Hochschule RheinMain
Fachbereich DCSM - Informatik
Marc Stöttinger

Security

SoSe 23
LV 4120, 7240

Übungsblatt 4

In dieser Übung werden Sie sich mit dem Risikomanagement beschäftigen. Im Rahmen dieser Übung werden Sie die Höhe des potenziellen Schadens von Bedrohungen ermitteln, die Eintrittswahrscheinlichkeit anhand des HEAVENS-Frameworks schätzen und einen Angriffsbaum erstellen, um die propagierte Eintrittswahrscheinlichkeit weiter zu verfeinern.

Aufgabe 4.1 (Risikomanagement):

Die B2DS-Backend-Applikation nimmt Registrierungen zur Bereitschaft zur Blutspende von Benutzern entgegen und speichert sie in einer Datenbank. Eine Registrierung besteht aus einem Blutspendereintrag mit Usernamen, Namen, Geburtstag, Emailadresse und der Blutgruppe sowie Rhesusfaktor. Administratoren können sich auf dem Server einloggen, um den B2DS-Server zu warten. Ihnen sind die folgenden technischen Details zum System bekannt:

- Die B2DS-Backend-Applikation wird auf einem Server gehostet und die Daten der Blutspender in der Datenbank.
- Die Blutspender können sich mit Ihrem Passwort bei der B2DS-Backend-Applikation anmelden.
- Admins authentifizieren sich auf dem Server mit 2-Faktoren: Passwort und Abfrage einer PIN, die via SMS an eine hinterlegte Nummer gesendet wird.
- Aufgrund seines begrenzten Speicherplatzes, hat der Server nur Speicherplatz für 4 Millionen Datensätze von Blutspendern.
- Zum Abschluss der Registrierung wird ein Bestätigungslink mit eine zufällig generierten 32-Bit Token gesendet. Über diesen Link kann sich der Spender einmalig direkt in sein Account einloggen und diesen bestätigen.

Führen Sie für das Asset Blutspenderdaten eine Bedrohungs- und Risikoanalyse sowie eine Risikobehandlung basierend auf HEAVENS durch, bei der Sie die folgenden Schutzziele berücksichtigen:

a) Verfügbarkeit der Blutspenderdaten
b) Vertraulichkeit der Blutspenderdaten

Geben Sie für jedes der Schutzziele in der Bedrohungs- und Risikoanalyse sowie für die Risikobehandlung die folgenden Informationen an:

- Eine begründete Schadenshöhe der Bedrohung

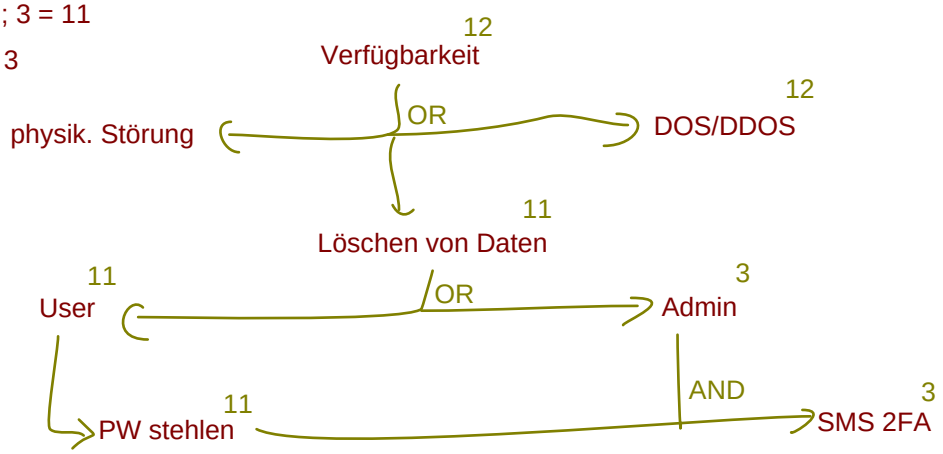
- Einen Angriffsbaum mit mindestens fünf weiteren Knoten (exklusive Wurzelknoten)
- Eine begründete Bewertung der Eintrittswahrscheinlichkeit für zwei Blätter
- Die propagierte Eintrittswahrscheinlichkeit
- Das resultierende Risiko
- Eine Handlungsempfehlung zum Umgang mit dem Risiko, ggf. mit technischer Maßnahme

a)

HEAVENS (DOS/DDOS wird gekauft): Zugriff 3 (internet) ; Expertise 3 (Laie); Wissen 3 (öffentlich); Geräte 3 (Standard) = 12

HEAVENS Passwort: 3 ; 2 ; 3 ; 3 = 11

HEAVENS 2FA: 0 ; 1 ; 1 ; 1 = 3



b)

HEAVENS Festplatte stehlen: 0 ; 2 ; 1 ; 2 = 5

HEAVENS Social Engineering: 3 ; 3 ; 2 ; 3 = 11