Hacking

Bei unserer IoT-Plattform **Mobile Control Center** fallen sensible Daten von vielen Maschinen und Kunden an.
Diese Daten müssen gegen eine Vielzahl von Angriffsszenarien geschützt werden.
Im Rahmen der Projektarbeit sollen bekannte Angriffsvektoren recherchiert sowie an der Zielapplikation ausgetestet werden.

Bewerbung an info@eberle.at

pete linforth/pixabay.com

Aufgabenbeschreibung

- Einarbeit ins System

  Analyse der bestehenden Daten und Datenstrukturen der Zielapplikation sowie der infrastrukturellen und netzwerktechnischen Umsetzung

- Recherche Angriffsvektoren

  Welche bekannte Angriffsvektoren gibt es? Wie können Webapplikationen im Allgemeinen angegriffen werden? Welche Patterns müssen bei der Entwicklung berücksichtigt werden? Welche zusätzlichen Möglichkeiten hat ein angemeldeter Benutzer, ein System
  anzugreifen? Was bedeutet CSRF, XSS, SQL Injection etc.? Welche Sicherheitslücken können von der

- Blackbox- und Whiteboxtests

  Das System soll zuerst mit dem Wissen einer externen Person getestet werden.

  Anschließend wird der Systemaufbau im Detail erklärt, um im nächsten Schritt gezieltere Angriffe ausprobieren zu können.

- Hardening

  Gefundene Sicherheitsprobleme werden in Zusammenarbeit mit der Entwicklungsabteilung gelöst. Zudem soll recherchiert werden, wie wir unser System weiter stärken können, um auch gegen zukünftige Angriffe gerüstet zu sein.