Endress+Hauser veiligheidscertificaten

Van instrument naar de cloud

Waarborg uw compliance op het gebied van cyberbeveiliging met een betrouwbare partner:
Endress+Hauser meetinstrumenten waarborgen de betrouwbare werking van procesinstallaties op talloze locaties wereldwijd.

Cyberveiligheid van industriële installaties en Industrial Internet of Things worden steeds belangrijker.

Om de kwaliteit van onze producten aan te kunnen tonen, hebben wij onze systemen getest aan de hand van de meest bekende veiligheidsnormen binnen de IT- en OT-wereld en hebben wij de bijbehorende certificering gekregen.

Contact:
Neem contact op met uw lokale Endress+Hauser vertegenwoordiging
www.addresses.endress.com

Meer informatie over Netilion?

netilion.endress.com

Verzekerd van productontwikkeling gedurende de levensduur Om de productiefaciliteiten van klanten zo goed mogelijk te beschermen, wordt er al in de plannings- en ontwikkelinsfase van de producten en diensten van Endress+Hauser, de basis gelegd voor een veilige werking.

TÜV Rheinland heeft bevestigd dat zowel het productontwikkelingsproces als het levenscyclusmanagement van de producten, voldoet aan de strengste internationale normen met de certificering conform IEC 62443-4-1.

Informatieveiligheid is essentieel
Endress+Hauser Digital Solutions is het competentiecentrum voor IIoT en digitalisatie van de Endress+Hauser Group. Deze afdeling heeft het ISO 27001-certificaat ontvangen voor informatieveiligheid. Het systeem is opgebouwd teneinde te voldoen aan de geldende regelgeving, zoals de regelgeving op het gebied van gegevensbescherming (DSMS, GDPR). Voldoen aan deze internationale norm is een nieuwe mijlpaal voor de organisatie.

- Op de eerste plaats wordt de veiligheid van de informatie en de gegevens van de klanten gewaarborgd.
- Op de tweede plaats heeft een extern certificeringsinstituut bevestigd dat ons systeem de juistheid, adequaatheid en voortdurende verbetering van onze veiligheidsmaatregelen waarborgt.

Cloud-beveiliging voor Netilion Een extern certificeringsinstituut heeft bevestigd dat het IIoT ecosysteem Netilion voldoet aan de eisen van ISO 27017. Deze internationaal erkende norm bevat aanvullende eisen voor veilige cloud-platforms. Cloud-based diensten bieden veel verschillende nuttige functionaliteiten. Tegelijkertijd kunnen deze het aanvalspotentieel van bedrijven vergroten, waardoor de angst om deze te gebruiken toeneemt. Voldoen aan de eisen uit de ISO 27017 waarborgt dat klanten kunnen vertrouwen op het Netilion-ecosysteem als veilige haven voor hun gegevens.

Endress+Hauser
People for Process Automation

Functies en eigenschappen Om te voldoen aan alle voorwaarden, is het noodzakelijk om de juiste eigenschappen en functies in de software te implementeren. Hier volgt een overzicht van enkele veiligheidsmaatregelen die wij hebben genomen.

Encryptie van wachtwoorden Om de vertrouwelijkheid van de gebruikerswachtwoorden te realiseren, bewaren wij deze niet als platte tekst. Aan de gebruikerszijde worden wachtwoorden gecodeerd met 'bcrypt + zout + peper' en bewaren we alleen de hash in onze database.

OAuth Om een veilige gebruikersidentificatie te ondersteunen tijdens het gebruik van de software, gebruiken we een token voor het identificeren van de gebruikers met onze cloud-service. Gebruikerswachtwoorden worden alleen overgedragen voor het genereren van tokens. Hierdoor wordt scamming gecompliceerder en wordt een veilige autorisatie gegarandeerd.

Alleen gecodeerde communicatiekanalen Het communicatiekanaal met onze cloud-service verloopt altijd via een veilige en gecodeerde https-verbinding. Daarbij wordt alle payload data gecodeerd conform industriële normen en onze cloudcomputers zijn betrouwbaar geverifieerd met een certificaat, uitgegeven door een wereldwijd gerenommeerd certificeringsinstituut.

Gebruikersinformatie De gebruiker heeft toegang tot het account en kan alle activiteiten uit het verleden bekijken. Dezelfde methodes worden gebruikt bij online bankieren voor het detecteren van mogelijk frauduleus gebruik of mislukte inlogpogingen.

Processen In geval van serieuze veiligheidsincidenten, welke zelfs in de meest veilige omgeving voordoen, hebben wij interne processen gemaakt om zo snel mogelijk te reageren en alle betrokken partijen te informeren teneinde onze klanten te beschermen tegen mogelijke schade.

Serverlocatie Wij gebruiken de beste cloud hosting-partners ter wereld en gebruiken alleen serverlocaties in Europa. Deze servers vallen onder het Europese recht en de Europese jurisdictie, welke de strengste is ter wereld. Onze klanten kunnen er zeker van zijn dat de gegevens onderworpen zijn aan de hoogste data-beveiligingsnormen ter wereld.

Edge Device data-beveiliging Een edge device is een kritisch punt in de architectuur omdat het een toegangspunt is van en naar de installatie van de gebruiker. Een FieldEdge device registreert alleen data uit het veld en draagt deze over naar de cloud. Wanneer een Netilion-functie wordt gebruikt waarbij schrijven naar een veldinstrument nodig is, wordt dit gedocumenteerd en moet vooraf door de gebruiker worden bevestigd.
Een FieldEdge download de firmware-updates uit de Netilion-cloud. Alle inkomende poorten van het internet naar de FieldEdge-instrumenten worden geblokkeerd. Om veilige downloads te garanderen, zijn deze updates gesigneerd en worden gecontroleerd met het originele bestand om manipulatie te voorkomen.

IEC 62443-voorschriften vormden de basis voor het ontwikkelen van de FieldEdge-instrumenten vanaf het allereerste begin.

Klantgegevens Alle klantgegevens die door ons worden gebruikt zijn alleen eigendom van de klant. Wij behouden ons het recht tot toegang tot deze gegevens voor, om onze diensten te kunnen leveren. Wanneer wij de klantgegevens delen met derden, zullen wij onze klanten vooraf over deze samenwerking informeren en garanderen dat deze dienstverlener ook werkt conform de genoemde voorwaarden en richtlijnen.

Beheer Alle activiteiten en maatregelen worden genomen om Netilion en de gegevens binnen Netilion te beveiligen als onderdeel van een groter systeem, waarbij alle processen worden beheerd door gedetailleerd beleid, standaarden, processen en instructies. Deze holistische aanpak zorgt ervoor dat alle delen van de informatie-waardeketen duidelijk zijn geïdentificeerd en beveiligd conform de behoeften.

www.addresses.endress.com

PU01272S/04/NL/05.21

Endress+Hauser

People for Process Automation