Ueb4

4.1

a)

Der Paragraph 202c bezieht sich auf unter anderem auf 202a der besagt dass das beschaffen der Daten unbefugt sein muss dies ist bei einem Auftrag nicht der Fall (Wichtig ist diesen Auftrag schriftlich Festzuhalten).

b)

- Vage Formulierung: Gesetz kann legitime Sicherheitsforscher und IT-Experten bestrafen. (Fall CDU und CCC)
- Einschränkung der Fähigkeiten von Sicherheitsexperten: Behinderung der Aufdeckung und Behebung von Schwachstellen.
- Schwächung der IT-Sicherheit insgesamt: Gesetz behindert Entwicklung und Einsatz legitimer Sicherheitswerkzeuge.
- Behinderung des Schutzes von Computersystemen und Netzwerken: Gesetz kann Anwendung sinnvoller Sicherheitsmaßnahmen erschweren.

4.2

a)

Edward Snowden und die Offenlegung von Informationen über Facebook und andere Branchenriesen:

- Snowden ist ein ehemaliger Mitarbeiter der CIA und NSA, der geheime Informationen über die Überwachungspraktiken dieser Agenturen öffentlich gemacht hat.
- Seine Enthüllungen haben eine globale Debatte über Datenschutz, Überwachung und die Rolle der Geheimdienste ausgelöst.
- Bezüglich Facebook und anderen Technologieunternehmen hat Snowden die Verbindungen zwischen diesen Unternehmen und den Geheimdiensten offenbart.
- Durch Programme wie PRISM hatte die NSA direkten Zugriff auf die Server dieser Unternehmen.
- Persönliche Daten, die von diesen Unternehmen gesammelt wurden, wurden potenziell für Überwachungszwecke genutzt.

b)

Ungültigkeitserklärung des Safe Harbor-Abkommens:

- Das Safe Harbor-Abkommen wurde vom Europäischen Gerichtshof für ungültig erklärt.
- Der Hauptgrund war, dass es den Datenschutz der europäischen Bürger nicht ausreichend schützte.
- Es gab Bedenken hinsichtlich der massiven Überwachung durch die US-Regierung und das Fehlen ausreichender Rechtsmittel für EU-Bürger gegen Missbrauch ihrer Daten.
- Der Gerichtshof entschied, dass die allgemeine und undifferenzierte Sammlung von Daten nicht mit den Datenschutzgrundsätzen der EU vereinbar ist.

c)

Maximilian Schrems' Kritik am US-EU Privacy Shield:

- Schrems hält das Abkommen für eine Neuauflage des alten Safe Harbor-Abkommens, das bereits für ungültig erklärt wurde.
- Er kritisiert, dass das Privacy Shield nicht den gleichen Datenschutzstandard bietet wie das EU-Recht, insbesondere in Bezug auf das Prinzip der "wesentlichen Äquivalenz".
- Er bemängelt das Fehlen wirksamer Rechtsmittel für EU-Bürger, die glauben, dass ihre Daten missbraucht wurden.
- Schrems kritisiert auch, dass das Abkommen die Möglichkeit der massenhaften Überwachung durch die US-Regierung nicht ausschließt.

4.3

a) Gestohlener USB-Stick mit verschlüsselten, personenbezogenen Daten

- Ja, es ist eine Verletzung personenbezogener Daten gemäß Art. 4 Nr. 12 DSGVO, da die Daten entwendet wurden.
- Die Informationspflicht kann abhängig von der Verschlüsselungsstärke und der Wahrscheinlichkeit eines unbefugten Zugriffs entfallen.
- Meldepflichtig gemäß Art. 33 DSGVO: Ja, innerhalb von 72 Stunden nach Kenntnisnahme der Verletzung.

b) Mehrminütiger Stromausfall, dadurch zwischenzeitlich kein Zugriff auf Daten möglich

- Nein, da keine Verletzung personenbezogener Daten vorliegt.
- Keine Informationspflicht.

- Keine Meldepflicht.

c) Cyber-Angriff auf Krankenhaus, dadurch für 30 Minuten kein Zugriff auf Patientendaten

- Ja, wenn die Integrität oder Verfügbarkeit der Daten beeinträchtigt wurde.
- Informationspflicht gemäß Art. 34 Abs. 1 DSGVO: Ja, wenn die Verletzung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt.
- Meldepflichtig gemäß Art. 33 DSGVO: Ja, innerhalb von 72 Stunden nach Kenntnisnahme der Verletzung.

d) Ransomware-Angriff, der Kundendaten verschlüsselt

- Ja, da die Verfügbarkeit der Daten beeinträchtigt ist.
- Informationspflicht gemäß Art. 34 Abs. 1 DSGVO: Ja, wenn die Verletzung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt.
- Meldepflichtig gemäß Art. 33 DSGVO: Ja, innerhalb von 72 Stunden nach Kenntnisnahme der Verletzung.

e) Kontoauszug per Briefpost an falschen Kunden verschickt

- Ja, da es zu einer unbefugten Offenlegung personenbezogener Daten gekommen ist.
- Informationspflicht gemäß Art. 34 Abs. 1 DSGVO: Ja, wenn die Verletzung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt.
- Meldepflichtig gemäß Art. 33 DSGVO: Ja, innerhalb von 72 Stunden nach Kenntnisnahme der Verletzung.

f) Werbe-E-Mail mit offenem Mailverteiler (CC statt BCC)

- Ja, da es zu einer unbefugten Offenlegung personenbezogener Daten gekommen ist.
- Informationspflicht gemäß Art. 34 Abs. 1 DSGVO: Ja, wenn die Verletzung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt.
- Meldepflichtig gemäß Art. 33 DSGVO: Ja, innerhalb von 72 Stunden nach Kenntnisnahme der Verletzung.