Security-Fundamente für eingebettete Systeme – ein Muss für moderne Entwicklung

In der heutigen vernetzten Welt sind eingebettete Systeme allgegenwärtig – von Automobilen über industrielle Steuerungen bis hin zu IoT-Geräten. Doch mit der zunehmenden Vernetzung steigen auch die Sicherheitsrisiken. Cyberangriffe, Datenlecks und unsichere Implementierungen können schwerwiegende Folgen haben. Wie also kann man Sicherheitsrisiken minimieren und robuste Systeme entwickeln? Die Antwort liegt in soliden Security-Fundamenten.

Warum ist Security für Embedded-Systeme essenziell?

Sicherheit war lange Zeit kein primäres Designkriterium für Embedded-Systeme. Doch vermehrt stattfindende Angriffe zeigen immer wieder, dass ungeschützte Systeme leicht kompromittiert werden können. Die Hauptgründe für eine starke Security-Basis sind:

- **Schutz vor Angriffen**: Eingebettete Systeme sind oft das Ziel von Hackern, die Schwachstellen in Firmware oder Kommunikation ausnutzen.
- **Einhaltung von Normen und Vorschriften**: Regulierungen wie ISO 21434 für Automobilsicherheit oder IEC 62443 für industrielle Steuerungen fordern systematische Sicherheitsmaßnahmen.
- **Sicherstellung der funktionalen Integrität**: Kritische Anwendungen müssen sicherstellen, dass sie erwartungsgemäß funktionieren und nicht durch Angriffe gestört werden.

Die Grundpfeiler der Security-Fundamente

Ein strukturiertes Sicherheitskonzept basiert auf mehreren wichtigen Aspekten:

1. Authentifizierung und Zugriffskontrolle

Ohne eine gesicherte Identitätsprüfung kann jedes System gefährdet sein. Häufige Probleme sind:

- Verwendung von Standardpasswörtern
- Fehlende Multi-Faktor-Authentifizierung (MFA)
- Speicherung von Passwörtern im Klartext

2. Sichere Kommunikation

Unverschlüsselte oder schlecht implementierte Protokolle können Datenlecks verursachen. Sichere Kommunikationsprotokolle sollten:

- Verschlüsselung nach aktuellen Standards nutzen
- Authentifizierungsmechanismen für drahtlose Kommunikation bereitstellen
- Schutz gegen Replay- und Man-in-the-Middle-Angriffe bieten

3. **Bedrohungsanalyse und Risikomanagement (TARA)**

Eine fundierte Bedrohungsbewertung (Threat Analysis and Risk Assessment, TARA) hilft, Sicherheitsrisiken zu identifizieren und Gegenmaßnahmen zu definieren:

- Identifikation von Bedrohungsszenarien
- Bewertung der Angriffspfade und Wahrscheinlichkeiten
- Ableitung und Priorisierung von Sicherheitsmaßnahmen

Best Practices für Embedded Security

Neben der Implementierung spezifischer Sicherheitsmaßnahmen ist es essenziell, bewährte Methoden anzuwenden:

- **Security by Design**: Sicherheitsanforderungen von Anfang an in den Entwicklungsprozess integrieren.
- **Defense in Depth**: Mehrere Sicherheitsschichten einbauen, um Angriffe zu erschweren.
- **Regelmäßige Sicherheitsupdates**: Schwachstellen zeitnah durch Patches schließen.
- **Sicherer Code**: Nutzung von Secure-Coding-Standards wie MISRA C:2012 Amendment 1 oder SEI CERT C++.

Fazit: Sicherheit ist ein Prozess, kein Zustand

Sicherheit in Embedded-Systemen ist keine einmalige Aufgabe, sondern ein kontinuierlicher Prozess. Unternehmen müssen ihre Systeme regelmäßig evaluieren, aktualisieren und gegen neue Bedrohungen absichern. Mit einem strukturierten Ansatz und den richtigen Security-Fundamenten können Entwickler robuste und widerstandsfähige Systeme schaffen.

Möchten Sie mehr über Security für Embedded-Systeme erfahren? Unser Training „**Security-Fundamente für Embedded-Systeme**“ bietet Ihnen praxisnahe Einblicke und bewährte Methoden, um Ihre Systeme sicher zu gestalten!

Weiterführende Informationen

1. MicroConsult Training: Security-Fundamente für Embedded-Systeme
2. MicroConsult Training & Coaching zum Thema Safety & Security
3. MicroConsult Fachwissen zum Thema Safety & Security
4. Alle MicroConsult Trainings & Coachings

Der MicroConsult-Newsletter

Wir informieren Sie mehrmals jährlich über Trends und Best Practices im Embedded Systems Engineering.

Erhalten Sie wertvolles Fachwissen und Tipps aus erster Hand von unseren Embedded-Experten!

Jetzt abonnieren!