Mündliche Abiturprüfung
Fach Informatik - Grundkurs

Prüfender Fachlehrer (Autor der Aufgabe): Brandon Eckoldt

Vorbereitungszeit: 20 min, Prüfungszeit 30 min

Informationssicherheit

Einordnung der Aufgabe in den Lehrplan, Taxonomie:

Die Prüfung ist dem Lernbereich 4: Informationssicherheit des Lehrplans Informatik für die Jahrgangsstufen 11/12 im Grundkurs zuzuordnen. Jedoch kommt es in der Aufgabenstellung auch zu Lernbereich übergreifenden Themen, die durch die Präsenz des Lernbereich „Informationssicherheit“ in anderen Bereichen zustande kommen. Beispiel ist dafür die Aufgabe 2c, welche das HTTPS- und TLS-Protokoll, bekannt aus dem Lernbereich 3 Netzwerke, thematisiert. Aufgabe 1 überprüft das Kennen grundlegender Prinzipien von Verschlüsselungsverfahren und Anwendung einfacher symmetrischer Verschlüsselungsverfahren Zudem wird die Fähigkeit zum Beurteilen/Sich positionieren erfasst, indem die Stärken und Schwächen der Verfahren verglichen werden sollen, sowie eine Anwendung einer Verschlüsselung mit Erklärung. Aufgabe 2 fokussiert auf das Kennen und Verstehen von Datensicherungsarten, Funktionsweisen und Anwendungsbereichen. Die Schüler sollen Anforderungen an die Informationssicherheit anhand eines Beispiels charakterisieren (Anwenden) und können Probleme der Informationssicherheit und des Datenschutzes analysieren, folglich das Https-Protokoll und seinen Beitrag zur Informationssicherheit verstehen. Aufgabe 3 erfordert ein Beurteilen/Sich positionieren zu Aussagen über Datenschutz im digitalen Zeitalter. 3a zielt auf die Erörterung einer Aussage ab, was eine eingehende Auseinandersetzung mit Argumenten und Gegenargumenten erfordert. Der Fokus liegt auf der Bedeutung der Grundprinzipien des Datenschutzes im digitalen Zeitalter. 3b hingegen fordert eine Diskussion der Herausforderungen des Datenschutzes und möglicher Lösungsansätze. Hier liegt der Schwerpunkt auf der Anwendung der Datenschutzprinzipien in konkreten Situationen und der Entwicklung von Strategien zur Wahrung der informationellen Selbstbestimmung.

Insgesamt deckt die Prüfungsaufgabe mehrere Stufen der Bloom'schen Taxonomie ab, wobei der Schwerpunkt auf dem Kennen, Verstehen und Beurteilen/Sich positionieren liegt. Es werden sowohl grundlegende Kenntnisse als auch die Fähigkeit, diese Kenntnisse zu bewerten und anzuwenden, geprüft.

<Brandon> <Eckoldt>,
Didaktik der Informatik, Universität Leipzig

Mündliche Abiturprüfung Informatik (Sachsen) - Thema: Informationssicherheit

Aufgabe 1: Kryptografische Verfahren

- **1a) Nennen** Sie eine Definition für die folgenden Verschlüsselungsverfahren: symmetrische Verschlüsselung und asymmetrische Verschlüsselung. **[2 BE]**

- **1b) Vergleichen** Sie symmetrische und asymmetrische Verfahren hinsichtlich ihrer Stärken und Schwächen im Kontext zu deren Anwendungsbereich. Nennen sie je 2 Stärken und Schwächen für die Verschlüsselungsverfahren **[5 BE]**

- **1c) Erläutern** Sie das Vigenère-Verschlüsselungsverfahren anhand der Verschlüsselung der folgenden Wortgruppe "WorldHello" mit dem Schlüsselwort "badec". Gehen Sie dabei auf die Funktionsweise und die mathematischen Grundlagen ein. **[8 BE]**

  Vignère-Tabelle zur Bearbeitung der Aufgabe 1c)

Klartext

Verschlüsselungstext

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

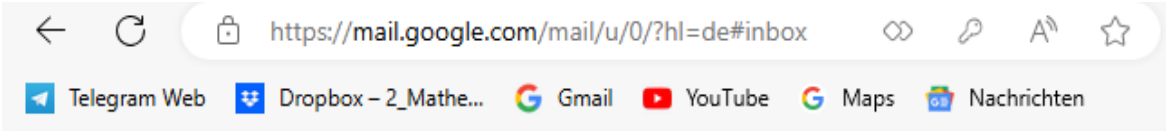
- **1d) Beurteilen** Sie die Aktualität des Vigenère-Verschlüsselungsverfahrens im Kontext moderner Datensicherheit und ob es heutzutage noch relevant ist. [3 B]

Aufgabe 2: Daten- und Informationssicherheit

- **2a) Beschreiben** sie 2 Vorgehensweisen der Backup-Erstellung zur Sicherung von Daten **[2 BE]**

- **2b)** Sie nutzen Ihren Webbrowser, um Ihre E-Mails abzurufen. In der Adressleiste des Browsers sehen Sie ein Schloss-Symbol und **https://** am Anfang der Webadresse. **Erläutern** Sie, welches Protokoll hier verwendet wird und inwiefern, es zur Gewährleistung der Informationssicherheit Ihrer E-Mails beiträgt, beziehen sie sich dabei auf die Informationssicherheitsanforderungen. **[8 BE]**

Angabe: Bild einer Browserleiste



Aufgabe 3: Datenschutz und Datensicherheit im gesellschaftlichen Kontext

Wählen sie **eine** der untenstehenden Aufgaben zur Bearbeitung aus!

- **3a) Positionieren** Sie sich zur folgenden Aussage: „Im digitalen Zeitalter sind die Grundprinzipien des Datenschutzes überholt und behindern den technologischen Fortschritt." **[4 BE]**

- **3b) Diskutieren** Sie die gesellschaftlichen Auswirkungen von Datenschutz-verletzungen und erörtern Sie Maßnahmen zur Stärkung der Datensicherheit. **[4 BE]**

Tabellarisches Erwartungsbild mit Angaben der jeweils erreichbaren BE und der Zuordnung zu den Anforderungsbereichen:

Aufgabe Nr.	Sachverhalt	AB1	AB2	AB3
1a		2	0	0
1b		0	4	1
1c		4	4	0
1d		0	2	1
2a		2	0	0
2b		2	6	0
3a		0	0	4
3b		0	0	4
	Summe BE	10	16	6
	Gesamt		32	

Note	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
BE	32	30	28	27	25	24	22	20	19	17	16	14	10	6	2	1=>

Musterlösung mit Angabe der Zuordnung der einzelnen BE:

Aufgabe 1: Kryptografische Verfahren

1a) **(2 BE)**

Symmetrische Verschlüsselung: Sender und Empfänger verwenden denselben Schlüssel zum Ver- und Entschlüsseln. **[1BE]**

Asymmetrische Verschlüsselung: Es gibt ein Schlüsselpaar (privater und öffentlicher Schlüssel). Der öffentliche Schlüssel dient zum Verschlüsseln, der private zum Entschlüsseln. **[1BE]**

1b) **(5 BE)**

* Schriftlich in Stichpunkten und mündlich in Sätzen

Verschlüsselungsverfahren	Schwächen	Stärken
Symmetrisch	- Schlüsselverteilung kann problematisch sein. - geringe verwaltungstechnische Skalierbarkeit der Schlüsse.	- Schneller als asym. - effizient für große Datenmengen. - einfacher Schlüsselaustausch.
Asymmetrische	- Langsamer als sym. - Rechenintensiver als sym. - nicht für große Datenmengen geeignet.	- Digitale Signaturen möglich. - höhere verwaltungstechnische Skalierbarkeit der Schlüssel als sym. - Schlüsselverteilung ist weniger problematisch.

1c) (8 BE)

Erläuterung des Vigenère-Verschlüsselungsverfahrens

Das Vigenère-Verschlüsselungsverfahren ist eine polyalphabetische Verschlüsselungsmethode, die mehrere Caesar-Chiffren verwendet, die durch ein Schlüsselwort gesteuert werden. Hier werde ich das Verfahren anhand der Verschlüsselung der Wortgruppe "WorldHello" mit dem Schlüsselwort "badec" erläutern.

Funktionsweise [4 BE]

Klartext und Schlüsselwort:

- Klartext: "WorldHello"
- Schlüsselwort: "badec"

Wiederholung des Schlüsselworts: Da das Schlüsselwort kürzer als der Klartext ist, wird es so oft wie nötig wiederholt, um die gleiche Länge wie der Klartext zu erreichen.

Klartext: W o r l d H e l l o; **Schlüssel:** b a d e c b a d e

Zuordnung der Buchstaben zu Zahlen: Jeder Buchstabe wird einer Zahl zugeordnet (A = 0, B = 1, ..., Z = 25).

Klartext: W (22), o (14), r (17), l (11), d (3), H (7), e (4), l (11), l (11), o (14),

Schlüssel: b (1), a (0), d (3), e (4), c (2), b (1), a (0), d (3), e (4), c (2)

Verschlüsselung: Jeder Buchstabe des Klartextes wird durch den entsprechenden Buchstaben des Schlüsselwortes verschoben. Dies geschieht durch Addition der Zahlenwerte und anschließende Modulo-Operation (mod 26), um sicherzustellen, dass das Ergebnis im Bereich des Alphabets bleibt.

Berechnungen: [1 BE]

- W (22) + b (1) = 23 → X
- o (14) + a (0) = 14 → o
- r (17) + d (3) = 20 → u
- l (11) + e (4) = 15 → p
- d (3) + c (2) = 5 → f
- H (7) + b (1) = 8 → l
- e (4) + a (0) = 4 → e
- l (11) + d (3) = 14 → o
- l (11) + e (4) = 15 → p
- o (14) + c (2) = 16 → q

* Der Prüfling muss die Transformation zweimal veranschaulichen, damit der Prüfer nachvollziehen kann, ob die Transformation verstanden wurde. (Tafel oder Blatt müssen zur Verfügung stehen)

Verschlüsselter Text: "Xupfleopq"

Mathematische Grundlagen [3 BE]

Die Vigenère-Verschlüsselung verwendet die Modulo-Arithmetik zur Verschlüsselung und Entschlüsselung. Die zentrale Operation ist die Addition der numerischen Werte der Buchstaben des Klartexts und des Schlüsselworts, gefolgt von einer Modulo-26-Operation, um sicherzustellen, dass die resultierenden Werte innerhalb des Bereichs der Buchstaben des Alphabets bleiben (0 bis 25).

Formel zur Verschlüsselung: $C_i = (P_i + K_i) \bmod 26$ **[1BE]**

C_i ist der i-te Buchstabe des Chiffretextes

P_i ist der i-te Buchstabe des Klartexts

K_i ist der i-te Buchstabe des Schlüsselworts

Formel zur Entschlüsselung: $P_i = (C_i - K_i + 26) \bmod 26$ **[1BE]**

Durch die Modulo-Operation wird sichergestellt, dass die Berechnungen innerhalb des Alphabets bleiben. Das Hinzufügen von 26 bei der Entschlüsselung stellt sicher, dass das Ergebnis nicht negativ wird. **[1 BE]**

* Der Prüfling muss die Formeln für die Verschlüsselung und Entschlüsselung bestimmen/entwickeln und erklären. (mündlich)

1d) **(3 BE)** Beispielhafte Argumentatiospunkte

1. Sicherheit gegen moderne Angriffsmethoden:

- Schwächen: Das Vigenère-Verfahren ist anfällig für verschiedene Angriffe, insbesondere die Kasiski-Analyse und die Friedman-Test, die es ermöglichen, die Länge des Schlüsselworts zu bestimmen und dann den Klartext zu rekonstruieren.
- Kryptoanalyse: Mit den heutigen Rechenressourcen und analytischen Techniken ist es relativ einfach, das Vigenère-Verschlüsselungsverfahren zu brechen. Sobald die Schlüssellänge bekannt ist, kann das Verfahren schnell kompromittiert werden.

3. Praktische Anwendung:

- Begrenzte Relevanz: Aufgrund seiner Schwächen wird das Vigenère-Verfahren heute nicht mehr in sicherheitskritischen Anwendungen verwendet. Es hat jedoch immer noch einen Bildungswert und wird oft in Kryptographie-Kursen verwendet, um grundlegende Konzepte zu lehren.
- Komplexitäts- und Leistungsanforderungen: Moderne Verschlüsselungsverfahren sind darauf ausgelegt, große Datenmengen effizient und sicher zu verarbeiten, was das Vigenère-Verfahren nicht leisten kann.

***** Der Prüfling muss sein Urteil argumentative untermauern.

Aufgabe 2: Daten- und Informationssicherheit in Netzwerken

2a) **(2 BE)**

Komplettsicherung [1 BE]

Funktionsweise: Erstellt eine exakte Kopie des gesamten Datenbestands zu einem bestimmten Zeitpunkt.

Anwendungsbereiche: Geeignet für die Sicherung kleiner bis mittlerer Datenmengen, da sie einfach durchzuführen und wiederherzustellen ist. Bietet den besten Schutz vor Datenverlust, da alle Daten in einem Backup vorhanden sind.

Differentielle Datensicherung [1 BE]

Funktionsweise: Speichert die Unterschiede zwischen dem aktuellen Datenbestand und der letzten Komplettsicherung.

Anwendungsbereiche: Effizienter als Komplettsicherungen, da nur geänderte Daten gespeichert werden. Erfordert jedoch eine Komplettsicherung als Basis.

Inkrementelle Datensicherung [1 BE]

Funktionsweise: Speichert nur die Änderungen seit der letzten Sicherung, unabhängig davon, ob es sich um eine Komplettsicherung oder eine differentielle Sicherung handelte.

Anwendungsbereiche: Sehr platzsparend, da nur die neuesten Änderungen gespeichert werden. Die Wiederherstellung kann jedoch komplexer sein, da mehrere Sicherungen benötigt werden.

2c) **(8 BE)**

HTTPS (Hypertext Transfer Protocol Secure): Protokoll zur sicheren Datenübertragung im Internet. Es stellt eine Erweiterung des HTTP-Protokolls dar und nutzt TLS zur Verschlüsselung. **[1BE]**

TLS (Transport Layer Security): Verschlüsselungsprotokoll, das die Grundlage für HTTPS bildet. Es sorgt für die sichere Übertragung von Daten zwischen Client (z.B. Webbrowser) und Server (z.B. Mailserver). **[1BE]**

Vertraulichkeit: TLS gewährleistet die Vertraulichkeit, indem es die Daten (in diesem Fall E-Mails) während der Übertragung verschlüsselt. Nur der Besitzer des passenden Schlüssels (der Mailserver) kann die Daten entschlüsseln und lesen. Dadurch wird verhindert, dass Unbefugte, die möglicherweise die Datenübertragung abfangen, auf die Inhalte der E-Mails zugreifen können. **[2BE]**

Integrität: TLS schützt die Integrität der Daten, indem es sicherstellt, dass die E-Mails während der Übertragung nicht unbemerkt verändert werden können. Dies geschieht durch den Einsatz von kryptografischen Hash-Funktionen und Message Authentication Codes (MACs), die eine Art Prüfsumme für die Daten bilden. **[2BE]**

Authentizität: TLS ermöglicht die Authentifizierung des Mailservers durch den Einsatz von digitalen Zertifikaten. Dadurch kann der Client überprüfen, ob er tatsächlich mit dem richtigen Server kommuniziert und nicht mit einem betrügerischen Server, der versucht, Daten abzufangen. **[2BE]**

***** Aufgabe soll schriftlich in Stichpunkten mündlichen in vollen Sätzen.

Aufgabe 3: Datenschutz und Datensicherheit im gesellschaftlichen Kontext (4 BE)

3a) Provokative These: „Im digitalen Zeitalter sind die Grundprinzipien des Datenschutzes überholt und behindern den technologischen Fortschritt."

Einleitung: Die provokative These „Im digitalen Zeitalter sind die Grundprinzipien des Datenschutzes überholt und behindern den technologischen Fortschritt" stellt die Relevanz und Angemessenheit traditioneller Datenschutzprinzipien in Frage. Diese Erörterung wird untersuchen, ob Datenschutzprinzipien tatsächlich veraltet sind und ob sie den technologischen Fortschritt behindern oder ob sie nach wie vor eine notwendige Grundlage für den Schutz individueller Rechte darstellen.

Hauptteil:

Argumente für die These:

Innovation und Effizienz: [1 BE]

Strikte Datenschutzregeln können Innovationsprozesse verlangsamen, da Unternehmen umfangreiche Ressourcen in die Einhaltung von Datenschutzbestimmungen investieren müssen, anstatt diese in Forschung und Entwicklung neuer Technologien zu stecken.

Große Datenmengen sind für die Entwicklung von KI und Big Data Analysen essenziell. Einschränkungen im Datenzugang können den Fortschritt in diesen Bereichen behindern.

Wettbewerbsfähigkeit: [1 BE]

Länder mit strengen Datenschutzgesetzen könnten im globalen Wettbewerb benachteiligt sein, da

Unternehmen in Ländern mit weniger strengen Regelungen schneller und effizienter arbeiten können.

Start-ups und kleine Unternehmen könnten durch hohe Compliance-Kosten überfordert werden, was ihre Marktchancen schmälert.

Nutzen für die Gesellschaft: [1 BE]

Der freie Fluss von Daten kann erhebliche Vorteile für die Gesellschaft bringen, wie zum Beispiel in der Gesundheitsforschung, wo große Datenmengen zu bedeutenden Durchbrüchen führen können.

Datengetriebene Innovationen können zur Verbesserung von Lebensqualität und Sicherheit beitragen, wie z.B. durch Smart Cities und personalisierte Medizin.

Argumente gegen die These:

Schutz der Privatsphäre: [1 BE]

Datenschutzprinzipien sind grundlegend für den Schutz der Privatsphäre und der individuellen Rechte. Ohne starken Datenschutz könnten persönliche Informationen missbraucht und die Privatsphäre verletzt werden.

Datenschutz verhindert die unkontrollierte Überwachung durch staatliche und private Akteure, was für die Aufrechterhaltung demokratischer Prinzipien essenziell ist.

Vertrauen der Nutzer: [1 BE]

Nutzervertrauen ist ein Schlüsselfaktor für den Erfolg digitaler Dienste. Unternehmen, die Datenschutz ernst nehmen, können das Vertrauen ihrer Kunden gewinnen und langfristig erfolgreicher sein.

Datenmissbrauchsskandale, wie die Facebook-Cambridge Analytica Affäre, zeigen die Risiken mangelnden Datenschutzes und die negativen Folgen für das Vertrauen der Nutzer.

Recht auf informationelle Selbstbestimmung: [1 BE]

Datenschutz ist eng mit dem Recht auf informationelle Selbstbestimmung verbunden. Nutzer müssen die Kontrolle über ihre persönlichen Daten behalten, um selbstbestimmt handeln zu können.

Ohne angemessenen Datenschutz könnten Nutzer gezwungen sein, ihre Daten preiszugeben, ohne die möglichen Konsequenzen vollständig zu verstehen oder zu akzeptieren.

***Für die Vergabe der vollen Bewertungseinheiten muss der Prüfling 3 Punkte für seine Argumentation/Stellungnahme präsentieren, die auf seine im Anschluss folgende Positionierung der These verweisen. (3 Argumente + Schlussfolgerung [1 BE])**

3b) **Diskutieren** Sie die gesellschaftlichen Auswirkungen von Datenschutzverletzungen und erörtern Sie Maßnahmen zur Stärkung der Datensicherheit. **[4 BE]**

Einleitung: Datenschutzverletzungen haben weitreichende gesellschaftliche Auswirkungen. Diese Diskussion soll die verschiedenen Ebenen der Auswirkungen solcher Verletzungen darstellen und

anschließend Maßnahmen erörtern, die zur Stärkung der Datensicherheit beitragen können.

Hauptteil stellt mögliche Argumentationen für die Diskussion:

1. Gesellschaftliche Auswirkungen von Datenschutzverletzungen:

Individuelle Auswirkungen: [1 BE]

Identitätsdiebstahl: Datenschutzverletzungen können zum Identitätsdiebstahl führen, was erhebliche finanzielle und emotionale Belastungen für die betroffenen Personen mit sich bringt.

Verlust der Privatsphäre: Persönliche Informationen können öffentlich gemacht oder missbraucht werden, was das Vertrauen in digitale Dienste erschüttert.

Wirtschaftliche Auswirkungen: [1 BE]

Unternehmensverluste: Unternehmen können erhebliche finanzielle Verluste durch Datenschutzverletzungen erleiden, einschließlich Kosten für Schadensbegrenzung, rechtliche Strafen und Verlust des Kundenvertrauens.

Marktstabilität: Wiederholte Datenschutzverletzungen können das Vertrauen in ganze Branchen untergraben und die Marktstabilität gefährden.

Gesellschaftliche und politische Auswirkungen: [1 BE]

Vertrauensverlust in Institutionen: Datenschutzverletzungen können das Vertrauen der Öffentlichkeit in staatliche und private Institutionen schwächen.

Gefahr für die Demokratie: Massenüberwachung und der Missbrauch von persönlichen Daten können demokratische Prozesse untergraben und zur Manipulation der öffentlichen Meinung beitragen.

2. Maßnahmen zur Stärkung der Datensicherheit: [1 BE]

Technologische Maßnahmen:

Verschlüsselung: Einsatz starker Verschlüsselungstechnologien, um Daten sowohl während der Übertragung als auch im Ruhezustand zu schützen.

Zugriffskontrollen: Implementierung von strengen Zugriffskontrollen und Authentifizierungsmechanismen, um sicherzustellen, dass nur autorisierte Personen Zugang zu sensiblen Daten haben.

Organisatorische Maßnahmen: [1 BE]

Sicherheitsrichtlinien: Entwicklung und Durchsetzung klarer Sicherheitsrichtlinien und -protokolle innerhalb von Organisationen.

Schulung und Sensibilisierung: Regelmäßige Schulungen für Mitarbeiter, um das Bewusstsein für Datenschutzrisiken und -praktiken zu erhöhen.

Rechtliche und regulatorische Maßnahmen: [1 BE]

Strengere Gesetze: Einführung und Durchsetzung strengerer Datenschutzgesetze und -

vorschriften, um Unternehmen zur Einhaltung hoher Sicherheitsstandards zu verpflichten.

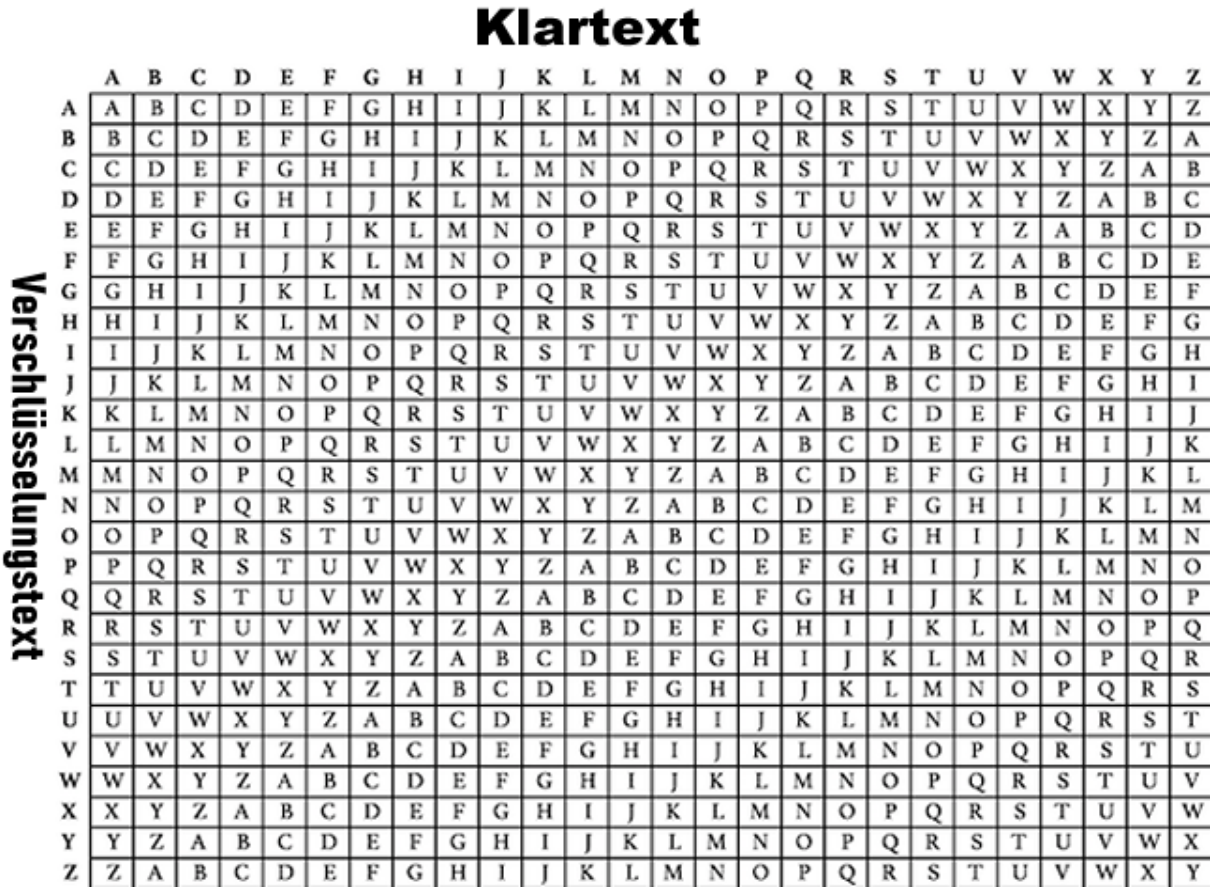
Sanktionen und Strafen: Verhängung erheblicher Strafen für Unternehmen und Institutionen, die Datenschutzverletzungen zulassen, um eine abschreckende Wirkung zu erzielen.

***Der Prüfling muss zum Erreichen der vollen Bewertungseinheiten 2 gesellschaftlichen Auswirkungen von Datenschutzverletzungen sowie 2 Maßnahmen zur Stärkung der Datensicherheit erbringen. *Schriftlich in Stichpunkten und mündlich in Sätzen. Es wurden jeweils 2 Auswirkungen für einen potenziellen Themenbereich vorgegeben.**

Hinweise zur Umsetzung (benötigte Arbeitsmittel, ggf. Software auf dem Prüfungsrechner, …):
Bei der Auswahl dieser Aufgabe ist zu beachten:

- Es stehen dem zu Prüfenden zur Bearbeitung der Aufgaben 1 Din A4 Blatt zur Verfügung (kariert, liniert oder blank).

Anhang: Abbildungen:



Quellenangabe, Abbildungsnachweise, …:

https://www.pitsdatenrettung.de/blog/inkrementelle-differenzielle-datensicherung/ Timestamp: 12:50 Uhr, 11.06.24

https://www.cloudflare.com/de-de/learning/ssl/transport-layer-security-tls/ Timestamp: 12:50 Uhr, 11.06.24

https://www.brandmauer.de/blog/it-security/schutzziele-der-informationssicherheit Timestamp: 12:50 Uhr, 11.06.24

https://www.ahd.de/differentielles-backup-sichern-sie-daten-effizienter/ Timestamp: 12:52 Uhr, 11.06.24

https://www.rst-beratung.de/themen/informationssicherheit#:~:text=Erweiterte%20Schutzziele%20der%20Informationssicherheit&text=%E2%80%9EMit%20dem%20Begriff%20Authentizit%C3%A4t%20wird,der%20angegebenen%20Quelle%20erstellt%20wurden. Timestamp: 12:55 Uhr, 11.06.24

https://www.elektronik-kompendium.de/sites/net/1910101.htm Timestamp: 12:55 Uhr, 11.06.24

https://www.elektronik-kompendium.de/sites/net/1910111.htm Timestamp: 12:55 Uhr, 11.06.24

https://www.youtube.com/watch?v=j9QmMEWmcfo&t=243s imestamp: 12:55 Uhr, 11.06.24

Erklärung der Freigabe zur Nachnutzung der Aufgabe:

Hiermit erkläre ich ____Ebou Brandon_____, _____Eckoldt_____ diese Aufgabe unter Wahrung des Urheberrechts erstellt zu haben.

Ich stelle diese Aufgabe zur Nachnutzung nach Lizenz CC BY-NC (Namensnennung, Bearbeitung, nicht kommerziell) zur Verfügung.

---------- E.B. Eckoldt ----------

(Unterschrift des Autors / elektron. Signatur)