(Signierung)

Empfänger

(Verifizierung)



3.) Erläutern Sie zwei wichtige Anforderungen, die ein Hash-Algorithmus, z.B. MD5 oder SHA 1, erfüllen muss.

3.4 RAID

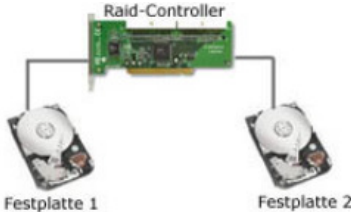
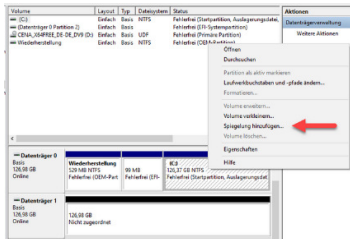
RAID

► Redundant Array of Independent Disks

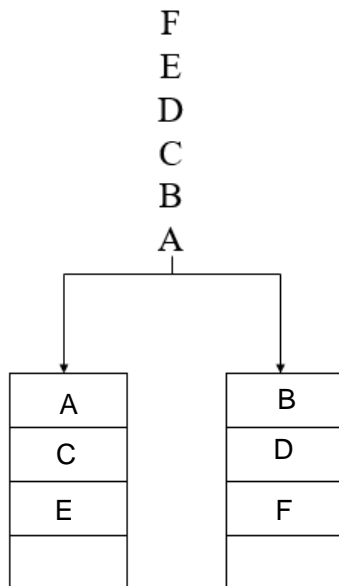
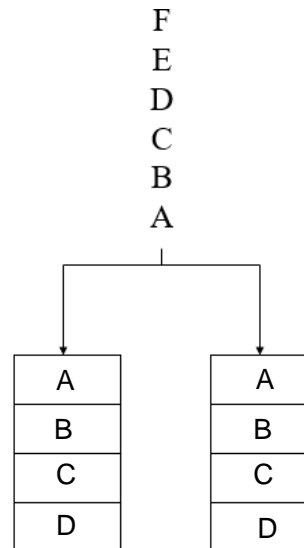


- Zusammenfassung mehrerer Festplatten zu einem Array, welches das Betriebssystem wie eine einzige große Festplatte verwaltet.
- Steigerung der Performance durch die gleichzeitige Nutzung mehrerer Laufwerke, auf denen die Daten verteilt sind.
- Erhöhung der Sicherheit und Verfügbarkeit der Daten durch Redundanz.
- RAID-Systeme lassen auf unterschiedliche Art und Weise aufbauen, man unterscheidet dabei verschiedene Level.
- Man unterscheidet zwischen:

Skript_LF4.docx

<h2>Hardware RAID</h2> 	<h2>Software-Raid</h2> 
<ul style="list-style-type: none"> + RAID-Funktionalität steht unabhängig vom Betriebssystem zur Verfügung + Entlastung der CPU des Systems durch eigene CPU auf dem Controller - Anschaffungskosten Controller - Bei einem Defekt vom Controller ist ein kompatibles Modell notwendig 	<ul style="list-style-type: none"> + Keine Kosten für RAID-Controller + RAID kann auch auf einer anderen Installation des Betriebssystems wieder genutzt werden - höhere CPU-Belastung - Funktionen wie automatische Wiederherstellung der Redundanz bei Ausfall einer Festplatte sind nicht gegeben

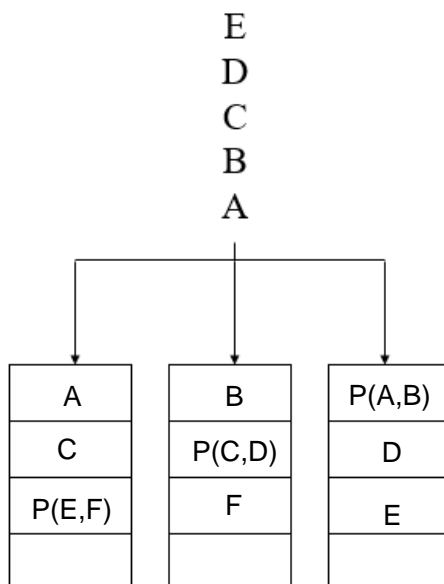
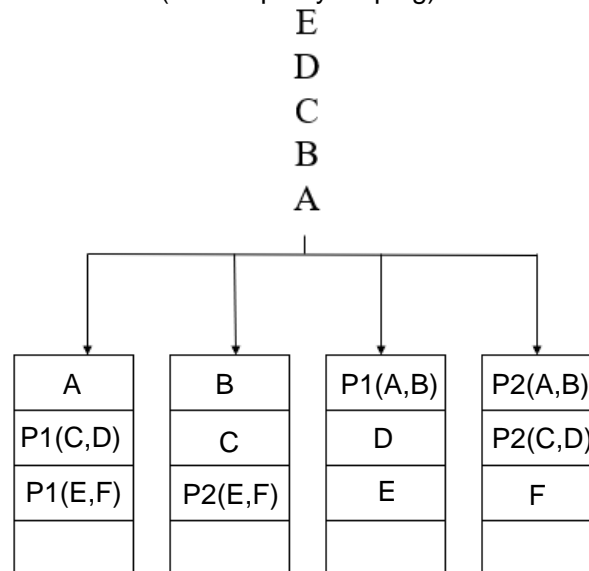
RAID-Level

RAID-0 (Striping)**RAID-1 (Mirroring)**

n = Anzahl Datenträger

Mindest-Plattenanzahl:	2	Mindest-Plattenanzahl:	2
Datensicherheit:	Nein	Datensicherheit:	Ja
Kapazität:	100%	Kapazität:	50% 1/n
tolerierter Ausfall:	0 / Keine	tolerierter Ausfall:	n-1

Performance: 200%

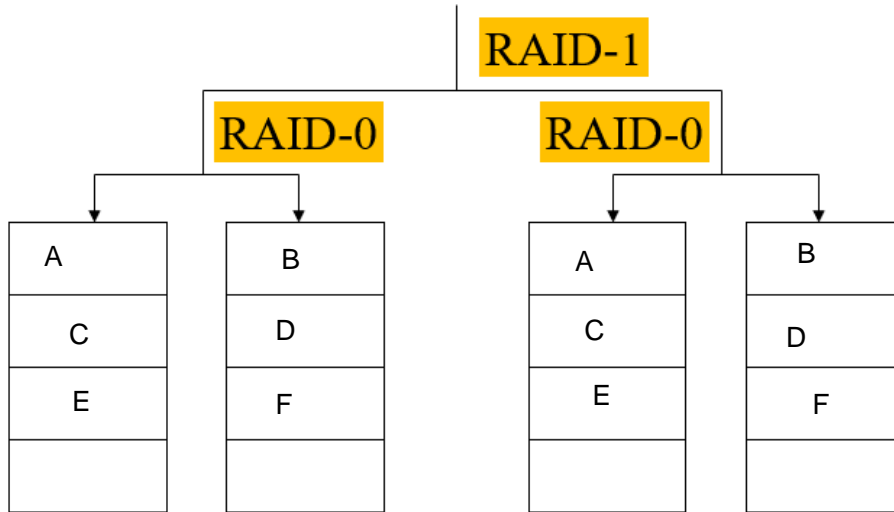
RAID-5 (Parity Striping)**RAID-6**
(double parity striping)

Mindest-Plattenanzahl:	3	Mindest-Plattenanzahl:	4
Datensicherheit:	Ja	Datensicherheit:	hoch
Kapazität:	n-1	Kapazität:	n-2
tolerierter Ausfall:	1	tolerierter Ausfall:	2

RAID-01

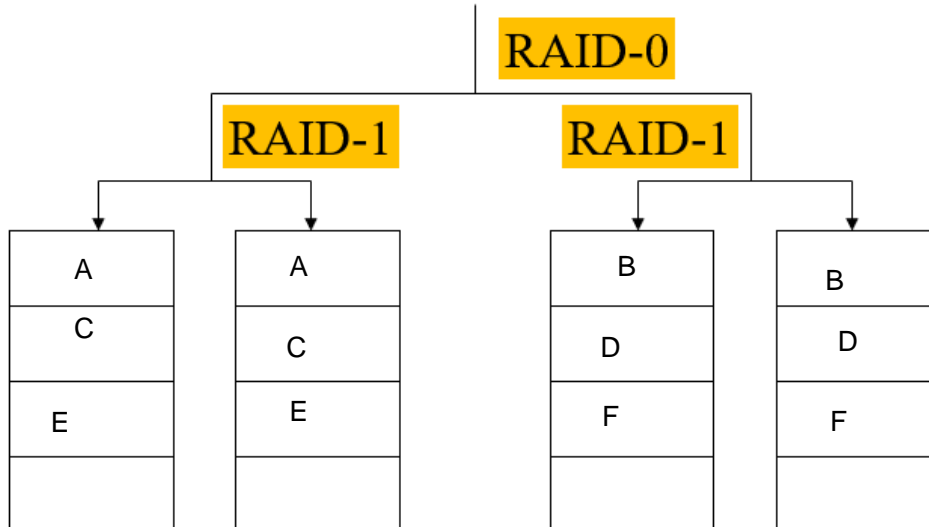
E
D
C
B
A

SMART = Safe Monitoring Reporting Technology
JBOD = Just A Bunch Of Disks
Hot Spare = "Reserve-Platte" für den Fehlerfall
AFR/MTBF = Annualized Failure Rate / MeanTime Between Failure



RAID-10

E
D
C
B
A



Skript_LF4.docx

Aufgaben:

1.) Sie haben ein RAID-Controller mit zehn identischen Festplatten. Die Kapazität jeder Festplatte beträgt 400 GiB.

a.) Ermitteln Sie rechnerisch die Netto-Speicherkapazität bei RAID-Level 6!

Kapazität 1 Platte (n) = 400GiB

Kapazität gesamt: $400\text{GiB} \cdot 10 = 4000\text{ GiB}$

Kapazität Nutzbar: $4000 - 800 = 3200\text{ GiB}$

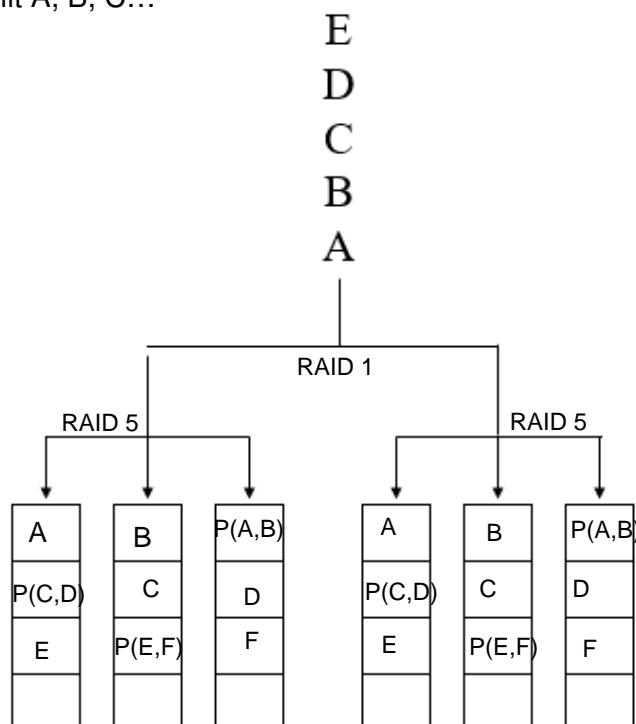
b.) Ermitteln Sie rechnerisch die Netto-Speicherkapazität bei RAID-Level 51!

Kapazität Nutzbar: $n-1 = 4000\text{GiB} - 400\text{GiB} = 3600\text{GiB} / 2 = 1800\text{GiB}$

2.) Vervollständigen Sie die untere Tabelle!

	RAID-Level				
	RAID-5	RAID-6	RAID-10	RAID-50	RAID-55
Netto-Speicherkapazität in % bei 6 Platten	50%	75%	50%	90%	

3.) Skizzieren Sie nachfolgend ein RAID-51-Array mit 6 Platten. Stellen Sie deutlich heraus, wie die Datenblöcke auf den einzelnen Festplatten verteilt werden und benennen Sie die Datenblöcke mit A, B, C...



3.5 Datensicherung (Backup und/oder Archivierung)

____> externes!!!

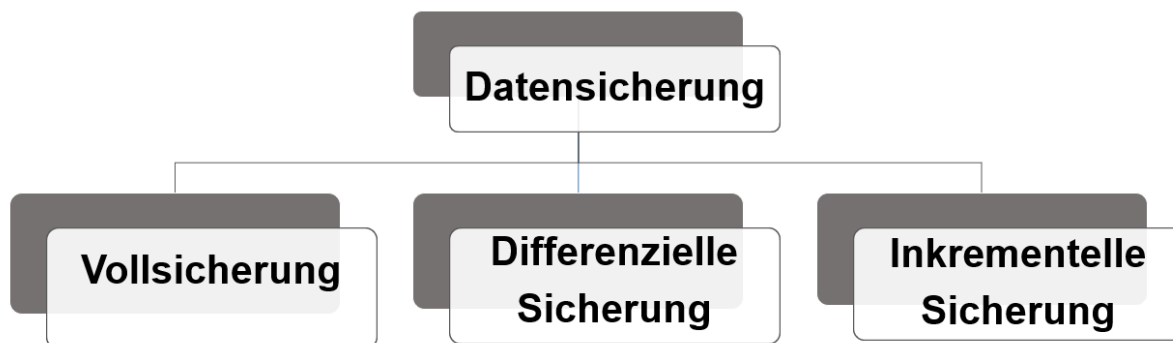
Datensicherung bezeichnet das Kopieren von Daten auf ein alternatives Speichermedium in der Absicht, diese im Fall eines Datenverlustes zurückkopieren zu können. Die gesicherten Daten werden als *Sicherungskopie*, oft auch als *Backup* bezeichnet. Die Wiederherstellung der Daten aus einer Sicherungskopie bezeichnet man als *Datenwiederherstellung*, *Datenrücksicherung* oder *Restore*.

Ziele der Datensicherung

- Gewährleisten der Datensicherheit, um ungeplante Ausfallzeiten (*Downtime*) zu vermeiden
- Entgangene Geschäfte und möglichen Konkurs vermeiden
- Gesetzliche Auflagen zur Speicherung oder Archivierung von Daten einhalten

Datensicherungsstrategien (Backup-Strategien)

Unter Datensicherungsstrategien versteht man die Art und Weise, wie Datensicherungen durchgeführt werden. Dabei wird grundsätzlich zwischen vollständiger Datensicherung, inkrementeller Datensicherung und differenzielle Datensicherung unterschieden.



Skript_LF4.docx

3.5.1 Vollsicherung

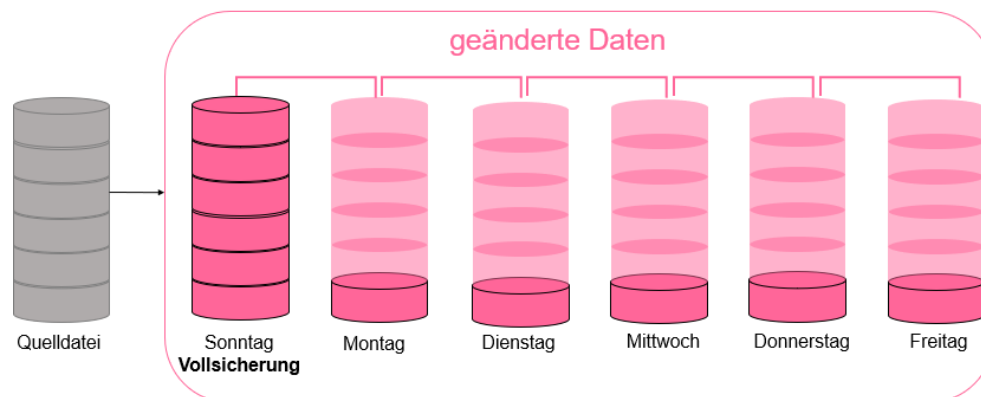
Bei einer **Vollsicherung** werden jedes Mal alle zu sichernden Daten in einer Sicherungsdatei auf dem Zieldatenträger gespeichert. Dadurch sind alle gesicherten Daten in nur einer Datei enthalten, was die Verwaltung der Backups vereinfacht.



3.5.2 Inkrementelle Sicherung

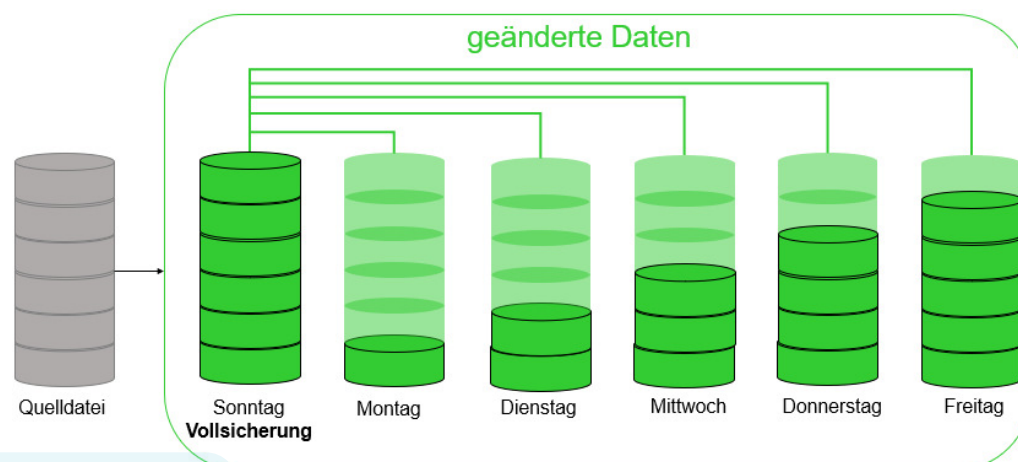
Bei einem **inkrementellen Backup** handelt es sich um eine Methode der Datensicherung, bei der nach einer ersten Vollsicherung ausschließlich die Dateien oder Informationen gesichert werden, die sich seit den vorangegangenen **inkrementellen Backups** verändert haben oder neu hinzugekommen sind.

Skript_LF4.docx



3.5.2 Differenzielle Sicherung

Ein **differenzielles Backup** ist eine Datensicherung, die alle Dateien kopiert, die seit der letzten vollständigen Sicherung geändert wurden. Diese schließt alle Daten ein, die auf irgendeine Weise erstellt, aktualisiert oder geändert wurden, und kopiert nicht jedes Mal alle Daten.



Das Archiv-Bit

Das Archivbit ist ein Dateiattribut, das genutzt wird, um neu angelegte oder veränderte Dateien zu kennzeichnen. Datensicherungsprogrammen kann damit signalisiert werden, dass die Datei noch nicht gesichert bzw. seit der letzten Sicherung modifiziert wurde.

Aktion	Archive-Bit		
	wird gesetzt	wird zurückgesetzt	wird nicht geändert
Eine Datei erstellen	X		
Eine Datei mit nichtgesetztem Archive-Bit umbenennen/verändern	X		
Eine Datei lesen			X
Ein Vollbackup durchführen		X	
Eine inkrementelle Datensicherung durchführen		X	
Eine differenzielle Datensicherung durchführen			X

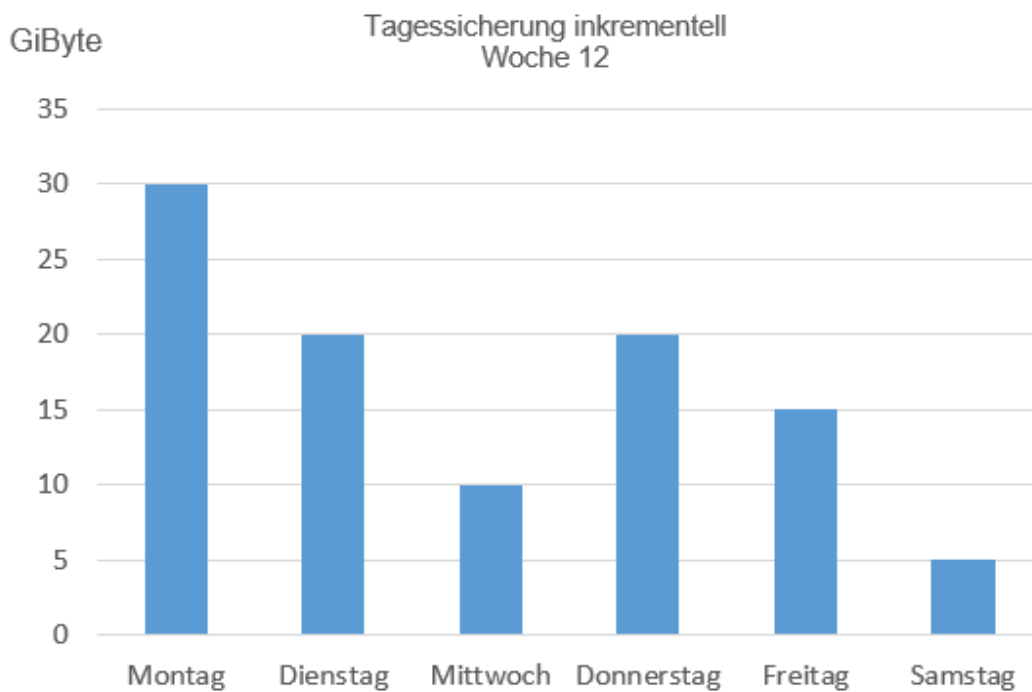
Skript_LF4.docx

Vor- und Nachteile der Datensicherungsstrategien:

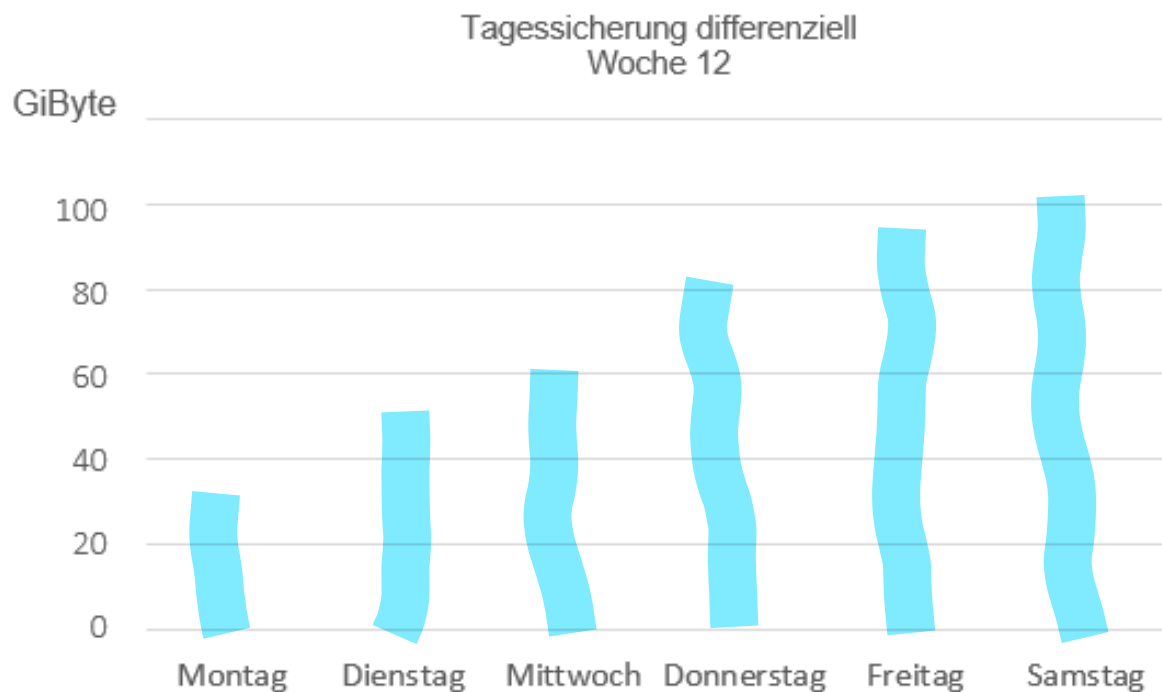
	Vollsicherung	Inkrementelle Sicherung	Differenzielle Sicherung
Vorteile	Bei einem restore wird immer nur ein Band benötigt (Die aktuelle Vollsicherung)	Braucht am wenigsten Speicher und damit am wenigsten Zeit	Bei einem restore sind immer nur zwei Bänder notwendig (Vollsicherung + differenz)
Nachteile	Hoher Speicher- und Zeitbedarf	Bei einem restore sind evtl. viele Bänder notwendig die in der richtigen Reihenfolge eingespielt werden müssen	Mehr Speicher / Zeitbedarf als inkrementell

Aufgaben:

1.) Folgendes Diagramm zeigt für die Woche 12 das Datenvolumen der Tagessicherung. Zurzeit wird die Tagessicherung inkrementell durchgeführt.



Es wird überlegt, die Tagessicherungen differenziell durchzuführen. Veranschaulichen Sie in dem Diagramm das Volumen der Tagessicherungen, falls diese differenziell erfolgen würden.



2.) Die Daten der Amledion GmbH sind auf einem Fileserver gespeichert.

Da auch an Wochenenden und Feiertagen neue Daten hinzukommen bzw. vorhandene Daten geändert werden, wird täglich ein Vollbackup auf einem Bandlaufwerk mit 36 GiByte Speicherkapazität und 30 MiByte/s Schreibgeschwindigkeit durchgeführt. Das Vollbackup vom Sonntag wird archiviert. Das gesamte Datenvolumen auf dem Fileserver beträgt zurzeit 6,2 GiByte.

a) Ermitteln Sie, wie lange der Fileserver pro Woche durch das tägliche Vollbackup blockiert wird. (Geben Sie den Rechenweg an. Ergebnis in *Stunden: Minuten: Sekunden* angeben)

Dv = Datenvolumen in GiByte | Dü = Datenübertragungsrate in MBit/s

$t = Dv/Dü$

$t = (6,2 * 1024^3 * 8) \text{ bit} / (30 * 10^6 \text{ bit/s})$

$t = 1775 \text{ s} / 3600 * 60 = 29\text{min}, 36\text{sek}$

b) Täglich werden durchschnittlich 5 MiByte neue Daten gespeichert und 7 MiByte vorhandene Daten geändert.

Ermitteln Sie für ein differenzielles und inkrementelles Backup die entsprechende wöchentliche Sicherungszeit, wenn einmal pro Woche ein Vollbackup gemacht wird. Verwenden Sie dazu die folgenden Tabellen:

differenzielles Backup		
Wochentag	Datenmenge	Dauer in Sekunden
Sonntag		
Montag		
Dienstag		
Mittwoch		
Donnerstag		
Freitag		
Samstag		
Sekunden/Woche		
(Std: Min: s) /Woche		

inkrementelles Backup		
Wochentag	Datenmenge	Dauer in Sekunden
Sonntag		
Montag		
Dienstag		
Mittwoch		
Donnerstag		
Freitag		
Samstag		
Sekunden/Woche		
(Std: Min: s) /Woche		

c) Geben Sie an, welche Bänder für eine Wiederherstellung der Freitags-Daten erforderlich sind.

- Vollbackup:
- Differenzielles Backup:
- Inkrementelles Backup:

Skript_LF4.docx

Tag	Sonntag	Montag	Dienstag	Mittwoch	Donnerstag	Freitag	Samstag	Sonntag
Datum	15.01.15	16.01.15	17.01.15	18.01.15	19.01.15	20.01.15	21.01.15	22.01.15
Bandnr.	V2	D1	D2	D3 (Inkr)	D4	D5	D6	V3
Sicherung	voll	diff	diff	Ink	diff	diff	diff	voll

Nennen Sie die Nummern der Bänder, die zur Datenwiederherstellung erforderlich sind, in der Reihenfolge ihrer Einspielung.

a.) Erläutern Sie, warum ein RAID-System diese Anforderung nicht erfüllen kann.

Plan zur Datensicherung

1. Monat	1. Woche	Mo	Band 1	
		Di	Band 2	
		Mi	Band 3	
		Do	Band 4	
		Fr	Band 5	
	2. Woche	Mo	Band 1	
		Di	Band 2	
		Mi	Band 3	
		Do	Band 4	
		Fr	Band 6	
	3. Woche	Mo	Band 1	
		Di	Band 2	
		Mi	Band 3	
		Do	Band 4	
		Fr	Band 7	
	4. Woche	Mo	Band 1	
		Di	Band 2	
Mi		Band 3		
Do		Band 4		
Fr		Band 8	Band 9	
2. Monat	5. Woche	Mo	Band 1	
		Di	Band 2	
		Mi	Band 3	
		Do	Band 4	
		Fr	Band 5	

[illegible]

Skript_LF4.docx