HINWEISE ZUR INDUSTRIAL SECURITY

Maßnahmen zur Steigerung der Gerätesicherheit

INHALT

1. EINLEITUNG

Um Ihre Industrieanlagen vor Angriffen von außen abzusichern, müssen Sie nicht nur sichere Komponenten auswählen, sondern diese auch korrekt konfigurieren. Nach dem Shift-Left-Prinzip der Security sollten Sie also schon während der Planung und Inbetriebnahme Ihrer Anlage auf den korrekten Einsatz Ihrer E-T-A-Komponenten achten.

Dieses Dokument gibt Ihnen allgemeine Hinweise zum sicheren Einsatz von E-T-A-Komponenten. Die Nutzerdokumentation der einzelnen Produkte gibt Ihnen teils detailliertere Informationen, wie diese Hinweise konkret angewendet werden bzw. welche Maßnahmen zusätzlich für eine gesteigerte Security anzuwenden sind. Wenden Sie die Hinweise aus diesem Dokument an, um die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten und Anlagen zu erhalten.

Neben der Anwendung dieser Hinweise empfehlen wir zusätzlich, in Ihrer Organisation Prozesse zur Durchsetzung von Informationssicherheitsmaßnahmen einzuführen. Dazu zählt zum Beispiel die Einführung eines Managementsystems für Informationssicherheit (ISMS) nach ISO/IEC 27001.

2. SICHERHEITSMAßNAHMEN FÜR KOMPONENTEN

Die Anwendung der folgenden Hinweise dient dem Zweck, die Sicherheit Ihrer Komponenten während Inbetriebnahme, Betrieb und Entsorgung zu erhöhen. Um die Sicherheit Ihrer Anlage zu gewährleisten, reicht es jedoch nicht, die einzelnen Hinweise isoliert anzuwenden. Viel mehr wird ein ganzheitliches Defense-in-Depth-Konzept benötigt, in dem Sie die Sicherheitsmaßnahmen über alle Komponenten hinweg aufeinander abstimmen und mehrere Schutzebenen einrichten.

2.1 Absicherung von Kommunikationskanälen

- Binden Sie Ihre Komponenten nicht in öffentliche Datennetze ein.
- Verhindern Sie unerlaubte Zugriffe auf Ihre Netzwerke und Komponenten, indem Sie eine Firewall einrichten.
- Koppeln Sie Ihre Anlagen von der restlichen Unternehmensinfrastruktur so weit wie möglich ab.
- Deaktivieren Sie nicht benötigte Kommunikationskanäle in Ihren Komponenten.
- Wenn Sie von der Ferne auf Ihre Anlagen und Komponenten zugreifen müssen, richten Sie dafür sichere Kanäle wie VPN oder HTTPS ein.

2.2 Absicherung vor unbefugtem Zugriff

- Wenn Ihre E-T-A-Komponente über eine Nutzerverwaltung verfügt, teilen Sie den verschiedenen Nutzergruppen nur die minimalen benötigten Rechte zu.
- Ändern Sie nach erster Inbetriebnahme Ihrer Komponenten die voreingestellten Zugangsdaten.
- Verwenden Sie ausnahmslos sichere Zugangsdaten für Ihre Komponenten, die den Sicherheitsrichtlinien Ihrer Organisation entsprechen.
- Ändern Sie die Zugangsdaten zu Ihren Komponenten regelmäßig, wie es in den Sicherheitsrichtlinien Ihrer Organisation gefordert wird.
- Schränken Sie den physikalischen Zugriff auf Ihre Komponenten ein, z. B. mithilfe von verschließbaren Schaltschränken.
- Machen Sie Gebrauch von Maßnahmen zur Manipulationserkennung, z. B. durch Plombieren von Geräten, die dies unterstützen.

2.3 Aufrechterhalten der Sicherheit

- Verwenden Sie für Ihre Komponenten stets die neueste Firmware. Softwareupdates finden Sie in den jeweiligen Produktbereichen unter www.e-t-a.de.
- Prüfen Sie regelmäßig, ob für Ihre Komponenten Updates vorliegen.
- Beachten Sie bei der Anwendung von Updates die zugehörigen Release Notes.
- Prüfen Sie regelmäßig die Security Advisories des E-T-A-PSIRT, wie sie mögliche Schwachstellen umgehen können. Details zum PSIRT finden Sie in Abschnitt 3.
- Bewahren Sie Zugangsdaten nicht in Klartext auf und nutzen Sie ggf. einen Passwortmanager.
- Machen Sie Gebrauch von den Funktionen zur Ereignisprotokollierung und werten Sie diese Protokolle regelmäßig und/oder automatisch aus.
- Führen Sie regelmäßig Backups Ihrer Komponentenkonfiguration durch.
- Führen Sie regelmäßig eine Bedrohungsanalyse durch. Aktualisieren Sie Ihr Bedrohungsmodell mithilfe der für Ihre Komponenten veröffentlichten Schwachstellen.

2.4 Sichere Entsorgung

- Löschen Sie sensible Daten nach Außerbetriebnahme von den von Ihnen eingesetzten Komponenten.
- Setzen Sie Ihre Komponenten nach Außerbetriebnahme mit den dafür vorgesehenen Kommandos zurück.

3. MELDUNG VON SICHERHEITSLÜCKEN

Das E-T-A Product Security Incidence Response Team (PSIRT) ist die zentrale Anlaufstelle für die Meldung und Veröffentlichung von Sicherheitslücken und Security Advisories. Das Team nimmt Meldungen über Sicherheitsvorfälle und Schwachstellen in unseren Komponenten an und arbeitet eng mit Ihnen zusammen, um schnellstmöglich Abschaltmaßnahmen zu erarbeiten.

Auf der PSIRT-Homepage werden Schwachstellen in E-T-A-Komponenten und Umgehungsmaßnahmen in Form von Security Advisories veröffentlicht. Bleiben Sie auf dem Laufenden, indem Sie regelmäßig die Webseite auf Neuigkeiten überprüfen.

Weitere Informationen zur Arbeit des PSIRT, Kontaktdaten und Meldungen von Sicherheitslücken finden Sie unter www.e-t-a.de/psirt.