Lernfeld 9: Netzwerke und Dienste bereitstellen

Funktionale Segmentierung von Enterprise IT Netzwerken

Projekt 4: Härtung des Ticketsystem-Prototyps unter Beachtung aktueller Security-Anforderungen nach dem Stand der Technik

Setting

Voraussetzung ist die prinzipielle Funktion folgender Prozesse im Prototyp aus Projekt 3:

- Dienste nur über Firewall nach Vorgaben erreichbar (vgl. Tabelle 1)
- Webbasierte Ticket-Erfassung direkt im Netzwerk des Virtualisierungs-Hosts
- Persistieren der Prozessdaten in einem Datenbanksystem im Unternehmens-Intranet.

Nutzbarkeit des Prototyps

Für den System-Test mit User-Stories bestehen zwei Alternativen:

1. Provision einer vorgefertigten Lösung (z.B. OS-Ticket)

2. Individuelle Softwarelösung der Funktionalität gemäß Mindestniveau

Mindestniveau für die Anwenderrollen Kunde und Supportmitarbeiter(MA):

Nach der Authentifizierung muss
der Kunde
- ein Ticket erstellen,
- Bearbeitungsstand eines Tickets einsehen,

der MA
- Liste der offenen Tickets mit Status anzeigen,
- Status eines Tickets ändern,
- Bearbeitungsstand eines Tickets einsehen

können.

Art und Umfang der eigenständigen Implementierung ist eine Gruppenentscheidung.

Hinweis: Für die Härtung haben die Alternativen konzeptuelle Vor- und Nachteile. Eine sorgfältige Prüfung der Auswahlentscheidung wird unbedingt empfohlen („point of no return“).

Aufgabe 1: Schutzbedarfsanalyse und TOM-Identifikation

Für die Härtung des Prototyps ist eine **Risikoanalyse** nach BSI-Standard 200-3 gemäß dem Vorgehensmodell „BSI Grundschutz“ für

- Web-Server
- Datenbank-Server

zu realisieren.

Zu erstellen ist eine tabellarische Gefährdungsübersicht von mindestens **fünf** Risiken, die begründet zu einzuordnen sind (vgl. Abb. 1 in der Broschüre Risikoanalyse).

Im Anschluss sind geeignete technisch-organisatorische Maßnahmen (TOM), auch unter Berücksichtigung des Aufwands- und Nachhaltigkeit-Aspekts, als Schutz zur Minimierung der Risiken zu beschreiben und deren Wirksamkeit zu erläutern („Behandlung von Risiken“).

Erfüllungsziel: Ende der 9. U-Woche

Aufgabe 2: Cybersecurity implementieren

Die praktische Behandlung der Risiken beinhaltet die Umsetzung von **sechs** Schutzmaßnahmen. Nachstehende Themen sind obligatorisch.

- Datensicherung des Datenbankservers im laufenden Betrieb nach Zeitplan
- E2E-Verschlüsselung der DMZ-Kommunikation mittels TLS (Zertifikats-Chain aus CA) [mit automatisierter Erneuerung]
- passwortfreie Anmeldung bei der Remote-Administration am Dienst-Server [und für die Dienst-Konfiguration]

Erfüllungsziel: Ende der 12. U-Woche

Aufgabe 3: Hacking Simulation

Gruppe 1 prüft und protokolliert Qualität der Schutzmaßnahmen des Prototyps der Gruppe 2, usw.

Abschluss: 13. U-Woche

Dresden, 7.02.2022