Physikalisch-Technische Bundesanstalt
Nationales Metrologieinstitut

Arbeitsgruppe 8.51 „Metrologische Software“ Stand: 07. April 2022

Merkblatt: Konfiguration von Universal-Betriebssystemen für Messgeräte

1 Allgemeines

Zweck dieses Merkblatts ist es, den Hersteller bei der Konfiguration eines rechtlich relevanten Universal-Betriebssystems[1] auf seinem Messgerät entsprechend den Anforderungen des WELMEC 7.2 Softwareleitfadens [1] und den Voraussetzungen des Merkblatts „Konfiguration rechtlich relevanter Software für Messgeräte [Spezialfall]“ [2] zu unterstützen.

Jede der folgenden Anforderungen muss durch technische Maßnahmen auf der Ebene der Hardware, des Betriebssystems oder der Anwendung erfüllt sein. Die implementierten Schutzmaßnahmen sind vom Hersteller zu dokumentieren und müssen dem aktuellen Stand der Technik entsprechen. Zusätzlich ist für die Prüfung nach dem WELMEC 7.2 Softwareleitfaden [1] bei höheren Risikoklassen eine Einreichung von Dateien zur rechtlich relevanten Konfiguration des Betriebssystems notwendig.

Es werden die dem RFC 2119 [3], [4] entsprechenden deutschen Schlüsselworte in den Anforderungen sinngemäß verwendet.

2 Eigenschaften der Hardware

Ohne sichere Hardware ist eine Absicherung des Betriebssystems nicht möglich.

1. Die Komponente, auf der das Betriebssystem läuft, muss physisch gegen unzulässige Zugriffe abgesichert sein.
2. Es darf keine offenen Schnittstellen mit der Möglichkeit von Speicherzugriffen geben.

Die Dokumentation muss die verwendeten Komponenten auflisten und ihre physischen Sicherungsmaßnahmen beschreiben.

3 Bootvorgang und Laden der rechtlich relevanten Software

Der Bootvorgang realisiert die Vertrauenskette von der sicheren Hardware bis hin zur geladenen rechtlich relevanten Software und gewährleistet damit die Integrität und Authentizität der rechtlich relevanten Software.

1. Nach dem Systemstart muss eine Vertrauenskette über die einzelnen Komponenten des Bootvorgangs aufgebaut sein.
2. Die Abarbeitung der Vertrauenskette kann zeitlich unterbrochen werden, solange ihre Integrität gewahrt bleibt.
3. Die Boot-Konfiguration muss vor unzulässiger Veränderung geschützt sein.
4. Das Booten über offene Schnittstellen muss unterbunden sein.

[1] Im Folgenden nur Betriebssystem genannt.

Die Dokumentation muss die Beschreibung der Vertrauenskette, des Vertrauensankers und der Boot-Konfiguration enthalten. Weiterhin sind die technischen Maßnahmen zur Verhinderung des Bootens über offene Schnittstellen und zur Wahrung der Authentizität und Integrität der vollständig geladenen rechtlich relevanten Software zu dokumentieren.

4 Zulässige Komponenten

Beim Start des Betriebssystems werden Gerätetreiber und Bibliotheken geladen sowie Dienste aktiviert.

1. Es sollte die kleinste Anzahl an Betriebssystem-Komponenten[2] vorhanden sein, die notwendig ist, um den Messbetrieb zu gewährleisten.

Die Dokumentation muss die geladenen und ladbaren Kernelmodule, Gerätetreiber und Softwarebibliotheken, die Beschreibung der Kernel-Konfiguration sowie die Dienste mit deren Ausführungszustand beschreiben.

Hervorzuheben sind die Komponenten, die der Hersteller selbst oder im Auftrag für den Messzweck oder dessen Unterstützung implementiert hat. Außerdem muss beschrieben werden, wie sichergestellt wird, dass die benötigten Systemressourcen für die betriebsgemäße Verwendung zur Verfügung stehen.

5 Schutz in Verwendung

Betriebssysteme verfügen über Mittel, um die Beeinflussung der rechtlich relevanten Software durch andere Software während des Betriebs, nach dem Inverkehrbringen, zu verhindern.

1. Die Ausführung von Software, die die rechtlich relevante Software in unzulässiger Weise beeinflussen kann, muss verhindert sein.
2. Das Betriebssystem sollte die Unverwechselbarkeit der Anzeige der rechtlich relevanten Software gewährleisten.
3. Das Rechtesystem muss derart konfiguriert sein, dass die bestimmungsgemäße Verwendung nicht unzulässig beeinflusst werden kann.
4. Die Administration darf nur unter Verletzung von Sicherungsmaßnahmen erfolgen.

Die Dokumentation muss den Darstellungsmodus der rechtlich relevanten Software, die Konfiguration der Benutzerverwaltung sowie die Regulierung der Programmausführung beschreiben. Weiterhin sind die technischen Maßnahmen zur Sicherung des Administrator-Accounts zu dokumentieren.

6 Rückwirkungsfreiheit der Schnittstellen

Die Kontrolle des Datenflusses durch Absicherung der Schnittstellen ist eine der zentralen Aufgaben in der Konfiguration des Betriebssystems.

1. Offene Hardware-Schnittstellen müssen gegen unzulässige Beeinflussung der rechtlich relevanten Software abgesichert sein.
2. Software-Schnittstellen zwischen Betriebssystem-Komponenten und rechtlich nicht relevanter Software müssen gegen unzulässige Beeinflussung der rechtlich relevanten Software abgesichert sein.
3. Nicht benötigte Schnittstellen sollten deaktiviert sein.

Die Dokumentation muss die offenen Hardware-Schnittstellen auflisten. Ist rechtlich nicht relevante Software vorhanden, müssen zusätzlich die Software-Schnittstellen der Betriebssystem-Komponenten zu dieser Software aufgelistet werden. Für alle genannten Schnittstellen sind die Konfiguration und Maßnahmen zur Kontrolle des Datenverkehrs zu dokumentieren.

[2] Kernelmodule, Dienste, Treiber, Bibliotheken, etc. (auch von Drittanbietern).

7 Prüfbarkeit und Nachweisbarkeit

Zur rechtlich relevanten Software gehören die Konfiguration des Betriebssystems sowie diejenigen Betriebssystem-Komponenten, die für die rechtlich relevante Aufgabe geändert oder ergänzt wurden.

1. Die Konfiguration der rechtlich relevanten Teile des Betriebssystems muss identifizierbar sein.
2. Sämtliche Änderungen an der Konfiguration müssen nachweisbar sein.

Die Dokumentation muss den Identifikator der Betriebssystem-Konfiguration sowie eine Beschreibung der Maßnahmen zur Identifizierbarkeit enthalten. Die Nachweisbarkeit von Änderungen an rechtlich relevanten Teilen des Betriebssystems muss dokumentiert sein.

8 Referenzen

[1] WELMEC, *WELMEC 7.2, 2015 Softwareleitfaden (Europäische Messgeräterichtlinie 2014/32/EU),* 2015.

[2] Physikalisch-Technische Bundesanstalt, Arbeitsgruppe 8.51 "Metrologische Software", *Merkblatt: Konfiguration rechtlich relevanter Software für Messgeräte [Spezialfall],* in der jeweils aktuellen Fassung.

[3] S. Bradner, „Key words for use in RFCs to Indicate Requirement Levels - RFC 2199," 21. Januar 2020. [Online]. Available: https://datatracker.ietf.org/doc/rfc2119/. [Zugriff am 22. März 2022].

[4] J.-L. Fuchs, „Schlüsselwörter zum Kennzeichnen von Anforderungen," 29. Mai 2018. [Online]. Available: https://github.com/adfinis-sygroup/2119/blob/master/2119de.rst. [Zugriff am 22. März 2022].