Vorgaben für externe Software-Entwickler

Externe Dienstleister, die bei der Software-Entwicklung von Fronius beteiligt sind, haben die folgenden Vorgaben einzuhalten:

Security by Design

Bereits in der Design-Phase des Systems sind IT-Sicherheit und Software-Sicherheits-Standards zu beachten und umzusetzen.

Security by Default

Jedes ausgelieferte Produkt hat - dem Schutzbedarf entsprechend - grundlegende IT-Sicherheitsanforderungen ggf. nach Maßgabe der von Fronius übermittelten Kontrollzielisten (OWASP-Standards) zu erfüllen.

Security in Deployment

„Security in Deployment" bezeichnet die Wartbarkeit eines Systems/Produkts, welches bereits beim Kunden im Einsatz ist. Das Produkt muss einfach verteilt und administriert werden können, um die Applikation auf dem neuesten Stand und damit langfristig sicher halten zu können.

Initiales IT-Sicherheitskonzept

Die Anforderungen der IT-Sicherheit müssen in einem initialen IT-Sicherheitskonzept spezifiziert werden. Je nach Produkt

- wird das IT-Sicherheitskonzept von Fronius erstellt und an den externen Dienstleister übermittelt, oder
- ist vom externen Dienstleister zu erstellen und von Fronius abzunehmen.

Für das initiale Sicherheitskonzept müssen insbesondere folgende Punkte dokumentiert werden:

- Kurze Beschreibung der Applikation (Zweck, Zielgruppe)
- High-Level Systemarchitektur der Applikation (Client/Server, Web, Einsatz von Cloud-Diensten) mit allen verbundenen Remote-Services,
- Verfügbarkeit der Applikation im Internet (ggf. Fernwartungs-Konzept),
- Autonomer Einsatz der Applikation beim Kunden (kein Backend erforderlich, keine Online-Anbindung),
- Ungefähre Anzahl der Benutzer, die auf die Applikation zugreifen,
- Systeme, von denen diese Applikation abhängig ist und Systeme, die von dieser Applikation abhängig sind.
- Das IT-Sicherheitskonzept ist in den entsprechenden System- und Architektur-Spezifikationen zu dokumentieren. Um eine Nachvollziehbarkeit zu gewährleisten, ist eine Revisionierung notwendig.

Maßnahmen im Entwicklungsprozess

- Zwingende Verwendung einer Versionsverwaltungs-Software
- „Veröffentlichte Binärdaten“ sind ausschließlich von Build-Systemen zu verwenden (Isolierte Entwicklungsumgebung)
- Programm-Code muss, sofern von Fronius gefordert, vor der Übernahme in das veröffentliche Produkt (z.B. „Master-Branch“, „Release-Branch“) durch ein Peer-Review auf IT-Sicherheit überprüft werden.

Sicherheitsrelevante Compilerwarnungen dürfen nicht ignoriert werden

Quellcode muss mit der höchsten verfügbaren Warnstufe kompiliert werden und daraus resultierende Compiler-Warnungen sind durch adäquate Quellcodeänderungen zu beheben. Das Ziel ist die Reduktion der sicherheitsrelevanten Compilerwarnungen auf ein Minimum. Falls es nicht möglich ist die Ursache der Warnungen zu beheben, ist eine entsprechende Dokumentation nötig (z.B. bei Verwendung einer veralteten 3rd-Party-Schnittstelle).

Eingesetzte Frameworks und Bibliotheken

Alle eingesetzten Frameworks und Programmbibliotheken, welche zumindest in veröffentlichten Versionen vorliegen, müssen dokumentiert werden. Frameworks und Programmbibliotheken müssen fortlaufend auf sicherheitsrelevante Fehler geprüft werden.

Funktionen, Protokolle und Sicherheitsfunktionen sollen auf offenen Standards basieren und müssen aus verlässlichen Quellen (Programmbibliotheken) verwendet werden (z.B. .Net, openssl). Dies gilt im Speziellen für folgende Themengebiete:

- Kryptografische Verfahren
- Zufallszahlengenerator
- Schlüsselaustausch bzw. Schlüssel- Passwortverwaltung
- Hash- oder MAC-Funktionen
- Verschlüsselung oder Signatur
- Authentisierung (z.B. Software-Tokens)
- Autorisierung
- Sitzungsmanagement (z.B. Erstellung von Session Keys, Ablauf von Sitzungen, Cookies)

Testsysteme und Produktiv-Daten

Auf Testsystemen dürfen ausschließlich Testdaten oder anonymisierte Produktivdaten verwendet werden. Ist dies nicht möglich, ist das Testsystem wie ein Produktivsystem zu konfigurieren und betreiben.