Certificaciones de seguridad de Endress+Hauser

De los equipos de campo a la nube

Para alcanzar fácilmente su cumplimiento de ciberseguridad, cuente con un colaborador de confianza

Los instrumentos de medida y componentes de Endress+Hauser aseguran el funcionamiento fiable de las plantas de proceso de incontables instalaciones industriales de todo el mundo.

La ciberseguridad en las plantas industriales y en el Internet industrial de las cosas es cada vez más importante.

Para acreditar la calidad de nuestros productos, hemos probado nuestros sistemas frente a algunos de los estándares de seguridad más prestigiosos del mundo de la TI y la TO, y hemos obtenido las certificaciones correspondientes.

Contacto

Póngase en contacto con su delegación local de Endress+Hauser
www.addresses.endress.com

¿Desea más información acerca de Netilion?

netilion.endress.com

Requisitos de ciclo de vida de desarrollo de productos Para ofrecer la mejor protección posible a los centros de producción de nuestros clientes, Endress+Hauser pone las bases de un funcionamiento seguro ya en la fase de planificación y desarrollo de sus productos y servicios.

TÜV Rheinland ha confirmado que el proceso de desarrollo de este producto y la gestión de ciclo de vida de los productos son conformes con los estándares internacionales más estrictos y están certificados según IEC 62443-4-1.

Seguridad de la información es crucial

Endress+Hauser Digital Solutions es el centro de competencia en IIoT y digitalización del Grupo Endress+Hauser. Esta entidad ha obtenido el certificado ISO 27001 para seguridad de la información. El sistema está diseñado de modo que se asegura el cumplimiento de la normativa aplicable, como, por ejemplo, los reglamentos de protección de datos (SGPD, RGPD).

El cumplimiento de esta norma internacional representa un gran hito para nuestra organización.

- En primer lugar, porque queda garantizada la seguridad de la información y los datos de nuestros clientes.
- En segundo lugar, porque una entidad de certificación externa ha confirmado que nuestro sistema garantiza la validez, idoneidad y mejora continua de nuestras medidas de seguridad.

Seguridad en la nube para Netilion

Una entidad de certificación externa ha confirmado que el ecosistema de IIoT Netilion cumple los requisitos de ISO 27017. Esta norma reconocida internacionalmente incluye requisitos adicionales para plataformas seguras en la nube. Los servicios basados en la nube ofrecen una gran variedad de funciones útiles. Sin embargo, también pueden aumentar la superficie de ataque de las empresas, lo cual genera recelo a la hora de utilizarlos. El cumplimiento de los requisitos de ISO 27017 garantiza que los clientes pueden confiar en el ecosistema Netilion para alojar sus datos de manera segura.

Endress+Hauser
People for Process Automation

Funciones y características Para cumplir todos los requisitos, el software debe incorporar las funciones y características adecuadas. A continuación se resumen algunas de las medidas de seguridad que adoptamos.

Cifrado mediante contraseña Para asegurar la confidencialidad de las contraseñas del usuario, no las almacenamos en texto sin formato. En el lado del usuario, las contraseñas se cifran con “bcrypt + salt + pepper”, y únicamente guardamos en nuestra base de datos el hash.

OAuth Para ofrecer una identificación de usuario segura durante el uso del software, utilizamos autenticación por token para identificar a los usuarios en el acceso a nuestro servicio de nube. Las contraseñas de usuario se transmiten únicamente para generar el token. Esto dificulta los intentos de estafa y garantiza una autorización segura.

Solo canales de comunicación cifrada La comunicación con nuestro servicio de nube se establece siempre mediante conexión https segura y cifrada. De este modo, todos los datos útiles se cifran de acuerdo con estándares del sector, y nuestros ordenadores en la nube se autentican de manera fiable mediante un certificado emitido por una entidad de certificación de prestigio mundial.

Información del usuario Al acceder a su cuenta, el usuario puede ver sus actividades anteriores. Esos mismos mecanismos se usan en la banca online para detectar posibles usos fraudulentos o intentos fallidos de inicio de sesión.

Procesos Para hacer frente a posibles incidentes de seguridad graves, que no pueden excluirse ni siquiera en los entornos más seguros, hemos definido una serie de procesos internos que nos permitirían reaccionar con la máxima celeridad e informar a todas las partes afectadas con el fin de mantener a salvo a nuestros clientes.

Ubicación de los servidores Trabajamos con los proveedores de alojamiento en la nube más potentes del mundo, y solo usamos ubicaciones de servidor en Europa. Estos servidores se operan bajo el amparo de la legislación y la jurisdicción europeas, unas de las más estrictas del mundo. Nuestros clientes pueden confiar en que sus datos están protegidos por los estándares de seguridad más elevados del planeta.

Seguridad de datos con edge device Un edge device es un punto crítico de la arquitectura, ya que representa el punto de acceso a la planta del usuario y desde ella. Un equipo FieldEdge registra únicamente datos de campo y los transmite a la nube. Cuando se usa una función de Netilion que requiere escribir en un equipo de campo, la operación se documenta y tiene que ser autorizada previamente por el usuario. Los equipos FieldEdge descargan sus actualizaciones de firmware de la nube de Netilion. Por lo tanto, todos los puertos entrantes desde Internet a los equipos FieldEdge están bloqueados. A fin de garantizar la seguridad de las descargas, estas actualizaciones se firman y se comparan con el archivo original para evitar manipulaciones.

En el desarrollo de los equipos FieldEdge se aplican desde el primer momento los requisitos de IEC 62443.

Datos de clientes Todos los datos de clientes que utilizamos son de propiedad exclusiva del cliente. Nos reservamos el derecho a acceder a dichos datos con el propósito de prestar nuestros servicios. En el caso de que compartamos datos de clientes con otros proveedores de servicios, informamos a nuestros clientes acerca de dicha cooperación antes de proceder al intercambio de datos y nos aseguramos de que el mencionado proveedor de servicios actúe conforme a las normas y condiciones especificadas.

Gobernanza Todas las actividades y medidas se adoptan para proteger Netilion, así como los datos que contiene, en el marco de un sistema más extenso en el que todos los procesos se rigen por políticas, estándares, procesos e instrucciones declarados. Este enfoque global asegura que todas las partes de la cadena de valor de la información estén claramente identificadas y protegidas de la manera adecuada en cada caso.

www.addresses.endress.com

PU01272S/04/ES/05.21

Endress+Hauser

People for Process Automation