Endress+Hauser Sicherheits-zertifizierungen

Von Feldgeräten in die Cloud

Erleichtern Sie Ihre Cybersecurity-Compliance mit einem verlässlichen Partner
Endress+Hauser Messgeräte und Komponenten gewährleisten den zuverlässigen Betrieb von Prozessanlagen in zahllosen Einrichtungen weltweit.

Cybersecurity in Industrieanlagen und dem Industrial Internet of Things gewinnt immer mehr an Bedeutung.

Um den Nachweis für die Qualität unserer Produkte zu erbringen, haben wir unsere Systeme gegen einige der bekanntesten Sicherheitsnormen in der IT- und OT-Welt getestet und die entsprechende Zertifizierung erhalten.

Kontakt
Bitte wenden Sie sich an Ihren lokalen Endress+Hauser Standort
www.addresses.endress.com

Mehr Details zu Netilion?

netilion.endress.com

Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung
Um den bestmöglichen Schutz für die Produktionseinrichtungen der Kunden zu bieten, legt Endress+Hauser bereits im Planungs- und Entwicklungsprozess seiner Produkte und Dienstleistungen die Grundlagen für einen sicheren Betrieb.

TÜV Rheinland hat mit der Zertifizierung der IEC 62443-4-1 bestätigt, dass Endress+Hauser die Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung erfüllt.

Informationssicherheit ist essentiell
Endress+Hauser Digital Solutions ist das Product Center für das IIoT und Digitalisierung in der Endress+Hauser Gruppe. Diese Organisation wurde nach ISO 27001 für Informationssicherheit zertifiziert. Das System ist so aufgebaut, dass es die Einhaltung geltender Vorschriften, wie z. B. Datenschutzbestimmungen (DSMS, DS-GVO), gewährleistet.

Die Erfüllung dieser internationalen Norm setzte einen neuen Meilenstein für das Unternehmen.

- Erstens ist die Sicherheit der Kundeninformationen und -daten gewährleistet.
- Zweitens bestätigte eine externe Zertifizierungsstelle, dass unser System die Korrektheit, Angemessenheit und kontinuierliche Verbesserung unserer Sicherheitsmaßnahmen sicherstellt.

Cloud-Sicherheit für Netilion Eine externe Zertifizierungsstelle bestätigte, dass das IIoT Ökosystem Netilion die Anforderungen aus ISO 27017 erfüllt. Diese international anerkannte Norm enthält zusätzliche Anforderungen für sichere Cloud-Plattformen. Cloud-basierte Dienste bieten eine hohe Vielfalt nützlicher Funktionalitäten. Gleichzeitig können sie die Angriffsfläche von Unternehmen erhöhen – wodurch eine stärkere Furcht vor ihrer Nutzung besteht. Die Konformität mit den Anforderungen aus ISO 27017 gewährleistet, dass Kunden sich auf die Sicherheit ihrer Daten im Netilion Ökosystem verlassen können.

Endress+Hauser
People for Process Automation

Funktionen und Leistungsmerkmale Um alle Anforderungen zu erfüllen, müssen die entsprechenden Funktionen und Leistungsmerkmale in der Software implementiert sein. Im Folgenden erläutern wir kurz die von uns ergriffenen Sicherheitsmaßnahmen.

Passwortverschlüsselung Um dem Benutzer einen erhöhten Passwortschutz zu bieten, speichern wir Passwörter nicht in Klartext. Auf der Benutzerseite werden Passwörter mit “bcrypt + Salt + Pepper” verschlüsselt, und wir speichern lediglich den Hash in unserer Datenbank.

OAuth Um eine sichere Benutzeridentifizierung während der Nutzung zu unterstützen, setzen wir einen Token-basierten Prozess ein, mit dem sich die Benutzer unseres Cloud-Services identifizieren lassen. Die Benutzerpasswörter werden ausschließlich zur Generierung der Tokens übertragen. Diese Vorgehensweise erschwert Scamming-Angriffe und gewährleistet eine sichere Autorisierung.

Nur verschlüsselte Kommunikationskanäle Der Kommunikationskanal zum Cloud-Service wird immer über eine sichere und verschlüsselte HTTPS-Verbindung hergestellt. Auf diese Weise werden alle Nutzlastdaten nach Industriestandards verschlüsselt. Zudem sind unsere Cloud-Services durch ein Zertifikat authentifiziert, das von einer weltweit anerkannten Zertifizierungsstelle ausgestellte wurde.

Benutzerinformationen Wenn ein Benutzer auf sein Konto zugreift, kann er sich seine letzten Aktivitäten anzeigen lassen. Die gleichen Mechanismen werden für Online-Banking verwendet, um eine mögliche betrügerische Nutzung oder fehlgeschlagene Anmeldeversuche zu erkennen.

Prozesse Für den Fall, dass es zu einem schwerwiegenden Sicherheitsvorfall kommen sollte – was selbst in der sichersten Umgebung vorkommen kann – haben wir hierfür interne Prozesse implementiert. Somit können wir so schnell wie möglich auf derartige Vorfälle reagieren und alle betroffenen Parteien informieren, um unsere Kunden wirkungsvoll zu schützen.

Server-Standort Wir arbeiten mit den stärksten Cloud-Hosting-Partnern weltweit zusammen und nutzen ausschließlich Server-Standorte in Europa. Diese Server befinden sich damit innerhalb der europäischen Gerichtsbarkeit und werden gemäß der europäischen Gesetzgebung – bei der es sich um die strengste weltweit handelt – betrieben. Unsere Kunden können vollkommen sicher sein, dass ihre Daten einem der höchsten Standards für Datensicherheit unterliegen.

Edge Device Datensicherheit Ein Edge Device ist ein kritischer Punkt in der Architektur, da es den Zugangspunkt von und zur Anlage des Benutzers darstellt. Ein FieldEdge Gerät zeichnet nur Daten aus dem Feld auf und überträgt diese in die Cloud. Wenn eine Netilion Funktion verwendet wird, die das Schreiben auf ein Feldgerät erfordert, wird dies dokumentiert und muss vom Benutzer vorher bestätigt werden.

Ein FieldEdge lädt seine Firmware-Updates von der Netilion Cloud herunter. Somit werden alle eingehenden Ports über das Internet zu den FieldEdge Geräten blockiert. Um sichere Downloads zu garantieren, werden diese Aktualisierungen signiert und gegen die Originaldatei geprüft, um Manipulationen zu verhindern. Die Anforderungen der IEC 62443 dienten von Anfang an als Grundlage für die Entwicklung der FieldEdge Geräte.

Kundendaten Alle von uns verwendeten Kundendaten sind ausschließliches Eigentum des Kunden. Wir behalten uns das Recht vor, auf diese Daten zuzugreifen, um unseren Service zu erbringen. Wenn wir Kundendaten externen Dienstleistern mitteilen müssen, informieren wir unsere Kunden vor dem Daten-austausch über diese Zusammenarbeit und stellen sicher, dass dieser Dienstleister gemäß den vorgegebenen Bedingungen und Leitfäden handelt.

Governance Alle Aktivitäten und Maßnahmen werden ergriffen, um Netilion und die Daten in Netilion als Teil eines größeren Systems zu schützen, in dem alle Prozesse durch detaillierte Richtlinien, Standards, Prozesse und Anweisungen geregelt sind. Dieser ganzheitliche Ansatz gewährleistet, dass alle Teile der Informationswertschöpfungskette eindeutig identifiziert und gemäß ihrem jeweiligen Bedarf geschützt werden.

Umweltfreundlich produziert und gedruckt auf Papier aus nachhaltiger Forstwirtschaft.

www.addresses.endress.com

PU01272S/04/DE/05.21

Endress+Hauser

People for Process Automation