INDUSTRIAL SECURITY

Maßnahmen zum Schutz von netzwerkfähigen Geräten mit Kommunikationsschnittstellen, Lösungen und PC-basierter Software vor unberechtigten Zugriffen

Anwenderhinweis
107913_de_03

1 Einleitung

Sie müssen Komponenten, Netzwerke und Systeme vor unberechtigten Zugriffen schützen und die Datenintegrität gewährleisten. Hierzu müssen Sie bei netzwerkfähigen Geräten, Lösungen und PC-basierter Software organisatorische und technische Maßnahmen ergreifen.

Phoenix Contact empfiehlt dringend den Einsatz eines Managementsystems für Informationssicherheit (ISMS) zur Verwaltung aller infrastrukturellen, organisatorischen und personellen Maßnahmen, die zur Erhaltung der Informationssicherheit notwendig sind.

Darüber hinaus empfiehlt Phoenix Contact, mindestens die folgenden Maßnahmen zu berücksichtigen.

Weiterführende Informationen zu den im Folgenden genannten Maßnahmen erhalten Sie auf den folgenden Webseiten[1]:

- bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html
- ics-cert.us-cert.gov/content/recommended-practices
- bsi.bund.de/DE/Themen/ICS/Empfehlungen/ICS/empfehlungen_node.html

2 Empfohlene Maßnahmen für Geräte und Lösungen

2.1 Komponenten und Systeme nicht in öffentliche Netzwerke einbinden

- Vermeiden Sie es, Ihre Komponenten und Systeme in öffentliche Netzwerke einzubinden.
- Wenn Sie Ihre Komponenten und Systeme über ein öffentliches Netzwerk erreichen müssen, verwenden Sie ein VPN (Virtual Private Network).

2.2 Firewall einrichten

- Um Ihre Netzwerke und darin eingebundene Komponenten und Systeme vor externen Einflüssen zu schützen, richten Sie eine Firewall ein.
- Um ein Netzwerk zu segmentieren oder eine Steuerung zu isolieren, verwenden Sie eine Firewall.

2.3 Nicht benötigte Kommunikationskanäle deaktivieren

- Deaktivieren Sie nicht benötigte Kommunikationskanäle (z. B. SNMP, FTP, BootP, DCP etc.) an den von Ihnen eingesetzten Komponenten.

[1] Letzter Zugriff am 12.02.2020

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

2.4 Defense-in-Depth-Mechanismen bei der Anlagenplanung berücksichtigen

Um Ihre Komponenten, Netzwerke und Systeme zu schützen, ist es nicht ausreichend, isoliert betrachtete Maßnahmen zu ergreifen. Defense-in-Depth-Mechanismen umfassen mehrere, aufeinander abgestimmte und koordinierte Maßnahmen, die Betreiber, Integratoren und Hersteller miteinbeziehen.

- Berücksichtigen Sie bei der Anlagenplanung Defense-in-Depth-Mechanismen.

2.5 Zugangsberechtigungen beschränken

- Beschränken Sie die Zugangsberechtigungen zu Komponenten, Netzwerken und Systemen auf die Personen, für die eine Berechtigung unbedingt notwendig ist.
- Deaktivieren Sie nicht genutzte Benutzerkonten.

2.6 Zugriffe absichern

- Ändern Sie die voreingestellten Anmeldeinformationen nach der ersten Inbetriebnahme.
- Verwenden Sie sichere Passwörter, deren Komplexität und Lebensdauer dem Stand der Technik entsprechen.
- Ändern Sie Passwörter entsprechend der für ihre Anwendung geltenden Regeln.
- Verwenden Sie Passwort-Manager mit zufällig erzeugten Passwörtern.
- Verwenden Sie, sofern möglich, zentrale Benutzerverwaltungen zur Vereinfachung des User Managements und der Anmeldeinformationen.

2.7 Bei Fernzugriff sichere Zugriffswege verwenden

- Verwenden Sie für einen Fernzugriff sichere Zugriffswege wie VPN (Virtual Private Network) oder HTTPS.

2.8 Sicherheitsrelevante Ereignisprotokollierung aktivieren

- Aktivieren Sie die sicherheitsrelevante Ereignisprotokollierung gemäß der Sicherheitsrichtlinie und der gesetzlichen Bestimmungen zum Datenschutz.

2.9 Aktuelle Firmware-Version verwenden

Phoenix Contact stellt regelmäßig Firmware-Updates zur Verfügung. Verfügbare Firmware-Updates finden Sie auf der Produktseite des jeweiligen Geräts.

- Stellen Sie sicher, dass die Firmware aller verwendeten Geräte immer auf dem aktuellen Stand ist.
- Beachten Sie die Change Notes zur jeweiligen Firmware-Version.
- Beachten Sie die Webseite des Product Security Incident Response Teams (PSIRT) von Phoenix Contact für Sicherheitshinweise zu veröffentlichten Sicherheitslücken.

2.10 Aktuelle Sicherheits-Software verwenden

- Um Sicherheitsrisiken wie Viren, Trojaner und andere Schad-Software zu erkennen und auszuschalten, installieren Sie auf allen PCs eine Sicherheits-Software.
- Stellen Sie sicher, dass die Sicherheits-Software immer auf dem aktuellen Stand ist und die neuesten Datenbanken nutzt.
- Nutzen Sie Whitelist-Tools zur Überwachung des Gerätekontexts.
- Um die Kommunikation Ihrer Anlage zu prüfen, nutzen Sie ein Intrusion-Detection-System.

Für die Absicherung von Netzwerken zur Fernwartung über VPN bietet Phoenix Contact als Security-Appliance z. B. die Produktlinie mGuard an, siehe hierzu den aktuellen Katalog von Phoenix Contact (phoenixcontact.net/products).

2.11 Regelmäßige Bedrohungsanalyse durchführen

Um festzustellen, ob die von Ihnen getroffenen Maßnahmen Ihre Komponenten, Netzwerke und Systeme noch ausreichend schützen, ist eine regelmäßige Bedrohungsanalyse erforderlich.

- Führen Sie regelmäßig eine Bedrohungsanalyse durch.

2.12 Zugriff auf die SD-Karte schützen

Geräte mit SD-Karten benötigen Schutz gegen unerlaubte physische Zugriffe. Eine SD-Karte kann mit einem herkömmlichen SD-Kartenleser jederzeit ausgelesen werden. Wenn Sie die SD-Karte nicht physisch gegen unbefugte Zugriffe schützen (z. B. mithilfe eines gesicherten Schaltschranks), sind somit auch sensible Daten für jeden abrufbar.

- Stellen Sie sicher, dass Unbefugte keinen Zugriff auf die SD-Karte haben.
- Stellen Sie bei der Vernichtung der SD-Karte sicher, dass die Daten nicht wiederhergestellt werden können.

3 Empfohlene Maßnahmen für PC-basierte Software

PC-basierte Software wird z. B. verwendet, um Geräte, Netzwerke oder Lösungen einzurichten, zu konfigurieren, zu programmieren und zu überwachen.

Eine Engineering-Software kann das Gerät oder die Lösung manipulieren.

- Um das Risiko der Manipulation zu reduzieren, führen Sie regelmäßig Sicherheitsbewertungen durch.

3.1 PC-basierte Härtungs- und Organisationsmaßnahmen

Schützen Sie PCs, die im Bereich der Automatisierungslösungen eingesetzt werden, gegen sicherheitsrelevante Manipulationen. Dabei helfen u. a. die folgenden Maßnahmen:

- Booten Sie Ihren PC regelmäßig nur von manipulationssicheren Datenträgern.
- Richten Sie restriktive Zugriffsrechte für diejenigen Personen ein, für die eine Autorisierung unbedingt erforderlich ist.
- Schützen Sie sich vor ungewollten Zugriffen mit starken Passwörtern und Regeln, um sie stark zu halten.
- Deaktivieren Sie nicht genutzte Dienste.
- Deinstallieren Sie nicht genutzte Software.
- Verwenden Sie eine Firewall zur Beschränkung des Zugriffs.
- Schützen Sie wichtige Verzeichnisse und Daten mithilfe von Whitelist-Tools gegen ungewollte Veränderungen.
- Aktivieren Sie die sicherheitsrelevante Ereignisprotokollierung gemäß der Sicherheitsrichtlinie und den gesetzlichen Bestimmungen zum Datenschutz.
- Aktivieren Sie den Aktualisierungsmechanismus gemäß der Sicherheitsrichtlinie.
- Aktivieren Sie die automatische Bildschirmsperre und die Abmeldung nach einer bestimmten Zeit der Inaktivität.
- Führen Sie regelmäßige Backups durch.
- Verwenden Sie nur Daten und Software aus zugelassenen Quellen.
- Verfolgen Sie keine Hyperlinks aus unbekannten Quellen, z. B. aus E-Mails.

3.2 Aktuelle Software verwenden

- Verwenden Sie immer die aktuelle Software-Version (für Engineering-Software, Betriebssysteme etc.).
- Prüfen Sie auf der jeweiligen Produktseite von Phoenix Contact die verfügbaren Software-Updates.
- Beachten Sie die Change Notes zur jeweiligen Software-Version.
- Beachten Sie die Webseite des Product Security Incident Response Teams (PSIRT) von Phoenix Contact für Sicherheitshinweise zu veröffentlichten Sicherheitslücken.

3.3 Aktuelle Sicherheits-Software verwenden

- Um Sicherheitsrisiken wie Viren, Trojaner und andere Schad-Software zu erkennen und auszuschalten, installieren Sie auf allen PCs eine Sicherheits-Software.
- Stellen Sie sicher, dass die Sicherheits-Software immer auf dem aktuellen Stand ist und die neuesten Datenbanken nutzt.

4 Phoenix Contact Sicherheitshinweise

4.1 Product Security Incident Response Team (PSIRT)

Das Product Security Incident Response Team (PSIRT) von Phoenix Contact sammelt und analysiert mögliche Sicherheitslücken in Produkten, Lösungen und Dienstleistungen von Phoenix Contact. Wenn eine Sicherheitslücke vorliegt, wird diese auf der PSIRT-Webseite unter „Aktuelle Sicherheitshinweise“ aufgelistet und ein entsprechender Sicherheitshinweis veröffentlicht. Die Webseite wird regelmäßig aktualisiert.

Um auf dem Laufenden zu bleiben, empfiehlt Phoenix Contact, den PSIRT-Newsletter zu abonnieren (unter „SERVICE“: „Anmeldung PSIRT-Newsletter“).

Jeder kann per E-Mail Informationen zu potenziellen Sicherheitslücken beim Phoenix Contact PSIRT einreichen.

Das Ziel des PSIRT ist es, mit den Meldern von Sicherheitslücken beim Umgang mit jeglichen vermuteten Sicherheitslücken bezüglich der Produkte, Lösungen und Dienste von Phoenix Contact professionell zusammenzuarbeiten.