Physikalisch-Technische Bundesanstalt
Nationales Metrologieinstitut

Arbeitsgruppe 8.51 „Metrologische Software“ Stand: 17. Mai 2021

Merkblatt:
Einrichtung eines Live-Mediums

1 Allgemeines

Dieses Dokument dient als Ergänzung zum Merkblatt „Konfiguration von Universal-Betriebssystemen für Messgeräte“ [1]. Es handelt sich um Anforderungen für Live-Medien, die *zusätzlich* oder in *modifizierter* Form gelten.

Falls ein Anzeigeprogramm und eine Kryptografie-Bibliothek auf dem Live-Medium zu rechtlich relevanten Zwecken eingesetzt werden, müssen sie entsprechend den Anforderungen des WELMEC 7.2 Softwareleitfadens [2] sowie des Merkblatts "Spezielle Anforderungen an Kryptografiemodule" [3] geprüft werden. Der Integritätsschutz für das Live-Medium ist entsprechend der Risikoklasse des zugehörigen Messgerätes zu wählen.

Jede der folgenden Anforderungen muss durch technische Maßnahmen auf der Ebene 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 [2] bei höheren Risikoklassen eine Einreichung von Dateien zur rechtlich relevanten Konfiguration des Live-Mediums notwendig.

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

Anmerkung zur Begrifflichkeit:

- Als Live-Medium wird das in logischer Form (ISO-Image) oder physischer Form (Datenträger) hinterlegte Live-System bezeichnet.
- Als Live-System wird das von einem Live-Medium gestartete Betriebssystem mit dem Anzeigeprogramm bezeichnet.

2 Eigenschaften der Hardware

Es sind keine speziellen Schutzmaßnahmen an der Hardware-Umgebung (Host-Rechner) zum Betrieb des Live-Systems notwendig.

3 Bootvorgang und Laden der rechtlich relevanten Software

Bei der Konfiguration des Starvorgangs ist beim Live-System zusätzlich darauf zu achten, dass es keine unzulässige Interaktion mit dem Host-Rechner geben darf.

1. Der Startvorgang des Live-Systems muss derart konfiguriert sein, dass ausschließlich das Live-System in den Arbeitsspeicher des Host-Rechners oder dessen virtualisierte Umgebung geladen wird.

2. Reproduzierbarkeit: Das Live-System muss aus dem Live-Medium stets in identischer Form wiederherstellbar sein.

Anmerkung: Die Eigenschaft der Reproduzierbarkeit ersetzt den Vertrauensanker bei dauerhaft installierten Betriebssystemen.

Die Dokumentation muss zusätzlich eine Beschreibung der Konfiguration des Startvorgangs des Live-Systems und dessen Schutzmaßnahmen enthalten.

4 Zulässige Komponenten

Die Anforderungen des Kapitels im Merkblatt „Konfiguration von Universal-Betriebssystemen für Messgeräte“ [1] gelten uneingeschränkt.

5 Schutz in Verwendung

Für das Live-System gelten zusätzlich die folgenden Anforderungen:

1. Nach dem Startvorgang sollte das Live-System in den Kiosk-Modus wechseln.
2. Das Nachladen oder Ausführen von Software aus weiteren Datenspeichern muss unterbunden sein.
3. Die zum Anzeigeprogramm übertragenen rechtlich relevanten Daten müssen über einen Integritätsschutz und einen Herkunftsnachweis verfügen.
4. Nach dem Inverkehrbringen darf das Live-System dauerhaft nicht mehr administrierbar sein.

Anmerkung: Zu weiteren Datenspeichern gehören auch die Datenspeicher des Host-Rechners.

Die Dokumentation muss zusätzlich die Schutzmaßnahmen gegen unzulässiges Nachladen und Ausführen von Software sowie das technische Mittel zur dauerhaften Sperrung der Administrierung des Live-Systems dokumentieren.

6 Rückwirkungsfreiheit der Schnittstellen

Die Anforderungen des Kapitels im Merkblatt „Konfiguration von Universal-Betriebssystemen für Messgeräte“ [1] gelten uneingeschränkt.

7 Prüfbarkeit und Nachweisbarkeit

Für das Live-System gelten zusätzlich die folgenden Anforderungen:

1. Über das Anzeigeprogramm und die rechtlich relevanten Teile des Betriebssystems auf dem Live-Medium muss ein Integritätsschutz vorhanden sein.
2. Die Integrität des ISO-Images muss vom Verwender vor dem Betrieb des Live-Systems überprüft werden können.
3. Bei einem Integritätsverlust darf das Live-System keine rechtlich relevanten Funktionen ausführen.

Anmerkung: Zu den rechtlich relevanten Teilen des Betriebssystems gehören wenigstens der Kernel, der Bootloader, die Schnittstellen, die Dienste, die Verwaltung der Benutzerrechte, die Bibliotheken zur Kryptografie sowie die Verzeichnisse mit der rechtlich relevanten Konfiguration des Betriebssystems.

Die Dokumentation muss zusätzlich eine Beschreibung der Schutzmaßnahmen zur Erhaltung der Integrität von Live-Medium und Live-System enthalten.

8 Referenzen

[1] Merkblatt: Konfiguration von Universal-Betriebssystemen für Messgeräte, Physikalisch-Technische Bundesanstalt, Arbeitsgruppe 8.51 „Metrologische Software“, in der jeweils aktuellen Fassung

[2] WELMEC 7.2, 2015 Softwareleitfaden (Europäische Messgeräterichtlinie 2014/32/EU), WELMEC, 2015

[3] Merkblatt: Spezielle Anforderungen an Kryptografiemodule, Physikalisch-Technische Bundesanstalt, Arbeitsgruppe 8.51 „Metrologische Software“, in der jeweils aktuellen Fassung

[4] S. Bradner, RFC 2119 - Key words for use in RFCs to Indicate Requirements Levels, März 1997, URL: https://tools.ietf.org/html/rfc2119 (zuletzt aufgerufen am 4. März 2021); deutsche Übersetzung: J.-L. Fuchs, Schlüsselwörter zum Kennzeichnen von Anforderungen, URL: https://github.com/adfinis-sygroup/2119/blob/master/2119de.rst (zuletzt aufgerufen am 4. März 2021)