Sicherheitsregeln

Sichern der Saia PCD®

Die Saia PCD® ist ein Netzwerkgerät und benötigt als solches eine geeignete Sicherheitskonfiguration, um die Gefahr eines unbefugten Zugriffs zu minimieren. Allgemeine Informationen über die Sicherung von SBC-Produkten entnehmen Sie bitte dem Informationsblatt «Allgemeine Sicherheitsvorkehrungen für IP-basierte Produkte von SBC». Zusätzlich zu Massnahmen im Informationsblatt «Allgemeine Sicherheitsvorkehrungen für IP-basierte Produkte von SBC» sind die nachfolgenden Empfehlungen zu beachten. Durch die Anwendung der gängigen Best-Practice-Richtlinien für Installation und Sicherheit verringern Sie die Gefahr eines böswilligen Angriffs auf Ihre IT durch gut ausgebildete und ausgestattete IT-Experten.

Sicherheitscheckliste

- ☐ Der Notfallwiederherstellungsplan beinhaltet alle relevanten Saia PG5®-Projekte, inklusive aller zugehörigen Bibliotheken.
- ☐ Der physikalische Zugriff auf die Saia PCD® ist eingeschränkt.
- ☐ Der physikalische Zugriff auf die mit der Saia PCD® verbundenen Netzwerke ist eingeschränkt.
- ☐ Auf allen PCDs von SBC wird die neueste Firmware-Version ausgeführt.
- ☐ Das Ethernet-Netzwerk ist gesichert (siehe «Netzwerkplanung und -sicherheit»).
- ☐ Alle nicht verwendeten Dienste, Ports und Kommunikationskanäle sind deaktiviert.
- ☐ Nicht erratbare Benutzernamen und starke Kennwörter wurden festgelegt.
- ☐ Den Saia PCD®-Benutzern wurde nur das Minimum an erforderlichen Berechtigungen erteilt.

Entwickeln eines Sicherheitsprogramms

Lesen Sie hierzu das Informationsblatt «Allgemeine Sicherheitsvorkehrungen für IP-basierte Produkte von SBC».

Notfallwiederherstellungsplan

Achten Sie bei der Aufstellung eines Notfallwiederherstellungsplans darauf, dass alle zum Wiederherstellen des Projekts benötigten Saia PG5®-Projektdateien und Bibliotheken eingeschlossen wurden.

Physikalische Voraussetzungen und Umgebungsbedingungen

Die Saia PCD® muss in einer geschlossenen Umgebung installiert werden, z. B. in einem gesicherten Anlagenraum oder abschließbaren Schaltschrank.
Bemerkung: Sorgen Sie für eine ausreichende Belüftung.

Sicherheits-Updates und Servicepakete

Stellen Sie sicher, dass auf allen Saia PCD®-Geräten die neueste Firmware-Version ausgeführt wird, insbesondere auf mit dem Internet verbundenen Systemen.

Virenschutz

Nicht zutreffend für die Saia PCD®.

Netzwerkplanung und -sicherheit

Ethernet-Netzwerk

Das von der Saia PCD® verwendete Ethernet-Netzwerk sollte möglichst über einen Luftspalt bzw. ein Virtual Private Network vom normalen Büronetzwerk getrennt sein.
Der physikalische Zugriff auf die Ethernet-Netzwerkinfrastruktur muss eingeschränkt werden. Zudem müssen Sie sicherstellen, dass die Installation den IT-Richtlinien Ihres Unternehmens genügt.
Die Saia PCD® darf nicht direkt mit dem Internet verbunden sein. Die Geräte müssen hinter einer Firewall oder in einem Virtual Private Network mit starkem Kennwortschutz und Internetsicherheitsprotokollen bereitgestellt werden, um die Gefahr eines unbefugten Zugriffs zu minimieren.

MS/TP-Netzwerk

Der physikalische Zugriff auf die MS/TP-Netzwerkinfrastruktur muss eingeschränkt werden.

RS-485-Netzwerk

Der physikalische Zugriff auf die RS-485-Netzwerkinfrastruktur muss eingeschränkt werden.

Profi-S-Bus-Netzwerk

Der physikalische Zugriff auf die Profi-S-Bus-Netzwerkinfrastruktur muss ein-geschränkt werden.

CAN-Netzwerk

Der physikalische Zugriff auf die CAN-Netzwerkinfrastruktur muss eingeschränkt werden.

USB

Der physikalische Zugriff auf den USB-Port der Saia PCD® muss eingeschränkt werden.

RS-232 (PGU)

Der physikalische Zugriff auf den RS-232(PGU)-Port der Saia PCD® muss eingeschränkt werden.

E/A-Bus

Der physikalische Zugriff auf den E/A-Bus der Saia PCD® muss eingeschränkt werden.

E/A-Erweiterungsport

Der physikalische Zugriff auf den E/A-Erweiterungsport der Saia PCD® muss eingeschränkt werden.

Dienste

Deaktivieren Sie alle nicht verwendeten Dienste. Sie verringern damit die Angriffsfläche und erhöhen die Leistung des Saia PCD®-Systems.

Webserver
Einige Saia PCD®-Geräte verwenden einen HTTP-Webserver, der bis zu zwei TCP-Ports überwachen kann. Es wird empfohlen, beide Überwachungsports zu deaktivieren. Wenn ein Webserver benötigt wird, stellen Sie sicher, dass dieser durch ein starkes Kennwort geschützt ist und dass Firewall-Regeln angewendet werden, um einen unerwünschten Zugriff zu verhindern.
Beachten Sie, dass Sie per HTTP mit Ihren FTP-Anmeldedaten auf das Dateisystem der Saia PCD® zugreifen können. Wenn der HTTP-Server aktiv ist, müssen Sie dafür sorgen, dass der FTP-Benutzer einen nicht erratbaren Benutzernamen und ein starkes Kennwort verwendet.

FTP-Server
Einige Saia PCD®-Geräte verwenden einen FTP-Dateiserver. Es wird empfohlen, den FTP-Server zu deaktivieren. Wenn ein FTP-Server benötigt wird, stellen Sie sicher, dass dieser durch die Verwendung nicht erratbarer Benutzernamen und starker Kennwörter geschützt ist.

BACnet IP
Aufgrund der geringen Sicherheit des BACnet-Protokolls dürfen Saia PCD®-Geräte, die BACnet IP unterstützen, unter KEINEN Umständen mit dem Internet verbunden werden. Das Saia PCD®-Sicherheitssystem bietet keinen Schutz vor BACnet-Schreibzugriffen. Der physikalische Zugriff auf die BACnet IP-Netzwerkinfrastruktur muss eingeschränkt werden. Wenn keine BACnet IP-Kommunikation benötigt wird, sollte die BACnet IP-Netzwerkkonfiguration im Saia PG5 Device Configurator deaktiviert werden.

SNMP-Server
Einige Saia PCD®-Geräte verwenden einen SNMP-Server. Der Zugriff auf den SNMP-Server erfolgt ohne Authentifizierung. Es wird daher empfohlen, den SNMP-Server zu deaktivieren. Wenn ein SNMP-Server benötigt wird, darf das Saia PCD®-Gerät unter KEINEN Umständen mit dem Internet verbunden sein. Zudem muss die SNMP-Konfiguration im Saia PG5 Device Configurator so definiert werden, dass nur eingeschränkter Zugriff erlaubt ist.

IP-Filterung
Die Saia PCD® ermöglicht ein White- und Blacklisting von IP-Adressen, um diesen den Zugriff auf das System zu erlauben bzw. zu untersagen. Es wird empfohlen, diesen Dienst zu aktivieren, da er zusätzliche Sicherheit bietet.

Virtuelle Umgebungen
Nicht zutreffend für die Saia PCD®.

Sichern von Drahtlosgeräten
Wenn ein Drahtlosnetzwerk verwendet wird, muss dieses entsprechend den IT-Richtlinien Ihres Unternehmens gesichert werden.

Systemüberwachung
Nicht zutreffend für die Saia PCD®.

Windows-Domänen
Nicht zutreffend für die Saia PCD®.

Allgemeine Sicherheitsvorkehrungen für IP-basierte Produkte von SBC

Die folgenden Best-Practice-Leitlinien helfen Ihnen, die Risiken zu minimieren. Die spezifischen Anforderungen jedes Standorts sind für jeden Fall separat zu prüfen. In den allermeisten Installationen würde eine Implementierung aller unten beschriebenen Sicherheitsvorkehrungen weit über das für eine angemessene Systemsicherheit erforderliche Mass hinaus gehen. Die Umsetzung der ersten vier Punkte für Local Area Networks erfüllt normalerweise die Anforderungen in den meisten Automations- und Leitnetzwerkinstallationen.

Local Area Networks (LAN) mit Komponenten von SBC
Um sicherzustellen, dass die Systeme eine angemessene Kennwortrichtlinie für den Benutzerzugriff auf die Dienste anwenden, fordert diese Leitlinie unter anderem Folgendes:
- Verwendung starker Kennwörter
- Empfohlenes Kennwortänderungsintervall
- Eindeutige Benutzernamen und Kennwörter für alle Systembenutzer
- Regeln für die Offenlegung von Kennwörtern

Verhindern Sie einen unbefugten Zugriff auf die Netzwerkgeräte, die in Verbindung mit den von der Saia-Burgess Controls AG bereitgestellten Systemen verwendet werden. Wie bei allen Systemen verringern Sie die Gefahr unbefugter Eingriffe, indem Sie den physikalischen Zugriff auf das Netzwerk und die Geräte unterbinden. Eine Best Practice für die Sicherheit von IT-Installationen ist es, Serverräume, Patchpanels und IT-Geräte in geschlossenen Räumen unterzubringen. Saia PCD®-Geräte müssen dementsprechend in geschlossenen Schaltschränken installiert werden, die sich wiederum in sicheren Anlagenräumen befinden.

Stellen Sie bei der Inbetriebnahme Folgendes sicher:
- Saia PCD® – Das Gerät ist mit einem Kennwort geschützt. Vergewissern Sie sich, dass den Benutzern entsprechende Benutzerebenen zugewiesen wurden.
- Visi.Plus – Das System ist mit einem Kennwort geschützt. Vergewissern Sie sich, dass den Benutzern entsprechende Benutzerebenen zugewiesen wurden, vom Administrator bis zum Basisbenutzer. Eine Best Practice ist es, die Zugriffsrechte für das Gastbenutzerkonto zu deaktivieren.

Wenden Sie eine geeignete Aktualisierungsrichtlinie für die installierte Infrastruktur als Bestandteil eines Service Level Agreements an. Die Richtlinie sollte u. a. die Aktualisierung der folgenden Systemkomponenten auf die neueste Version beinhalten:
- Geräte-Firmware für Controller, RIO, HMI usw.
- Supervisor-Software, wie Visi.Plus
- PC-/Serverbetriebssysteme
- Netzwerkinfrastruktur und alle Remote-Zugriffssysteme

Konfigurieren Sie separate IT-Netzwerke für die Automations- und Leitsysteme und für das unternehmensinterne IT-Netzwerk des Kunden. Hierzu können Sie entweder VLANs (virtuelle LANs) in der IT-Infrastruktur des Kunden konfigurieren oder eine separate, air-gapped Netzwerkinfrastruktur für die Automations- und Leitsysteme installieren.

Beschränken Sie nach der Inbetriebnahme des Systems den IP-Verkehr auf dem Automations- und Leitnetzwerk (z. B. mittels Zugriffslisten) auf die für den Normalbetrieb erforderlichen Protokolltypen, wie S-Bus, BACnet usw.
Weitere Informationen zu dem im Normalbetrieb erforderlichen Datenverkehr entnehmen Sie bitte der Produktdokumentation.

Wenn an der Schnittstelle zur Saia PCD® ein zentraler System-Supervisor (z. B. Visi-Plus) eingesetzt wird und das System keinen direkten Zugriff auf die Webserver einzelner Geräte benötigt, sollte der Webserverzugriff in der Konfiguration der Netzwerkinfrastruktur eingeschränkt werden.

Dynamische VLANs mit MAC-Adressenzuordnung können eine unbefugten Verbindung von Geräten mit dem System verhindern und die Gefahr minimieren, dass Informationen aus dem Netzwerk von Fremden abgehört werden.

Remotezugriff auf IT-basierte Gebäudeleitsysteme
- Für einen ggf. benötigten Remotezugriff auf die Saia PCD®-Systeme sollten Sie die VPN-Technologie (Virtual Private Network) verwenden, um die Gefahr, dass Daten abgehört werden, zu verringern und um zu verhindern, dass die Steuerungsgeräte direkt mit dem Internet verbunden sind.
- Das Produkt SBC.Connectivity ist eine verwaltete Konnektivitätslösung für die mobile Kommunikation, z. B. per GPRS, 3G usw., und für die drahtgebundene Kommunikation mit einer entfernten Saia PCD®. Der Dienst erzeugt ein sicheres Netzwerk für einen einfachen VPN-Zugriff auf die Geräte.

Kunden, die gängige Best-Practice-Richtlinien für Installation und Sicherheit anwenden, minimieren so die Gefahr eines böswilligen Angriffs auf ihre IT durch gut ausgebildete und ausgestattete IT-Experten. Ausführliche Informationen entnehmen Sie bitte der jeweiligen Produktdokumentation.

Saia-Burgess Controls AG
Bahnhofstrasse 18 | 3280 Murten | Schweiz | www.saia-pcd.com
T +41 26 580 30 00 | F +41 26 580 34 99
support@saia-pcd.com | www.sbc-support.com

Internationale Vertretungen und SBS Vertriebsgesellschaften:
www.saia-pcd.com/contact
PP26-620 11.2015 GER01