Certificados de segurança Endress+Hauser

Dos equipamentos em campo até a nuvem

Facilite sua conformidade de segurança cibernética com um parceiro de confiança

Os instrumentos de medição e componentes Endress+Hauser garantem a operação confiável das instalações de processo em incontáveis empresas no mundo todo.

A segurança cibernética na indústria e a Internet das Coisas Industrial (IIoT, na sigla em inglês) está se tornando cada vez mais importante.

Para provar a qualidade de nossos produtos, testamos nossos sistemas contra alguns dos padrões de segurança mais conhecidos no mundo do TI e TO, e obtemos os certificados correspondentes.

Contato
Entre em contato com a sua filial Endress+Hauser local
www.addresses.endress.com

Mais detalhes sobre o Netilion?

netilion.endress.com

Requisitos seguros do ciclo de vida de desenvolvimento do produto

Para oferecer a melhor proteção possível para as instalações produtivas de seus clientes, a Endress+Hauser estabelece os alicerces para operações seguras desde as etapas de planejamento e desenvolvimento de seus produtos e serviços.

A TÜV Rheinland confirmou que esse processo de desenvolvimento de produtos, assim como o gerenciamento do ciclo de vida dos produtos, atende aos mais altos padrões internacionais com uma certificação conforme IEC 62443-4-1.

Segurança das informações é essencial

Endress+Hauser Digital Solutions é o centro de competência para IIoT e digitalização no Grupo Endress+Hauser. Essa entidade conquistou a certificação ISO 27001 para segurança das informações. O sistema foi construído para assegurar a conformidade a normas aplicáveis, como as regulamentações de proteção de dados DSMS, GDPR).

Alcançar esse padrão internacional é um novo marco para a organização.

- Primeiro, a segurança das informações e dados dos clientes é garantida.
- Segundo, um órgão de certificação externo confirmou que nosso sistema garante que nossas medidas de segurança sejam corretas, adequadas e estejam sempre sendo aprimoradas.

Segurança na nuvem para o Netilion

Um órgão de certificação externo confirmou que o ecossistema de IIoT Netilion atende aos requisitos do ISO 27017. Esse padrão reconhecido internacionalmente contém requisitos adicionais para plataformas baseadas em nuvem seguras. Serviços baseados em nuvem oferecem uma grande variedade de recursos úteis. Ao mesmo tempo, eles podem aumentar a superfície de ataque das empresas – o que aumenta seu medo de usá-las. A conformidade com os requisitos do ISO 27017 garante que os clientes podem confiar que o ecossistema Netilion oferece um porto seguro para seus dados.

Endress+Hauser
People for Process Automation

Funções e recursos Para cumprir todos os requisitos, é necessário ter funções e recursos adequados implementados no software. Os elementos à seguir descrevem algumas das medidas de segurança que tomamos.

Criptografia de senhas Para oferecer a confidencialidade das senhas, nós não as armazenamos em texto claro. Do lado do usuário, as senhas são criptografadas com 'bcrypt + salt + pepper' e nós salvamos apenas a hash em nossa base de dados.

OAuth Para suportar a identificação segura de usuários durante o uso do software, usamos um processo baseado em token para identificar usuários em relação ao nosso serviço na nuvem. As senhas dos usuários são transmitidas apenas para geração do token. Isso complica as tentativas de fraude e garante uma autorização segura.

Canais de comunicação criptografados apenas O canal de comunicação ao nosso serviço na nuvem é sempre estabelecido através de uma conexão https segura e criptografada. Assim, todos os processamentos de dados são criptografados conforme padrões da indústria, e nossos computadores na nuvem são autenticados com segurança através de um certificado emitido por uma autoridade de certificação de renome mundial.

Informações do usuário Ao acessar sua conta, o usuário é capaz de visualizar atividades passadas. Os mesmos mecanismos de bancos onlines são usados para detectar possíveis fraudes ou tentativas falhas de login.

Processos No caso de incidentes sérios de segurança, que podem ocorrer no mais seguro dos ambientes, temos processos internos estabelecidos para reagir o mais rápido possível e informar todas as partes afetadas de forma a manter nossos clientes seguros.

Localização do servidor Utilizamos os mais fortes parceiros em hosting na nuvem do mundo e usamos servidores localizados apenas na Europa. Esses servidores são operados sob as leis e jurisdição europeias, que são umas das mais rígidas do mundo. Nossos clientes podem ter certeza de que seus dados estão sujeitos a um dos maiores padrões de segurança de dados do mundo.

Segurança de dados do edge device Um edge device é um ponto crítico na arquitetura porque representa o ponto de acesso da planta do usuário ou para a planta. Um dispositivo FieldEdge registra apenas dados do campo e os transmite para a nuvem. Se for usado uma função do Netilion que requer escrever em um dispositivo de campo, esse procedimento é documentado e precisa ser confirmado pelo usuário com antecedência.

Um FieldEdge baixa suas atualizações de firmware do serviço na nuvem Netilion. Assim, todas as portas de entrada da Internet para os dispositivos FieldEdge devem ser bloqueados. Além disso, para garantir downloads seguros, essas atualizações são assinadas e verificadas com o arquivo original para evitar manipulação.

Os requisitos IEC 62443 serviram de base para o desenvolvimento dos dispositivos FieldEdge desde o início.

Dados do cliente Todos os dados de clientes usados por nós são propriedade apenas do cliente. Reservamos o direito de acessar esses dados para prover nossos serviços. Caso compartilhemos os dados de clientes com prestadores de serviço terceirizados, informamos nossos clientes sobre essa parceria antes da troca de dados e garantimos que esse prestador de serviço aja conforme os termos e condições fornecidos.

Governança Todas as atividades e medidas são tomadas para proteger o Netilion e os dados contidos pelo Netilion como parte de um sistema maior, onde todos os processos são governados por políticas, padrões, processos e instruções detalhados. Essa abordagem holística garante que todas as partes da cadeia de valores da informação sejam identificadas claramente e protegidas conforme suas necessidades.

www.addresses.endress.com

PU01272S/04/PT/05.21

Endress+Hauser

People for Process Automation