

Leitfaden IT-Sicherheit von PLT-Systemen in Betriebsstätten des WVER

Die Entwicklungen der letzten Jahre in der Prozess-Leittechnik und der Unternehmensstruktur lassen eine isolierte lokale Bedienung und Beobachtung einer Automation als nicht mehr zeitgemäß erscheinen.

Hierbei ist ein Zusammenwachsen der physikalischen Plattformen der Office-IT und der PLT als großer Kostenvorteil zu werten. Allem voran sind hierbei Standardisierungen mittels Windows/Intel und TCP/IP/Ethernet gemeint.

Komponenten und Dienstleistungen sind beherrschbarer und schneller verfügbar als früher. Diese Entwicklung birgt aber auch Gefahren. Probleme der Office-IT wie Schadsoftware und Sabotage sind nun auch in der Produktionsebene präsent.

Daher sind bei Neuanschaffungen und Migrationen von Leitsystemen folgende Richtlinien zu beachten:

1. Die SPS-Ebene ist physikalisch vom Intranet zu trennen

- Eigener Switch.
- Eigenes IP-Netz zur separaten Netzwerkkarte des PLS-Servers.
- Kein Eintrag des Standardgateways in der SPS.
- Der Kennwort-Schreibschutz der SPS ist zu aktivieren.
- Der IP-Schutz (falls vorhanden) ist zu aktivieren.
- Sollten Steuerungen über das Netz umgesetzt werden, so muss verschlüsselt werden und der IP-Schutz aktiviert sein.

2. Der PLT-Server/Client

- Die Hard- und Software wird durch das zentrale Sachgebiet 3.54 IT/PLT projektiert und beschafft.
- Der lokale PLT-Server verfügt über 2 Netzwerkkarten:
Eine für das Intranet und eine weitere für das SPS-Netz.
- Der lokale PLT-Server verfügt über mindestens 2 baugleiche Festspeichersysteme welche ohne RAID betrieben werden.
- Standorte mit Schichtbetrieb-Besetzung werden mit redundanten Systemen ausgestattet.
- Einbindung in den zentralen Active-Directory-Service (ADS) der IT/PLT.

- In der Firewall (zentrale Vorgabe der ADS) aktivierte Ausnahmen werden von der IT-Sicherheit vorgegeben.
- Anforderung Betriebssysteme: Mindestens Windows 10 oder Windows 2016 Server (unter Beachtung der Kompatibilität des Leitsystemlieferanten).
- Der zentrale Anti-Virus mit mindestens täglicher Aktualisierung ist zu installieren.
- Betriebssystem-Updates sind automatisiert zu installieren.
 Client: Die Installation der OS-Updates erfolgt automatisch. Sollte ein Neustart erforderlich sein, wird dieser vom Betriebspersonal durchgeführt. Erfolgt dies nicht, so wird nach Ablauf einer vorgegebenen Zeit der Neustart automatisch ausgeführt.
 Server: Die Installation der OS-Updates erfolgt durch das zentrale Sachgebiet 3.54 der IT/PLT. Sind Neustarts erforderlich so werden diese in Absprache mit dem Betriebspersonal durchgeführt.
 Anwendungsupdates werden anlassbezogen in Absprache mit dem Betriebspersonal durch das zentrale Sachgebiet 3.54 IT/PLT installiert.
- Netzfregaben sind nur mit ADS-Userkonten vorzunehmen. Das Jeder-Konto mit Vollzugriff wird nicht verwendet. Netzfregaben werden ausnahmslos durch das zentrale Sachgebiet 3.54 IT/PLT vorgenommen.
- OPC-DA DCOM-Berechtigungen sind nur auf die ADS-Konten zu legen welche einen Zugriff benötigen.
- Der Gastzugriff bleibt gesperrt.
- Administratoren-Kennwörter haben min. 8 Stellen und beinhalten ein Sonderzeichen.
- Das lokale und zentrale Administratoren-Kennwort der PLT-Anwendung und deren OS sowie der dazugehörigen Logfiles ist nur der zentralen Administration des UB 3.5 und dem Fachbereich IT bekannt.
- Der Wartungszugriff erfolgt ausnahmslos über den VPN-Zugang der WVER-IT (FB 2.5). Ein VPN-Account ist durch den Dienstvorgesetzten zu beantragen. Bei externen Dienstleistern erfolgt die Beantragung über den UB 3.5.
 Eine direkte Einwahl in das WVER-Intranet unter Umgehung der WVER-Sicherheitssysteme ist untersagt.
- Der Zugriff mittels Remote-Viewer-Tools mit Administratorenrechte ist nur von ausgewiesenen Usern oder IP-Adressen möglich.
- Einen Wartungszugriff einer Fremdfirma muss vorher erfragt und terminiert werden.
- Installationen von Software, insbesondere Remoteapplikationen sind von der IT/PLT-Leitung im Vorfeld zu genehmigen.
- Bei Lieferung von Hard- und Software verpflichtet sich der Auftragnehmer dahingehend, dass die Komponenten frei von Funktionen sind, welche der Vertraulichkeit, Integrität und Verfügbarkeit zuwiderläuft. Dies bezieht sich auf Funktionen zum unerwünschten Aus- oder Einleiten von Daten sowie dem Manipulieren von Daten oder der Ablauflogik von Funktionserweiterungen.

3. Bedienung von Prozessbildern

- Die Bedienungsberechtigung der lokalen Prozessbilder wird vom Abwassermeister geregelt. Hierbei sind die User-Gruppen der Administratoren, der Bedienungsberechtigten und der Beobachter bereits vorgegeben. Lokale Benutzerkonten mit Bedienberechtigungen benötigen einen Personenbezogenen Account.

4. Web-Bilder

- Es wird gemäß Beschluss der Dezernatskonferenz vom 18.04.2012 keine Bedienung über Web ermöglicht.
- Parametrier-Buttons der Trend- und Alarmfenster, welche nicht temporär sind, müssen deaktiviert werden.

5. Datensicherung und Datenschutz

- Die Sicherung der Betriebsdaten erfolgt im Minutentakt auf ein zentrales Speichermedium der Verwaltung des WVER und wird von dort im 24 h Takt auf ein weiteres räumlich getrenntes Speichermedium gespiegelt.
- Imagesicherungen der lokalen Systeme werden alle 3 Monate erstellt und vor Ort gesichert. 3 Quartalskopien werden auf einem zentralen NAS-System gesichert.
- Bei lokalen Änderungen der SPS/PLS-Programme ist umgehend das zentrale Sachgebiet 3.54 IT/PLT zu benachrichtigen bzw. die aktuelle Programmversion der Backup-Administration zwecks zentraler Sicherung zu übergeben.
- Das zentrale Sachgebiet 3.54 IT/PLT ist zur Einhaltung von IT-Standards und Datenschutzbestimmungen verpflichtet und weisungsbefugt gegenüber internen wie externen Dienstleistern in der Ausführung ihrer IT-bezogenen Tätigkeit.

6. WLAN

Beim Einsatz von WLAN-Techniken sind folgende Sicherheitseinstellungen zu beachten:

- Der WPA2-Schlüssel ist 32-stellig, Groß-/Kleinschreibung sowie min. zwei Sonderzeichen.
- Der MAC-Filter für kommunizierende Endgeräte ist einzurichten.
- Die SSID ist als „unsichtbar“ zu deklarieren.
- Das WLAN-Routerpasswort ist 32-stellig, Groß-/Kleinschreibung, sowie min. zwei Sonderzeichen (darf nicht gleich mit dem WPA2-Schlüssel sein).

7. Messtechnik

- Änderungen an der Messtechnik, welche zentral aufgezeichnet werden sind umgehend dem UB 3.5 zu melden.

Hierbei sind folgende Punkte gemeint:

- Änderung des Messbereiches.
- Ausfall der Messung oder Stilllegung.
- Umbenennung der Messeinrichtung.
- Änderung des Messortes.

8. Beschaffung

- Die Beschaffung von PLT Hard- und Software ist durch die DA00_1205 geregelt und erfolgt über den zentralen Sachbereich 3.54 IT/PLT oder wird von dort aus freigegeben.

Wilhelm Frings

Sachbereichsleiter UB 3.54