Beveiligingsregels

Saia PCD® beveiligen

Saia PCD®-producten bevinden zich in een netwerk en dus moet de beveiliging goed zijn geconfigureerd zodat het risico op ongeoorloofde toegang beperkt blijft. Voor algemene informatie over het beveiligen van SBC-producten raadpleegt u het informatieblad "Algemene best practices voor de beveiliging van producten die zijn gebaseerd op SBC IP".
Naast de acties die worden beschreven in het informatieblad "Algemene best practices voor de beveiliging van producten die zijn gebaseerd op SBC IP", moet het advies worden gevolgd dat wordt beschreven in de volgende secties. Het invoeren van normale algemeen aanbevolen installatie- en beveiligingsrichtlijnen beperkt het risico op een kwaadwillende IT-aanval door een ervaren en goed uitgeruste IT-expert.

Beveiligingschecklist

- ☐ Alle aanverwante Saia PG5®-projecten inclusief alle afhankelijke bibliotheken zijn opgenomen in het noodherstelplan.
- ☐ De fysieke toegang tot Saia PCD® is beperkt.
- ☐ De fysieke toegang tot netwerken die zijn aangesloten op Saia PCD® is beperkt.
- ☐ Op alle SBC PCD's wordt de meest recente versie van firmware uitgevoerd.
- ☐ Het Ethernet-netwerk is beveiligd – zie "Planning en beveiliging van het netwerk".
- ☐ Alle services, poorten en communicatiekanalen die niet worden gebruikt, zijn uitgeschakeld.
- ☐ Gebruikersnamen kunnen niet worden geraden en de ingestelde wachtwoorden zijn sterk.
- ☐ Gebruikers op Saia PCD® hebben rechten op het laagste niveau dat nodig is.

Een beveiligingsprogramma ontwikkelen
Raadpleeg het informatieblad "Algemene best practices voor de beveiliging van producten die zijn gebaseerd op SBC IP".

Noodherstel plannen
Bij de ontwikkeling van het noodherstelplan moet u ervoor zorgen dat alle relevante Saia PG5®-projectbestanden en alle bibliotheken die nodig zijn voor het opnieuw opbouwen van het project worden opgenomen.

Fysiek en omgeving
Saia PCD® moet worden geïnstalleerd in een afgesloten omgeving, bijvoorbeeld in een beveiligde installatieruimte of een afgesloten kast.
Opmerking: zorg voor afdoende ventilatie.

Beveiligingsupdates en servicepacks
Zorg dat overal op Saia PCD® de meest recente versie van de firmware wordt uitgevoerd, met name op systemen die naar internet zijn gericht.

Virusbescherming
Niet van toepassing voor Saia PCD®.

Planning en beveiliging van het netwerk

Ethernet-netwerk
Het is aan te bevelen het Ethernet-netwerk dat door Saia PCD® wordt gebruikt, met een air gap of VPN (virtual private network) gescheiden te houden van het normale kantoornetwerk. Fysieke toegang tot de infrastructuur van het Ethernet-netwerk moet worden beperkt. U moet er ook voor zorgen dat de installatie voldoet aan het IT-beleid van uw bedrijf. Saia PCD® mag niet rechtstreeks op internet worden aangesloten. De apparaten moeten veilig worden geïmplementeerd achter een firewall of in een VPN met sterke wachtwoordbeveiliging en andere beveiligingsprotocollen, om het risico op ongeoorloofde toegang tot een minimum te beperken.

MS/TP-netwerk
Fysieke toegang tot de infrastructuur van het MS/TP-netwerk moet worden beperkt.

RS-485-netwerk
Fysieke toegang tot de infrastructuur van het RS-485-netwerk moet worden beperkt.

Profi-S-Bus-netwerk
Fysieke toegang tot de infrastructuur van het Profi-S-Bus-netwerk moet worden beperkt.

CAN-netwerk
Fysieke toegang tot de infrastructuur van het CAN-netwerk moet worden beperkt.

USB
Fysieke toegang tot de Saia PCD® USB-poort moet worden beperkt.

RS-232 (PGU)
Fysieke toegang tot de Saia PCD® RS-232 (PGU)-poort moet worden beperkt.

I/O-aansluiting
Fysieke toegang tot de Saia PCD® I/O-aansluiting moet worden beperkt.

I/O-uitbreidingspoort
Fysieke toegang tot de Saia PCD® I/O-uitbreidingspoort moet worden beperkt.

Services
Schakel alle services uit die niet worden gebruikt. Hierdoor verkleint u het aanvalsoppervlak en kunnen de prestaties van een Saia PCD®-systeem beter worden.

Webserver
Sommige Saia PCD®-systemen worden geleverd met een HTTP-webserver die kan luisteren op maximaal twee TCP-poorten. U wordt aangeraden beide luisterende poorten uit te schakelen. Als er een webserver nodig is, zorg dan dat de webserver is beveiligd met een sterk wachtwoord en dat er firewallregels zijn ingesteld ter bescherming tegen ongewenste toegang.
Let op: het is mogelijk het bestandssysteem van een Saia PCD® te benaderen via HTTP met behulp van FTP-toegangsgegevens. Als de HTTP-server actief is, moet u ervoor zorgen dat FTP-gebruikers niet-raadbare gebruikersnamen en sterke wachtwoorden hebben.

FTP-server
Sommige Saia PCD®-systemen worden geleverd met een FTP-bestandsserver. U wordt aangeraden de FTP-server uit te schakelen. Als er een FTP-server nodig is, zorg dan dat de FTP-server is beveiligd met niet-raadbare gebruikersnamen en sterke wachtwoorden.

BACnet IP
Vanwege de onveilige aard van het BACnet-protocol mogen Saia PCD®-systemen die BACnet IP ondersteunen, ONDER GEEN ENKELE VOORWAARDE worden aangesloten op internet. Het beveiligingssysteem van Saia PCD® beschermt niet tegen schrijfacties van BACnet. Fysieke toegang tot de infrastructuur van het BACnet IP-netwerk moet worden beperkt. Als er geen BACnet IP-communicatie nodig is, moet de BACnet IP-netwerkconfiguratie in de Saia PG5 Device Configurator worden uitgeschakeld.

SNMP-server
Sommige Saia PCD®-systemen worden geleverd met een SNMP-server. Voor de toegang tot de SNMP-server is geen verificatie nodig. U wordt aangeraden de SNMP-server uit te schakelen. Als er een SNMP-server nodig is, mogen Saia PCD®-apparaten ONDER GEEN ENKELE VOORWAARDE worden aangesloten op internet. Bovendien moet de SNMP-configuratie in Saia PG5 Device Configurator zodanig worden uitgevoerd dat alleen beperkte toegang is toegestaan.

IP-filter
Saia PCD® staan het gebruik toe van witte en zwarte lijsten met IP-adressen waaraan toegang tot het systeem moet worden verleend of geweigerd. U wordt aangeraden deze service in te schakelen als extra beveiligingslaag.

Virtuele omgevingen
Niet van toepassing voor Saia PCD®.

Draadloze apparaten beveiligen
Als er een draadloos netwerk wordt gebruikt, moet dit in overeenstemming met het IT-beleid van uw bedrijf worden beveiligd.

Systeembewaking
Niet van toepassing voor Saia PCD®.

Windows-domeinen
Niet van toepassing voor Saia PCD®.

Algemene best practices voor de beveiliging van producten die zijn gebaseerd op SBC IP

De volgende richtlijnen staan in volgorde van toenemende beperking. De exacte vereisten van elke site moeten per geval worden bepaald. Voor de grote meerderheid van de installaties geldt dat wanneer alle hieronder beschreven beperkingsniveaus worden geïmplementeerd, dat veel meer is dan nodig is voor een afdoende systeembeveiliging. Het implementeren van de eerste vier punten met betrekking tot LAN's (Local Area Networks) is in het algemeen voldoende om te voldoen aan de vereisten voor de meeste netwerkinstallaties voor automatiseringsbeheer.

LAN's (Local Area Networks) met SBC-componenten
Zorg dat de systemen werken met een geschikt wachtwoordbeleid voor gebruikerstoegang voor alle services. Deze richtlijn moet in ieder geval het volgende omvatten:
- Het gebruik van sterke wachtwoorden
- Een aanbevolen tijdsduur waarna wachtwoorden moeten worden gewijzigd
- Unieke gebruikersnamen en wachtwoorden voor elke gebruiker van het systeem
- Regels voor het openbaar maken van wachtwoorden

Voorkom ongeoorloofde toegang tot de netwerkapparatuur die wordt gebruikt samen met systemen die worden geleverd door Saia-Burgess Controls AG. Voor elk systeem geldt dat het voorkomen van fysieke toegang tot het netwerk en de apparatuur het risico op ongeoorloofde interferentie verlaagt. Met best practices voor de beveiliging van IT-installaties zorgt u ervoor dat serverruimtes, patchpanelen en IT-apparatuur zich in afgesloten ruimtes bevinden. Saia PCD®-apparatuur moet worden geïnstalleerd in afgesloten kasten, die zich op hun beurt weer bevinden in beveiligde ruimtes.

Houd bij het uitvoeren van opdrachten rekening met het volgende:
- Saia PCD® – zorg dat het apparaat is beveiligd met een wachtwoord. Zorg dat er geschikte gebruikersniveaus zijn toegewezen aan de gebruikers van de site.
- Visi.plus – zorg dat het apparaat is beveiligd met een wachtwoord. Zorg dat er geschikte gebruikersniveaus zijn toegewezen aan de gebruikers van de site, van administratieve gebruikers tot aan algemene gebruikers. Het is een best practice om de toegangsrechten voor gastgebruikers uit te schakelen.

Implementeer een geschikt updatebeleid voor de op de site geïnstalleerde infrastructuur, als onderdeel van een SLA (serviceovereenkomst). Onderdeel van dit beleid moet in ieder geval zijn dat de volgende systeemcomponenten worden bijgewerkt naar de meest recente versie:
- Firmware voor apparaten als controller, RIO, HMI, enz.
- Supervisorsoftware, zoals Visi.Plus-software
- Besturingssystemen voor pc's/servers
- Netwerkinfrastructuren en eventuele systemen voor externe toegang

Configureer afzonderlijke IT-netwerken voor de automatiseringsbeheersystemen en het bedrijfs-IT-netwerk van de klant. U kunt dit doen door VLAN's (virtuele LAN's) te configureren binnen de IT-infrastructuur van de klant of door een speciale afzonderlijke netwerkinfrastructuur met air gap te installeren voor de automatiseringsbeheersystemen.
Als het systeem eenmaal is opgezet, beperkt u IP-verkeer op het automatiseringsbeheernetwerk (bijvoorbeeld met toegangslijsten) tot de protocoltypen die nodig zijn voor normaal gebruik, dus S-Bus, BACnet enz. Raadpleeg de productdocumentatie voor meer informatie over het communicatieverkeer dat nodig is voor normaal gebruik.
Wanneer Saia PCD® wordt benaderd via een gecentraliseerde systeemsupervisor (zoals Visi.Plus) waarbij het systeem geen rechtstreekse toegang nodig heeft tot de webserver van de afzonderlijke apparaten, moet de netwerkinfrastructuur zodanig worden geconfigureerd dat toegang tot de webserver wordt beperkt.
Dynamische VLAN's die gebruik maken van MAC-adrestoewijzing, kunnen beveiliging bieden tegen het ongeoorloofd verbinding maken van een apparaat met het systeem, en kunnen het risico verlagen dat ontstaat als een persoon informatie op het netwerk bekijkt.

Voor externe toegang tot IT-gebouwbesturingssystemen
- Als externe toegang tot Saia PCD® -systemen nodig is, gebruikt u VPN-technologie (Virtual Private Network) om het risico te verlagen dat er gegevens worden onderschept en om te voorkomen dat de besturingsapparaten rechtstreeks op internet worden geplaatst.
- Het SBC.Connectivity-product is een oplossing voor beheerde connectiviteit die mobiele communicatie zoals GPRS, 3G enz. mogelijk maakt, evenals bedrade communicatie voor externe verbindingen met Saia PCD®. De service voorziet in een beveiligd netwerk dat eenvoudige VPN-toegang tot de apparaten biedt.

Klanten die normale algemeen aanbevolen installatie- en beveiligingsrichtlijnen invoeren, beperken het risico op een kwaadwillende IT-aanval door een ervaren en goed uitgeruste IT-expert. Raadpleeg de documentatie van het desbetreffende product voor meer informatie.

Saia-Burgess Controls AG
Bahnhofstrasse 18 | 3280 Murten | Zwitserland | 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 vertegenwoordigers & SBC Sales-bedrijven:
www.saia-pcd.com/contact
PP26-620 11.2015 DUT01