IT/Dev Praktikum: Automatisierung von Sicherheitstests für Telemis-Installationen

Automatisierung von Sicherheitstests für Telemis-Installationen

Telemis ist ein Medizintechnikunternehmen, das sich auf PACS/MACS-Lösungen, digitale Pathologie und Business Intelligence für das Gesundheitswesen spezialisiert hat. Unsere Produkte helfen Gesundheitseinrichtungen, privaten Praxen usw., medizinische Bildgebung und Gesundheitsdaten effizient zu verwalten. Bei Telemis pflegen wir eine enge Atmosphäre, in der gegenseitige Unterstützung und spontane Zusammenarbeit die Norm sind.

Projektziel

Das Hauptziel dieses Praktikums ist das Konzipieren, Entwickeln und Implementieren eines automatisierten Sicherheits-Testframeworks. Dieses Framework wird kontinuierlich die Sicherheitslage unserer Webanwendungen und Portale, die bei Kunden (Krankenhäusern) eingesetzt werden, bewerten und sicherstellen, dass sie sicher konfiguriert und gegen gängige Schwachstellen gehärtet sind.

Kontext

Telemis liefert kritische Softwarelösungen für das Gesundheitswesen. Unsere Anwendungen sind in komplexen IT-Umgebungen in zahlreichen Krankenhäusern installiert. Die manuelle Überprüfung der Sicherheit jeder einzelnen Installation ist zeitaufwendig und lässt sich nicht effektiv skalieren.

Um unsere Sicherheitslandschaft proaktiv zu verwalten, müssen wir von manuellen Stichproben zu einem kontinuierlichen und automatisierten Validierungsprozess übergehen. Der Praktikant wird eine Lösung entwickeln, die regelmäßig eine Liste von Kunden-URLs auf falsche Sicherheitskonfigurationen und Schwachstellen scannt, wie sie in unseren internen Penetrationstests identifiziert wurden.

Praktikumsziele (angepasst an Dauer und Kenntnisstand)

- Einarbeitung in unsere bestehenden Sicherheits-Testberichte und Dokumentationen.

- Automatisierung spezifischer Sicherheitsprüfungen. Beispiele:
    - Überprüfung der Gültigkeit von TLS/SSL-Zertifikaten und der Stärke der Chiffrierung.
    - Erkennung von freigegebenen Administrationsportalen oder -diensten.
    - Überprüfung auf Informationslecks durch Fehlerseiten, Header (z. B. Serverversion) und Stack-Traces.
    - Suche nach Standard-Anmeldeinformationen an bekannten Endpunkten.
- Aufbau einer Kern-Engine, die eine Liste von Ziel-URLs entgegennimmt und die Suite von Testskripten systematisch gegen jede davon ausführt.
- Dokumentation des Frameworks, der einzelnen Testskripte sowie des Verfahrens zur Durchführung der Scans und zur Interpretation der Ergebnisse.

Was der Praktikant aus dieser Erfahrung mitnehmen wird

- Praktische Cybersecurity-Fähigkeiten: Sammeln Sie praktische Erfahrung beim Identifizieren und Testen realer Sicherheitsschwachstellen in einer Unternehmensumgebung.
- Automatisierung & DevSecOps: Lernen Sie, wie man Automatisierungstools für Sicherheit von Grund auf aufbaut – eine sehr gefragte Fähigkeit im Bereich DevSecOps (Development, Security, and Operations).
- Webanwendungssicherheit: Vertiefen Sie Ihr Verständnis dafür, wie Webanwendungen angegriffen werden und, was noch wichtiger ist, wie sie gesichert und gehärtet werden.
- Einblick in die Gesundheits-IT: Gewinnen Sie wertvolle Erfahrung bei der Arbeit an Sicherheitsherausforderungen in dem kritischen und stark regulierten Sektor der Gesundheitstechnologie.

Profil

- Student der Informatik, Cybersicherheit, Informationstechnologie oder eines verwandten Fachgebiets.
- Starke Scripting-Kenntnisse, vorzugsweise in Python.
- Gutes Verständnis von Webtechnologien und -protokollen (HTTP/HTTPS, APIs, Cookies, Header).