Regole di protezione

Come proteggere Saia PCD®

Saia PCD® offre prodotti di rete che, in quanto tali, devono avere una protezione configurata correttamente per ridurre il rischio di un accesso non autorizzato. Per informazioni generali sulla protezione dei prodotti SBC consultare «Best practice generali per la protezione dei prodotti SBC basati su IP». Oltre alle azioni descritte in questo documento è necessario attenersi ai consigli contenuti nelle sezioni seguenti. Adottare le normali best practice per l'installazione e la protezione può ridurre il rischio di un attacco IT dannoso da parte di un informatico dotato delle conoscenze e degli strumenti necessari per violare il sistema.

Checklist per la protezione

- ☐ Tutti i progetti relativi a Saia PG5®, comprese tutte le librerie dipendenti, sono inclusi nel piano di ripristino di emergenza.
- ☐ L'accesso fisico a Saia PCD® è limitato.
- ☐ L'accesso fisico alle reti collegate a Saia PCD® è limitato.
- ☐ Tutti i dispositivi PCD SBC eseguono l'ultima versione del firmware.
- ☐ Rete Ethernet protetta, vedere «Pianificazione e protezione della rete».
- ☐ Tutti i servizi, le porte e i canali di comunicazione non in uso sono disattivati.
- ☐ Sono impostati nomi utenti impossibili da indovinare e password molto sicure.
- ☐ Gli utenti di Saia PCD® dispongono solo dei privilegi meno richiesti.

Sviluppo di un programma di protezione

Fare riferimento a «Best practice generali per la protezione dei prodotti SBC basati su IP».

Pianificazione del ripristino di emergenza

Quando si sviluppa il piano di ripristino di emergenza è necessario accertarsi che esso includa tutti i file di progetto Saia PG5® pertinenti e tutte le librerie per ricreare il progetto.

Considerazioni di carattere fisico e ambientale

Saia PCD® deve essere installato all'interno di un ambiente sicuro, ad esempio nel locale protetto di un impianto o in un armadio dotato di serratura.
Nota: garantire una ventilazione adeguata.

Aggiornamenti di protezione e service pack

Accertarsi che tutti i Saia PCD® eseguano l'ultima versione del firmware, soprattutto sui sistemi con connessione Internet.

Protezione antivirus

Non applicabile a Saia PCD®.

Pianificazione e protezione della rete

Rete Ethernet

Si consiglia di separare la rete Ethernet utilizzata da Saia PCD® dalla normale rete dell'ufficio mediante un air gap o una rete virtuale privata.
È necessario limitare l'accesso fisico all'infrastruttura della rete Ethernet. Inoltre, è necessario garantire che l'installazione sia conforme ai criteri informatici della propria azienda.
Saia PCD® non deve essere collegato direttamente a Internet. I dispositivi vanno distribuiti in maniera sicura dietro un firewall o in una rete virtuale privata protetta da una password molto sicura e da protocolli di sicurezza informatica per ridurre al minimo il rischio di un accesso non autorizzato.

Rete MS/TP

È necessario limitare l'accesso fisico all'infrastruttura della rete MS/TP.

Rete RS-485

È necessario limitare l'accesso fisico all'infrastruttura della rete RS-485.

Rete Profi-S-Bus

È necessario limitare l'accesso fisico all'infrastruttura della rete Profi-S-Bus.

Rete CAN

È necessario limitare l'accesso fisico all'infrastruttura della rete CAN.

USB

È necessario limitare l'accesso fisico alla porta USB di Saia PCD®.

RS-232 (PGU)

È necessario limitare l'accesso fisico alla porta RS-232 (PGU) di Saia PCD®.

Bus I/O

È necessario limitare l'accesso fisico al bus I/O di Saia PCD®.

Porta di estensione I/O

È necessario limitare l'accesso fisico alla porta di estensione I/O di Saia PCD®.

Servizi

Disattivare tutti i servizi non in uso. Questa operazione riduce la superficie esposta all'attacco e può migliorare le prestazioni di un sistema Saia PCD®.

Server Web
Alcuni Saia PCD® forniscono un server Web HTTP che può essere in ascolto su due porte TCP al massimo. Si consiglia di disattivare entrambe le porte in ascolto. Se è necessario utilizzare un server Web accertarsi che sia protetto da una password molto sicura e che siano implementate delle regole firewall per impedire l'accesso non autorizzato.
Ricordare che è possibile accedere al file system di un Saia PCD® mediante il protocollo HTTP utilizzando le credenziali FTP. Se il server HTTP è attivo accertarsi che gli utenti FTP abbiano nomi utenti impossibili da indovinare e password molto sicure.

Server FTP
Alcuni Saia PCD® forniscono un server file FTP. Si consiglia di disattivare il server FTP. Se è necessario utilizzare un server FTP accertarsi che sia protetto mediante nomi utente impossibili da indovinare e password molto sicure.

BACnet IP
A causa della natura poco sicura del protocollo BACnet, i Saia PCD® che supportano BACnet IP NON DEVONO essere collegati a Internet in nessuna circostanza. Il sistema di protezione Saia PCD® non protegge dalle scritture BACnet. È necessario limitare l'accesso fisico all'infrastruttura della rete BACnet IP. Se le comunicazioni BACnet IP non sono richieste, la configurazione della rete BACnet IP deve essere disattivata nel Device Configurator di Saia PG5.

Server SNMP
Alcuni Saia PCD® forniscono un server SNMP. L'accesso al server SNMP avviene senza autenticazione. Si consiglia di disattivare il server SNMP. Se è necessario utilizzare un server SNMP il dispositivo Saia PCD® NON DEVE essere collegato a Internet in nessuna circostanza. Inoltre, la configurazione SNMP effettuata nel Device Configurator di Saia PG5 deve consentire solo l'accesso limitato.

Filtro IP
Saia PCD® consente la creazione di liste bianche e nere per garantire o negare l'accesso al sistema. Si consiglia di attivare questo servizio per fornire un ulteriore livello di protezione.

Ambienti virtuali
Non applicabile a Saia PCD®.

Protezione dei dispositivi wireless
Se si utilizza una rete wireless è necessario proteggerla in conformità ai criteri informatici della propria azienda.

Monitoraggio del sistema
Non applicabile a Saia PCD®.

Domini Windows
Non applicabile a Saia PCD®.

Best practice generali per la protezione dei prodotti SBC basati su IP

Le guideline seguenti sono state pensate per migliorare la prevenzione. I requisiti specifici di ogni sito vanno valutati caso per caso. La grande maggioranza delle installazioni che implementano tutti i livelli di prevenzione descritti di seguito supera di gran lunga i criteri necessari per una protezione soddisfacente dei sistemi. In genere, integrare i primi quattro elementi nelle reti locali (LAN) è sufficiente per soddisfare i requisiti della maggior parte delle installazioni delle reti di controllo automazione.

Reti locali (LAN) che integrano i componenti Saia-Burgess Controls AG
Accertarsi che il sistema utilizzi criteri password appropriati per l'accesso degli utenti a tutti i servizi inclusi in queste guideline, ma non limitati a:
- Utilizzo di password molto sicure
- Una durata ciclo consigliata per le password
- Nomi utenti e password univoci per ogni utente del sistema
- Regole di diffusione password

Prevenire l'accesso non autorizzato alle apparecchiature di rete utilizzate insieme ai sistemi forniti da Saia-Burgess Controls AG. In qualsiasi sistema prevenire l'accesso fisico alla rete e alle apparecchiature riduce il rischio di interferenza da parte di utenti non autorizzati. Le best practice per la protezione delle installazioni informatiche prevedono che i locali dei server, i pannelli di interconnessione e le apparecchiature IT siano protetti in ambienti dotati di serrature. L'apparecchiatura Saia PCD® deve essere installata all'interno di armadi con serratura, posizionati a loro volta nei locali protetti di un impianto.

Quando si completa la messa in servizio di:
- Saia PCD®: accertarsi che il dispositivo sia protetto da una password. Accertarsi che agli utenti del sito siano assegnati livelli utente appropriati.
- Visi.Plus: accertarsi che il sistema sia protetto da una password. Accertarsi che agli utenti del sito siano assegnati livelli utente appropriati, dall'utente amministratore fino all'utente generico. È una buona norma disattivare i diritti di accesso per l'account dell'utente guest.

Adottare criteri di aggiornamento appropriati per l'infrastruttura installata sul sito nell'ambito di un contratto di servizio. I criteri devono includere, ma non solo, l'aggiornamento dei seguenti componenti di sistema all'ultima versione:
- Firmware dispositivo per controller, RIO, HMI, ecc.
- Software supervisore, ad esempio Visi.Plus
- Sistemi operativi di PC/server
- Infrastruttura di rete e altri sistemi di accesso remoto

Configurare reti IT separate per i sistemi di controllo automazione e per la rete informatica aziendale del cliente. È possibile effettuare questa operazione configurando le reti VLAN (LAN virtuali) all'interno dell'infrastruttura IT del cliente o installando un'infrastruttura di rete separata da air gap e dedicata ai sistemi di controllo automazione.

Una volta messo in servizio il sistema, limitare il traffico IP sulla rete di controllo automazione (ad esempio mediante elenchi di accesso) ai tipi di protocollo richiesti per il funzionamento normale, ovvero S-Bus, BACnet, ecc… Ulteriori informazioni sul traffico richiesto per il funzionamento normale sono disponibili nella documentazione del prodotto.

Se si interfaccia Saia PCD® mediante un supervisione di sistema centralizzato (ad esempio Visi.Plus) e il sistema non richiede l'accesso diretto al server Web di singoli dispositivi, l'infrastruttura di rete deve essere configurata in modo da limitare l'accesso al server Web.

Assegnando gli indirizzi MAC è possibile proteggere le reti VLAN dinamiche dal collegamento non autorizzato di un dispositivo al sistema e ridurre il rischio associato a una singola informazione di monitoraggio sulla rete.

Per l'accesso remoto ai sistemi di controllo edifici basati su IT
- Se l'accesso remoto è necessario nei sistemi Saia PCD®, utilizzare la tecnologia VPN (Virtual Private Network) per ridurre il rischio dell'intercettazione dei dati e per proteggere i dispositivi di controllo dal posizionamento diretto in Internet.
- SBC.Connectivity è una soluzione di connettività gestita che facilita le comunicazioni mobili come GPRS, 3G, ecc. e la comunicazione cablata per il collegamento remoto a Saia PCD®. Il servizio fornisce una rete sicura che offre un semplice accesso VPN ai dispositivi.

I clienti che adottano le normali best practice per l'installazione e la protezione possono ridurre il rischio di un attacco IT dannoso da parte di un informatico dotato delle conoscenze e degli strumenti necessari per violare il sistema. Ulteriori informazioni sono disponibili nella documentazione specifica del prodotto.

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

Rappresentanti di vendita e azienda partner SBC internazionali:
www.saia-pcd.com/contact
PP26-620 11.2015 ITA01