Ciberseguridad en plantas industriales con IIoT

¿Qué hay que tener en cuenta?

Las soluciones IIoT y los servicios digitales ofrecen un alto potencial para optimizar las instalaciones industriales. ¿Cuáles son los criterios de seguridad de los datos para evaluar la seguridad de un servicio digital?

Endress+Hauser

No hay duda de que la computación en la nube y el Internet de las cosas (IoT) han afectado al mundo de la industria. Las soluciones IIoT y los servicios digitales ofrecen un alto potencial para optimizar las instalaciones industriales. Antes de elegir e implementar una nueva solución digital, surge la cuestión de la ciberseguridad en las plantas industriales. Cuando se utiliza para proteger las plantas operativas, así como la propiedad intelectual de una empresa, todas las nuevas tecnologías digitales deben demostrar que son seguras.

¿Cuáles son los criterios de seguridad de los datos para evaluar la seguridad de un servicio digital? ¿Hasta qué punto puede confiar en su gestión de la seguridad de la información? ¿Cuáles son los principales aspectos de la ciberseguridad en la industria con respecto al procesamiento de datos sensibles? Cada vez que se implementa una solución IIoT en una instalación industrial, contiene datos confidenciales que requieren un grado especial de protección. Además, la conectividad a Internet necesita atención y cuidado permanente. La tecnología se desarrolla muy rápidamente, y cada sistema debe seguir continuamente la evolución de la ciberseguridad, tanto en una planta industrial como en cualquier otra instalación. La gestión fiable

» La tecnología se desarrolla muy rápidamente y cada sistema debe seguir continuamente la evolución de la ciberseguridad

» Antes de elegir e implementar una nueva solución digital, surge la cuestión de la ciberseguridad en las plantas industriales

de la seguridad de la información no solo comprende el cifrado de datos, sino que también requiere un enfoque general que incluya:

- **Cumplimiento de la legislación y las normas:** deben cumplirse las directrices legales pertinentes y las normas recomendadas (por ejemplo, ISO 27001, GDPR, etc.).

- **Seguridad de los datos:** es evidente que una solución IIoT contendrá datos confidenciales. Estos deben ser tratados con cuidado de acuerdo con procesos estrictos.

- **Ubicaciones de servidor:** siempre que se utilice la tecnología de computación en la nube, los datos se almacenarán en servidores alojados por el proveedor. Debido a la jurisdicción local, la ubicación de los servidores indica un nivel más alto o menor de ciberseguridad. Las ubicaciones europeas ofrecen los más altos estándares gracias a la ley de privacidad de datos.

- **Procesos organizativos:** la ciberseguridad no es posible sin emplear procesos organizativos que definan qué datos deben ser tratados por quién, de qué manera y en qué momento.

- **Transparencia:** los proveedores de confianza de soluciones digitales tienen un sistema de soporte claro y transparente que muestra al cliente el estado de su consulta en cualquier momento.

- **Características de la aplicación**: la interfaz de usuario de un servicio digital debe tener características de ciberseguridad relevantes con respecto a las contraseñas, cierre de sesión, etc. Todos esos puntos deben ser considerados, implementados y revisados regularmente al proporcionar una tecnología IIoT. Los marcos, leyes y prácticas recomendadas existentes de auditoría y normalización pueden ser un apoyo práctico durante la implementación.

- **Cumplimiento de la legislación y las normas**: al establecer una gestión profesional de la seguridad de la información mediante tecnologías IIoT, el sistema debería cumplir con los siguientes estándares básicos:

  - Gestión de la seguridad de la información ISO 27001.
  - Sistema de gestión de servicios ISO 20000.
  - Sistema de Gestión de Calidad ISO 9001.

- **Seguridad de los datos:** los usuarios tienen derecho a introducir, acceder, actualizar y eliminar sus datos almacenados y procesados en el Cloud. Todas las medidas deben cumplir con los requisitos del RGPD.

- **Ubicaciones de servidores:** desde el punto de vista de la ciberseguridad, los servidores ubicados en la Unión Europea se consideran unos de los más seguros.

- **Procesos organizativos:** el proveedor de servicios tiene que tener un proceso para reaccionar rápidamente en casos de emergencias de seguridad de datos, todo conforme al RGPD. Se informará inmediatamente a las partes afectadas y se tomarán las contra acciones.