Murrelektronik Generelle Betriebsanweisung zur Steigerung der Cybersicherheit

Hinweis

Um einen sicheren Betrieb zu gewährleisten, sind die nachfolgenden Inhalte in der gesamten Applikation bzw. an der gesamten Anlage zu berücksichtigen.

Allgemein

- Das Einhalten der Empfehlungen und Richtlinien dieses Kapitels regelmäßig überprüfen.
- Das Betreiben des Geräts in internen Netzwerken erhöht die Datensicherheit. Interne und externe Netzwerke unabhängig voneinander betreiben.
- Das Netzwerk in Teilbereiche segmentieren.
- Das Aufteilen in logische Segmente via VLAN beschränkt unbefugte Zugriffe.
- Login-Sessions wie zum Beispiel SSH oder webbasiertes Management ordnungsgemäß schließen.
- Netzwerkkommunikation zum Beispiel mithilfe von VPN verschlüsseln.
- Die Benutzerdokumentationen zusammenhängender Geräte auf weitere Sicherheitshinweise prüfen.
- Geräte-Logs auswerten und auf Anomalien überprüfen.
- Ungenutzte Ports deaktivieren.

Authentifizierung

- Standardpasswörter bei Inbetriebnahme des Geräts ersetzen.
- Auf die Verwendung unterschiedlicher Passwörter für unterschiedliche Systeme achten.
- Passwörter an einem sicheren Ort verschlüsselt hinterlegen.
- Regelmäßiges Ändern der Passwörter erhöht die Sicherheit.
- Bei Verdacht kompromittierter Passwörter diese sofort ändern.
- Datenübertragungen, die im Kontext eines Authentifizierungsprozesses stehen, wenn möglich verschlüsseln.

Passwortrichtlinien

Empfohlene Mindestanforderungen an Passwörter:

- eine Länge von 12 Zeichen
- ein Sonderzeichen
- eine Ziffer 0 ... 9
- ein Kleinbuchstabe
- ein Großbuchstabe

Software

- Die Firmware der Geräte stets aktuell halten.
  - Informationen zu sicherheitsrelevanten Updates, siehe shop.murrelektronik.com.
  - Bereitgestellte Prüfsummen verwenden.
- Nur Protokolle aktivieren, die für den Einsatz des Geräts nötig sind.
- Das Management des Geräts mit einer ACL beschränken.
- Eine VLAN-Strukturierung verwenden.
- Einen zentralen Logging-Server verwenden.
- Den logischen Zugriff auf das Gerät auf autorisiertes Fachpersonal beschränken.
- Jedem Nutzer nur Rechte gewähren, die für seine Rolle notwendig sind.

Physischer Zugriff

- Den physischen Zugriff auf das Gerät auf autorisiertes Fachpersonal beschränken.
- Ungenutzte physische Schnittstellen auf dem Gerät sperren.
- Regelmäßig auf Unversehrtheit überprüfen.