FHIR Security

Präsentiert von Stefan Mandic

Agenda

- FHIR Security
- Time Keeping
- Communication Security
- Authentication
- Authorization
- Audit
- Digital Signatures
- Attachments
- Labels
- Data Managment Policies
- Narrative
- Input Validation

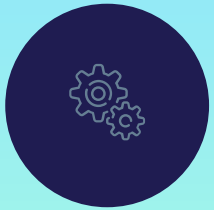
FHIR Security

Die Daten, die in FHIR ausgetauscht werden sind hochsensibel und müssen daher geschützt werden. Der Angriff auf die Daten könnte lebensgefährlich sein, daher spielt die Sicherheit eine sehr große Rolle.

Time Keeping

Datenaustausch läuft zeitlich synchronisiert ab durch NTP/SNTP

NTP verwendet Coordinated Universal Time (UTC), um die Kommunikationsgeräte auf die Millisekunde genau zu synchronisieren



Transaktionscode verwenden für das Tracking verschiedener Prozesse verwendet

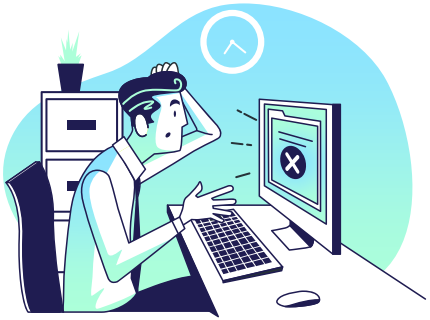
Communication Security

- Der Datenaustausch **muss** gesichert bzw. verschlüsselt werden
- HTTPS (HyperText Transfer Protocol Secure) beim Browser als Protokoll für die Sicherheit
- Verwendung zusätzlicher Sicherheitsmethoden für eine API Authentifizierung von DNS Antworten
- Vor jedem HHTP-Befehl wird eine TLS-Kommunikation (Transport Layer Security) eingerichtet

Authentication

- Jeder Benutzer von FHIR muss sich authentifizieren.
- Die Identität muss sichergestellt werden.
- OpenID Connect kann verwendet werden um die Identität des Endbenutzers zu überprüfen
- Bei Identitätsprüfung einzelner Benutzer: Oauth, Anmeldung/Authentifizierung verläuft über anderen Server

Oauth



Open Authorization ist eine tokenbasierte Autorisierung und Authentifizierung

Benutzername und Passwort werden hierbei nicht offengelegt.

Smart on FHIR

- SMART on FHIR ermöglicht es den Zugriff auf Daten sicher anzufordern und diese Daten dann zu empfangen und zu verwenden.
- Dazu unterteilt man es in 3 Abschnitten
    - Identitäts und Zugriffsverwaltung
    - Zugriff auf Datne
    - Start

Authorization/Access Control

- Benutzer haben strikt definierte Rollen & Rechte
- Übermittlung der Daten ist nicht zugelassen, außer die andere Partei ist berechtigt sie zu erhalten.
- 2 Access Control Modelle:
  - RBAC (Role-Based Access Control)
    - Berechtigungen werden in Rollen unterteilt.
  - ABAC (Attribute-Based Access Control)
    - Die Benutzer erstellen Anforderungen, anschließend werden diese genehmigt oder abgelehnt.

Audit

- Audit sorgt für Rückverfolgbarkeit, alle Änderungen werden automatisch dokumentiert:
  - Wer hat die Änderung vorgenommen?
  - Was wurde geändert?
  - Wann wurde es geändert?

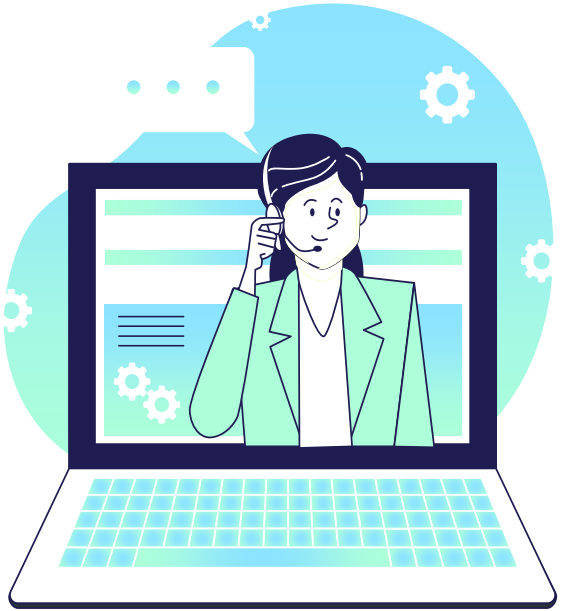
Digital Signatures

- Ressourcen können unter Verwendung der Herkunft Ressource signiert werden.
- Elektronische Daten werden an ein elektronisches Dokument angehängt und bestimmen die Identität des Unterzeichners und die Integrität des signierten Dokuments.

Attachments

- FHIR Ressourcen enthalten Anhänge, diese können Verweise auf Inhalte sein, oder auch in base64 code enthalten.
- Sie sind daher ein Sicherheitsrisiko

Labels



- Die FHIR Ressource ist mit einem Security-Label gekennzeichnet, diese genehmigen Lese-, Änderungs- und andere Vorgänge
- Der Empfänger von Ressourcen ist verpflichtet, die Handhabungsvorbehalte der Etiketten durchzusetzen.

Data Management Policies

- Datenverwaltungsrichtlinien müssen angepasst sein und diese müssen eingehalten werden.
- Es liegt in der vollen Verantwortung des Entwicklers sicherzustellen, dass relevante Vorschriften und andere Anforderungen erfüllt werden.
- Beachtet werden muss:
    - Ist die Richtlinie legal?
    - Ist die Richtlinie sicher?

Narrative

- Die Darstellung von aktiven Inhalten ist mit Sicherheitsproblemen verbunden, deshalb ist dies strikt verboten.
- Was muss beachtet werden bzw. eingehalten werden?
    - Validation des Narratives
    - Keine vertraulichen Informationen bei Verweise auf Daten.
    - Nur vertrauenswürdige Links, diese müssen im EHR laufen.

Input Validation

- Die Eingabedaten müssen auf das richtige Format kontrolliert werden, um unerwünschtes Systemverhalten zu vermeiden.
- Wenn dies nicht beachtet wird, birgt dies einige Risiken
    - Fuzzing
    - Injection attacks
    - Invalid Input Attacks

Fuzzing

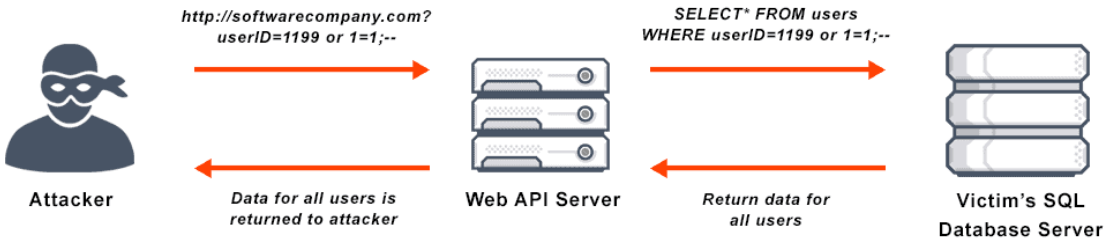
- Fuzzing ist der Prozess des Auffindens von Sicherheitslücken in Input-Parsing-Code durch wiederholtes Testen des Parsers mit modifizierten Inputs.
- Wenn das Programm mit einigen vom Fuzzer generierten Daten reproduzierbare Probleme verursacht, kann man anhand dessen der genauen Ursache nachgehen.

Invalid input attacks

- Angriffe zur Eingabevalidierung finden statt, wenn ein Angreifer absichtlich Informationen in ein System oder eine Anwendung eingibt, um die Funktionalität des Systems zu beeinträchtigen. Manchmal kann eine Webanwendung einen bösartigen Angriff oder einen Angriff zur Eingabevalidierung verursachen, während sie im Hintergrund läuft.
- Z.B SQL Injection

Injection attacks

- Ein Injection Attack ist ein bösartiger Code, der in das Netzwerk eingespeist wird und alle Informationen aus der Datenbank an den Angreifer weiterleitet.



Quellen

https://www.hl7.org/fhir/security.html

https://www.hl7.org/fhir/security.html#authentication

https://www.hl7.org/fhir/security.html#binding

Vielen Dank für Ihre Aufmerksamkeit!