Konfiguration von Antivirenprogrammen für den JURA KI Assistenten

(Stand: 19.03.2026)

Der JURA KI Assistent nutzt Systemfunktionen, die von Antivirenprogrammen gelegentlich als verdächtig eingestuft werden können. Um eine reibungslose Nutzung zu gewährleisten, sollten Ausnahmen für die Anwendung und spezifische Sicherheitsfunktionen konfiguriert werden.

Hintergrund: Warum Antivirenprogramme blockieren können

Antivirenprogramme verwenden verschiedene Mechanismen, um Bedrohungen zu erkennen. Legitime Anwendungen können aufgrund dieser Mechanismen blockiert werden:

1. **Verhaltensbasierte Analysen:**
   - ✓ Programme werden basierend auf ihrem Verhalten analysiert. Ähnlichkeiten zu schädlicher Software können zu einer Blockierung führen.
2. **Heuristik und Machine Learning:**
   - ✓ Muster und Verhaltensweisen, die Malware ähneln, können auch in sicheren Programmen fälschlicherweise erkannt werden.
3. **Signaturbasierte Erkennung:**
   - ✓ Programme werden mit bekannten Malware-Datenbanken abgeglichen. Falschmeldungen (False Positives) können zu einer Blockierung führen.
4. **Potenziell unerwünschte Anwendungen (PUA):**
   - ✓ Anwendungen können als unerwünscht eingestuft werden, wenn sie bestimmte Verhaltensweisen aufweisen.

Schritte zur Konfiguration von Ausnahmen

Schritt 1: Globale Ausnahmen hinzufügen

1. Navigieren Sie in Ihrer Antivirensoftware zu den Einstellungen für Ausnahmen (je nach Software z. B. „Global Exclusions“, „Ausnahmeliste“ oder „Whitelist“).
2. Fügen Sie die folgenden Dateien/Pfade des JURA KI Assistenten zur **Liste der Ausnahmen (Whitelist)** hinzu:
   - ✓ C:\anonym\anonymer.exe (Hauptanwendung)
   - ✓ C:\anonym\anonymer.update.exe (Update-Prozess)
   - ✓ Optional -empfohlen!-: Das gesamte Verzeichnis C:\anonym\, um zukünftige Änderungen zu berücksichtigen
   - ✓ C:\ProgramData\JuraSoft\ (benutzerbezogene Daten/Sessions)
   - ✓ C:\Users\<username>\Dokumente\jura-ki\ (Logs und weitere Anwendungsdaten)
   - ✓ C:\Users\<username>\Dokumente\jura-ki\ssl\ (SSL-Zertifikate für HTTPS)

     Dieses Verzeichnis enthält die automatisch generierten SSL-Zertifikate (cert.pem, key.pem) des HTTPS-Servers (bei aktivierter Integration des JURA KI Assistenten in RA-MICRO Essentials). Einige Antivirenprogramme überwachen Verzeichnisse mit .pem-Schlüsseldateien oder blockieren den Zugriff darauf.

3. Zusätzliche Ausnahmen für **temporäre Sandbox-Prozesse (Turbo.net)**
   Der JURA KI Assistent nutzt eine virtualisierte Umgebung über Turbo.net. Dabei werden Prozesse und temporäre Dateien in dynamisch erzeugten Verzeichnissen innerhalb der Sandbox ausgeführt. Durch aktuelle Sicherheitsmechanismen wie HTTPS-/TLS-Verifizierung kann es vorkommen, dass Antiviren- oder Endpoint-Security-Lösungen nicht nur einzelne Hilfsprozesse, sondern auch weitere Bestandteile dieser virtualisierten Umgebung fälschlich blockieren. Bitte ergänzen Sie daher folgenden Pfad in Ihre Ausnahmeliste:

   ✓ C:\Users*\AppData\Local\Turbo.net\Sandbox\Assistent*

   Diese Ausnahme stellt sicher, dass alle durch die Anwendung innerhalb der Turbo.net-Sandbox gestarteten Prozesse und erzeugten Dateien korrekt ausgeführt bzw. verarbeitet werden.

   Hinweis:
   Falls Ihre Sicherheitslösung mit einer enger gefassten Ausnahme zuverlässig funktioniert, kann alternativ weiterhin nur der folgende Pfad freigegeben werden:

   ✓ C:\Users*\AppData\Local\Turbo.net\Sandbox\Assistent*\local\stubexe**.exe

4. Legen Sie fest, welche Schutzmechanismen für diese Dateien oder Verzeichnisse ausgenommen werden sollen. Mindestens folgende Optionen sollten ausgeschlossen werden:

   ✓ Echtzeitscan

   ✓ Verhaltensanalyse

Schritt 2: Anwendungssteuerung anpassen

Falls der JURA KI Assistent als **potenziell unerwünschte Anwendung (PUA)** erkannt wird, überprüfen Sie die **Anwendungssteuerungsrichtlinien:**

✓ Navigieren Sie zu den Richtlinien oder Einstellungen für **Application Control.**

✓ Fügen Sie die Prozesse **anonymer.exe, anonymer.update.exe** und ggf. **certutil.exe** zur **„Allow List“** hinzu.

Integration JURA KI Assistent in RA-MICRO Essentials

Beim Start installiert anonymer.update.exe automatisch ein selbstsigniertes HTTPS-Zertifikat in den Windows-Stammzertifikatsspeicher. Dies geschieht über folgenden Systemaufruf mit erhöhten Rechten (UAC):

✓ certutil -addstore Root "C:\Users\<username>\Dokumente\jura-ki\ssl\cert.pem"

Einige Antivirenlösungen blockieren Schreibzugriffe auf den Stammzertifikatsspeicher. Die Anwendung certutil.exe sollte daher in Verbindung mit dem Aufruf durch anonymer.update.exe als vertrauenswürdig eingestuft werden.

Hinweis zur Anwendungserkennung von Sandbox-Prozessen:

Einige Antivirenlösungen erkennen python.exe oder cmd.exe, wenn sie über die Sandbox gestartet werden, als potenziell unerwünschte Anwendung (PUA). In diesem Fall sollten Sie auch diese temporären Pfade zur **„Allow List“** hinzufügen, sofern Ihre Software diese pfadbasiert erlaubt.

✓ Empfohlener Pfad für die Zulassung:
C:\Users*\AppData\Local\Turbo.net\Sandbox\Anonymer*\local\stubexe**.exe

Schritt 3: HTTPS und SSL-Inspektion

Der JURA KI Assistent verwendet **HTTPS** für die lokale Kommunikation, sofern die **Integration in RA-MICRO Essentials** aktiviert wird. Die Anwendung läuft auf zwei lokalen Ports:

- ✓ http://localhost:5050 — Kompatibilitäts-/Weiterleitungsserver
- ✓ https://localhost:5051 — HTTPS-Hauptserver

SSL/TLS-Inspektion: Antivirenlösungen mit HTTPS-Inspektion (z. B. Kaspersky, ESET, Avast Business, Bitdefender GravityZone) können die Verbindung zu localhost:5051 unterbrechen, da das selbstsignierte Zertifikat dabei nicht mehr als vertrauenswürdig erkannt wird. Daher sind **Ausnahmen** für **localhost** und **127.0.0.1 von der SSL/TLS-Inspektion** zu setzen.

Cross-Origin-Anfragen (Essentials-Integration): Im Rahmen der RA-MICRO Essentials-Integration wird der JURA KI Assistent als iFrame innerhalb von ***.es.ra-micro.**de geöffnet. Der Browser stellt dabei **Cross-Origin-Anfragen** an **https://localhost:5051.** Einige Webschutzmodule blockieren solche Anfragen als Schutz vor „localhost-Probing". HTTPS-Anfragen an https://localhost:5051 sind im Webschutzmodul zuzulassen, auch wenn diese aus einem externen Ursprung stammen.

Schritt 4: Ausnahmen für Exploit-Erkennung hinzufügen

Falls Ihre Antivirensoftware Exploit-Schutzfunktionen enthält, prüfen Sie die Einstellungen für **Exploit-Erkennung** (z.B. „Dynamic Shellcode Protection“, „HeapHeapProtect“, „Memory Protection“). Um Fehlalarme zu vermeiden und eine stabile Ausführung zu ermöglichen, sollte folgender Pfad bei Bedarf als Ausnahme hinterlegt werden – insbesondere für den Exploit-Typ **DynamicShellcode,** der bei Ausführung von **python.exe** in der Sandbox des JURA KI Assistenten auftreten kann:

- ✓ C:\Users*\AppData\Local\Turbo.net\Sandbox\Anonymer*\local\stubexe**.exe

Diese Freigabe stellt sicher, dass dynamisch erzeugte Hilfsprozesse korrekt ausgeführt werden können, ohne vom Exploit-Schutz blockiert zu werden.

Schritt 5: Zuweisen der Whitelist zu einer Web-Filter-Policy

1. Nachdem Sie die URL-Liste erstellt haben, gehen Sie **zurück** zur **Web-Filter-Policy** und fügen die neue **Whitelist-URL-Gruppe** in den Bereich der **Erlaubten Kategorien oder Zulässigen URL-Kategorien** hinzu.
2. Speichern Sie die Änderungen.

Schritt 6: Umgang mit False Positives

Falls der JURA KI Assistent weiterhin blockiert wird:

1. **Dateien zur Überprüfung einreichen:**

   Melden Sie die betroffenen Dateien direkt an den Entwickler Ihrer Antivirensoftware, insbesondere:

   - ✓ *anonymer.exe, anonymer.update.exe*
   - ✓ sowie temporäre Prozesse wie *python.exe* oder *cmd.exe,* sofern sie aus der Turbo.net Sandbox (stubexe) stammen.

2. **Protokolle analysieren:**

   Überprüfen Sie die Protokolle der Antivirensoftware, um weitere Details zur Blockierung zu erhalten. Achten Sie dabei insbesondere auf „Dynamic Shellcode"- oder „Memory Protection"-Ereignisse.

3. **Support kontaktieren:**

   Wenden Sie sich an den Support der Antivirensoftware, falls die oben genannten Schritte das Problem nicht lösen. Geben Sie idealerweise die vollständigen Pfade, Dateihashes und betroffenen Exploit-Typen mit an.

Wichtige Hinweise

Die genauen Menüpunkte und Begriffe können je nach Antivirensoftware unterschiedlich sein. Konsultieren Sie die Dokumentation Ihrer Software, um die relevanten Einstellungen zu finden. Stellen Sie sicher, dass die Ausnahmen nur für bekannte und vertrauenswürdige Programme wie den JURA KI Assistenten konfiguriert werden, um die Systemsicherheit nicht zu gefährden.