Hochschule RheinMain
Fachbereich DCSM - Informatik
Marc Stöttinger

Security
SoSe 23
LV 4120, 7240

Übungsblatt 3

In dieser Übung werden Sie sich mit dem Thema Datenschutz und dem Einsatz von Informationssicherheitsmanagementsystemen befassen. Sie werden die Möglichkeit haben, einen von vier Anwendungsfällen der Blutspende-App B2DS exemplarisch zu nutzen, um den PDCA-Zyklus des ISMS durchzuführen.

Personenbezogen: unmittelbarer Bezug: Name, Adresse, Telefonnummer. Können eine Person eindeutig identifizieren

Aufgabe 3.1 (Datenschutz):

a) Was ist der Unterschied zwischen personbezogenen und personbeziehbare Daten? Geben Sie jeweils ein paar Beispiele zu den Begriffen im Kontext der Blutspende-App aus der letzten Übungseinheit.

Personenbeziehbar: kein direkter Bezug(ohne Zusatzinformationen): Email, Blutgruppe, Bankverbindung, Standort, IP-Adresse

b) Nennen Sie fünf wichtige Rechte, die ein Benutzer im Bezug auf seine personenbezogenen Daten im Kontext der DSGVO hat. Geben Sie pro Recht ein Beispiel an. Gerne können Sie diese im Kontext der Blutspende-App aus der letzten Übungseinheit motivieren.

1) Anrecht drauf,welche Daten, erhoben & weiterverarbeitet werden. 2) Löschung der Daten 3) Einschränkung der Weitergabe von Daten 4) Widerspruch 5) Vermeidung von (automatisierter) Entscheidungsfindung

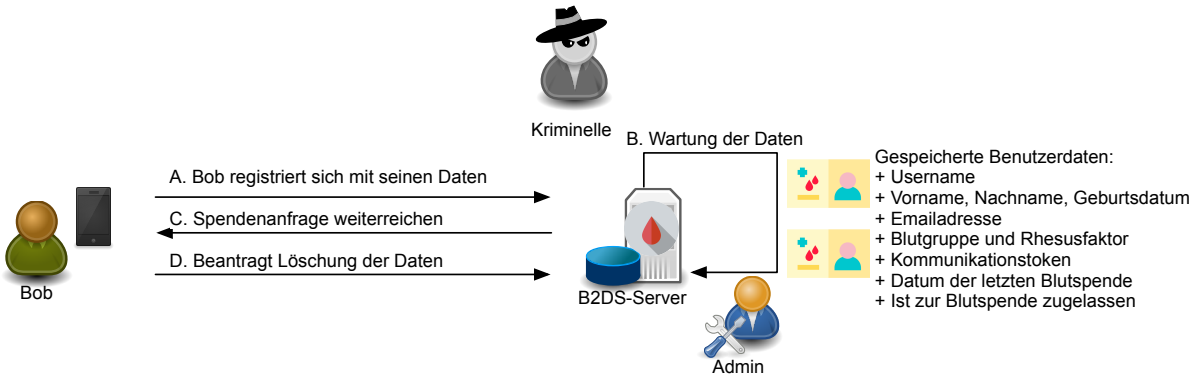
Aufgabe 3.2 (Standarts zu Sicherheitsprozessen):

a) Zu welchem ISO-Standard ist die BSI-200-X Familie kompatibel?
ISO-IEC 27001 Familie

b) Welcher BSI-Standard sollte bei der Planung und Umsetzung der Blutspende-App berücksichtigt werden und warum?

Aufgabe 3.3 (ISMS):

In dieser Aufgabe sollen Sie den PDCA-Zyklus exemplarisch für einen Kernprozess des Blutspende-Services der Blood2Donate-Anwendung durchlaufen. Der Geschäftsführer Ihrer Firma, die die Anwendung betreibt, hat als wichtigstes Ziel für Blood2Donate die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der Benutzerdaten festgelegt.



a) Welches sind die elementaren Phasen des PDCA-Zyklus in einem Informationssicherheitsmanagementsystem und welche Aktivitäten müssen in der jeweiligen Phase durchgeführt werden?

b) Wählen Sie einen der vier Anwendungsfälle aus und führen Sie die vier Phasen anhand dessen durch, unter Berücksichtigung der vom Geschäftsführer ausgesprochen Ziele.

Fall C:
Plan: sicher & schnell Daten weiterleiten [Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit
Do: Verschlüsselung, Authentifizierung der Daten, Protokollierung des Datenempfangs
Check: Datenfluss messen, Prüfen ob Daten oder Informationen gültig/lesbar sind
Act: ß

Fall A:
Plan: Dritter ändert Bobs Daten. Dupletten, Daten könnten beim Transfer zum Server gelesen werden
Do: Passwort. Prüfen auf Doppeleinträge. Datentransfer verschlüsselt & authentisch
Check: Anmeldeprozess überprüfen ("richtig" abmelden & Tokens löschen). Skript das Fake-Accounts anlegt & Unittests. + Daten abfragen und checken ob man z.B. Session-Tokens oder andere Informationen extrahieren kann.
Act: VPN oder HTTPS Verbindung notwendig