White paper

Cybersecurity für die Monitoring Box inklusive Gateway

Author
Falko Kraus, Product management - Endress+Hauser SICK GmbH+Co. KG
Dr. Sören Geffken, Research & Development - Endress+Hauser SICK GmbH+Co. KG

Endress+Hauser
People for Process Automation

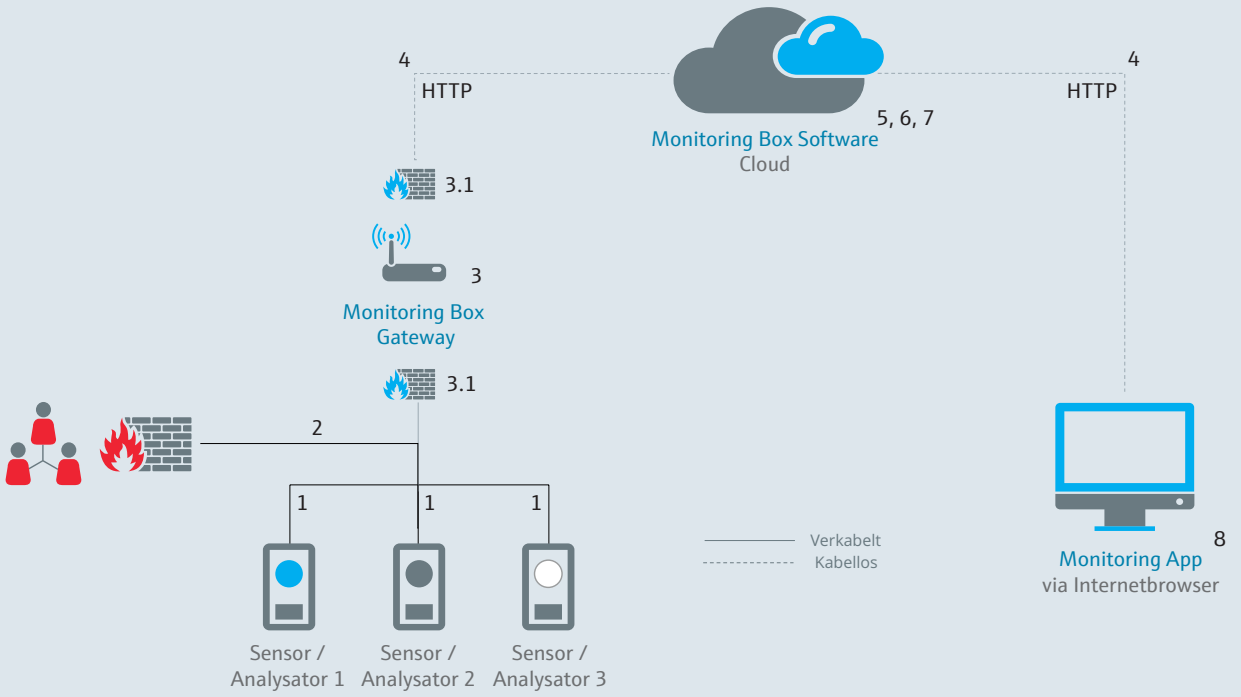
1. Einleitung und Hintergrund

Als Bestandteil seiner Serviceprodukte hat Endress+Hauser ein neues System aus Software und Hardware entwickelt: die Monitoring Box. Dieses System ermöglicht es, statusrelevante Daten aus Analysatoren und Sensoren mithilfe einer Kombination aus einem Gateway und einer Cloud-Anwendung in einem Online-Dashboard zu visualisieren (Condition Monitoring). Durch die permanente Überwachung und Auswertung statusrelevanter Parameter unterstützt Endress+Hauser den Kunden dabei, die Verfügbarkeit seiner Geräte zu erhöhen, die Serviceaufwände zu verringern, und bietet die Grundlage für Data-Analytic-Services wie Predictive Maintenance.
Um das System (Monitoring Box), die Daten und die damit verbundenen Geräte des Kunden zu schützen und die Risiken im Bereich der IT-Sicherheit zu minimieren, hat Endress+Hauser diverse Maßnahmen getroffen.

Die folgenden Seiten richten sich an Interessenten der Monitoring Box und geben eine erste Übersicht über die Cybersecurity-
Maßnahmen, wie sie bei einer standardmäßigen Installation der Monitoring Box vorhanden sind. Individualisierte Installationen und individuelle IT-Infrastrukturen erfordern gegebenenfalls weitere Maßnahmen oder Anpassungen bestehender Maßnahmen.

2. Hardwarekomponenten

Um mit der Monitoring Box eine Zustandsüberwachung für Sensoren implementieren zu können, ist das Zusammenspiel verschiedener Hard- und Softwarekomponenten nötig. In der folgenden Systemübersicht werden diese Komponenten beschrieben und es wird im Einzelnen auf die jeweilige Komponente und die für die IT-Sicherheit getroffenen Maßnahmen eingegangen.



(1) Unidirektionaler Datenverkehr (nur lesender Zugriff auf die Sensordaten)
(2) Unabhängige Datenübertragung, da nicht im Kundennetzwerk
(3) Firewall integriert im Monitoring Box Gateway
(4) SSL/TLS-Verschlüsselung durch HTTPS
(5) Validierung von Eingangsdaten an jeglichen Schnittstellen
(6) Brute-force Schutzmaßnahmen
(7) Kontinuierliche Überwachung der verwendeten Softwarepakete auf Schwachstellen
(8) Role-Based-Access

Abb.1: Die Systemübersicht zeigt, welche Schutzmaßnahmen Endress+Hauser an welcher Stelle im System getroffen hat, um die Kommunikation und die übermittelten Daten vor Angriffen und Manipulationen zu schützen.

2.1. Monitoring Box Gateway

Das Monitoring Box Gateway (SSG-E) in Abb. 2 fungiert als Gateway, um Daten der Analysatoren und Sensoren direkt von der Edge zu sammeln und als Smart Data an die Cloud zu übertragen.
Die Monitoring Box nutzt standardmäßig die Einwegkommunikation vom Gateway zur Cloud. Die Sensordaten werden an das Gateway übergeben und an die Endress+Hauser-Cloud gesendet. Die Konfiguration der Sensoren oder die Kommunikation der Sensordaten in die andere Richtung ist nicht vorgesehen. In der Standardkonfiguration ist das Gateway über eine gesicherte Verbindung mit einem Wartungskanal versehen, sodass Endress+Hauser problemlos Sicherheitsupdates einspielen kann.

Abb.2: Monitoring Box Gateway

2.2. Server

Um die Daten bei der Übertragung von der Monitoring Box zum Server und bei der Übertragung vom Server zum Dashboard oder Frontend zu schützen, wird die Verschlüsselung, Authentifizierung und Identifikation mit TLS umgesetzt.
Die Server, auf denen die Daten der Monitoring Box verarbeitet werden, stehen in Deutschland und unterliegen dadurch deutschem und europäischem Recht und somit insbesondere der DSGVO. Einrichtung und Einhaltung diverser Sicherheitsmaßnahmen verhindern den Zugriff und die Manipulation durch Unbefugte. Jegliche Datenkommunikation ist durch Authentifizierung und Autorisierung entsprechend geschützt, sodass Berechtigungen beim Lesen und Schreiben der Daten auf allen Kommunikationsebenen geprüft, gesichert und eingehalten werden.

2.3. Sensoren

Die Datenübertragung vom Sensor zum Monitoring Box Gateway realisiert Endress+Hauser mithilfe diverser Protokolle und Plugins (z.B. TCP/IP oder RS485). Die Übertragung der Daten vom Analysator oder Sensor an das Monitoring Box Gateway und von dort an den Server lässt sich unabhängig vom Kundennetzwerk über dedizierte Schnittstellen durchführen. Die physikalische oder virtuelle Trennung der involvierten Netze verhindert einen Eingriff in das lokale Kundennetzwerk. Die Übertragung vom Sensor erfolgt kabelgebunden über die in der Industrie üblichen Protokolle wie TCP/IP, serielle Schnittstellen wie Modbus RS485 oder USB. Dank der erwähnten unidirektionalen Verbindung zwischen Analysator bzw. Sensor und Gateway ist ein Zugriff auf den Analysator oder Sensor über die Monitoring Box nicht möglich.

3. Softwarekomponenten

Die wesentliche Softwarekomponente aus Sicht des Nutzers der Monitoring Box ist die Browseranwendung (Dashboard oder auch Frontend genannt). Der Zugriff auf das Dashboard erfolgt über https://monitoringbox.endress.com. Die Authentifizierung findet über das Single-Sign-on-System von Endress+Hauser – Entra-ID – statt. Die Autorisierung für den Zugriff auf die gespeicherten Daten wird mithilfe rollenbasierter Zugriffskontrolle überprüft.
Die folgenden Abschnitte beschreiben die für die sichere Nutzung der Browseranwendung von Endress+Hauser vorausgesetzte Umgebung und die Schutzmaßnahmen zur Sicherstellung der sicheren Nutzung und des Datenschutzes.

3.1. Browseranwendung

Über die Browseranwendung erhalten Nutzer Zugriff auf die Funktionen der Monitoring Box und hierbei insbesondere Einblicke in die aufgezeichneten Sensordaten.
Jeder Nutzer hat eine eindeutige Nutzerkennung, eine Endress+Hauser-Identifikationsnummer. Jedem Nutzeraccount werden nach Anmeldung auf dem Dashboard nur die jeweils zugehörigen und eigenen Assets angezeigt. Um eine eindeutige Zuordnung der erfolgten Serverzugriffe nachzuweisen, dürfen keine Gruppenaccounts eingesetzt werden. Dieses dient der Nachvollziehbarkeit der angeforderten Daten, sodass eine Überprüfung aufgetretener Fehler und fehlgeschlagener Zugriffsversuche möglich ist.

3.2. Genutzte Protokolle

Bei der Datenübertragung zwischen Gateway und Cloud sowie zwischen Cloud und Frontend oder Browser werden gängige Protokolle genutzt. Bei der Implementierung der Software hat Endress+Hauser allgemein anerkannte Sicherheitsmaßnahmen getroffen. Im Folgenden sind die wichtigsten Protokolle und Standards exemplarisch beschrieben.

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) ist ein Kommunikationsprotokoll, mit dem die Daten abhörsicher über das Internet übertragen werden. Es stellt eine Transportverschlüsselung per TLS dar. Die HTTPS-Kommunikation zwischen Dashboard und Server ist den üblichen Sicherheitsanforderungen entsprechend konfiguriert, sodass bekannte Angriffsszenarien auf die Kommunikation nicht umsetzbar sind.

TLS

TLS ist ein hybrides Verschlüsselungsprotokoll und fester Bestandteil der HTTPS-Verschlüsselung. Es dient der Authentifikation von Client und Server bei der Datenübertragung im Internet. Endress+Hauser verwendet neue TLS-Versionen. Die Verwendung älterer Versionen zur Unterstützung älterer Browserversionen wird ständig geprüft und neu bewertet.

SSH
Secure Shell (SSH) bezeichnet sowohl ein Netzwerkprotokoll als auch Programme, mit deren Hilfe man auf sichere Art und Weise eine verschlüsselte Netzwerkverbindung mit einem Ferngerät herstellen kann. Endress+Hauser nutzt SSH für Fernwartungen des Monitoring Box Gateways. Die für die Fernwartung genutzten Dienste sind nicht direkt aus dem Internet und aus dem lokalen Netzwerk erreichbar.

TCP
Das Standardprotokoll TCP ist beim Datentransfer vom Analysator oder Sensor zum Gateway im Einsatz.

Serielle Protokolle
Sensoren und Analysatoren, die über keine TCP-Schnittstelle verfügen, lassen sich über serielle Protokolle wie Modbus RTU an die Monitoring Box anbinden.

4. Cybersecurity

Um das System gegenüber Schadsoftware und anderen IT-sicherheitsrelevanten Gefahren zu schützen, hat Endress+Hauser verschiedene Cybersecurity-Maßnahmen umgesetzt. Der Fokus lag hierbei zunächst auf einem unabhängigen externen Sicherheitsaudit. Auf Basis von dessen Ergebnissen wurden anschließend relevante Themen bezüglich der Datensicherheit und Datenintegrität identifiziert und konkrete Maßnahmen hierfür abgeleitet.

Externer Sicherheitsaudit
Mit der Durchführung des Sicherheitsaudits hat Endress+Hauser ein unabhängiges Unternehmen betraut. Im Zuge dieses Audits wurden verschiedene Aspekte der Monitoring Box bezüglich Cybersecurity ausführlich und umfassend getestet.

4.1. Generelle Überprüfung
Der Startpunkt für das externe Audit war eine gründliche Analyse der Dashboard-Applikation. Im Zuge dieser Maßnahme wurden im ersten Schritt die verwendeten Authentifizierungs- und Autorisierungsmechanismen getestet. Hierbei lag der Fokus insbesondere auf Folgendem: Es war sicherzustellen, dass einzelne Benutzer nur exakt die Aktionen durchführen konnten, für die sie zuvor eine Berechtigung erhalten hatten.
Ein weiterer Schwerpunkt dieser Analyse war eine umfassende Untersuchung der während der Datenkommunikation verwendeten Verschlüsselungstechnologien.

4.2. Penetrationstest
Im nächsten Schritt führte der externe Dienstleister mit den offenen Schnittstellen der Monitoring Box einen Penetrationstest durch. Hierbei analysierte der Dienstleister detailliert die Kommunikation zwischen Gateway und Server sowie zwischen Dashboard und Server. Jegliche im Zuge des Tests offengelegten Schwachstellen wurden anschließend überarbeitet und behoben.

4.3. Schwachstellenanalyse
Abschließend fand im Rahmen des Audits eine detaillierte Schwachstellenanalyse zwischen dem Entwicklerteam von Endress+Hauser und den Prüfern des externen Dienstleisters statt. Diese Analyse stellt insbesondere die Grundlage für die abgeleiteten weiterführenden Maßnahmen dar. Während dieser Analyse wurden auch die geplanten Weiterentwicklungen der Monitoring Box diskutiert und die damit
einhergehenden neuen Angriffsszenarien identifiziert.

4.4. Kontinuierliche Weiterentwicklung
Nach Abschluss der Auditierung wurden die gewonnenen Erkenntnisse verwendet, um diese in der kontinuierlichen Weiterentwicklung der Monitoring Box fest zu verankern. Beispielsweise werden die verwendeten Softwarepakete sowohl auf dem Gateway wie auch auf dem Server regelmäßig und automatisiert mit bekannten Schwachstellenlisten verschiedener Anbieter abgeglichen, um bei Bedarf eine rechtzeitige und schnelle Reaktion zu ermöglichen.

5. Angriffsszenarien und Gegenmaßnahmen

Informationssicherheit steht für Endress+Hauser bei der Monitoring Box im Fokus. Man kann bei Informationssicherheit nach Datensicherheit und Datenintegrität unterscheiden. Auf beide wird im Folgenden genauer eingegangen

5.1. Datensicherheit
Datensicherheit besitzt ein System oder eine Übertragung dann, wenn die Daten nicht verloren gehen und unautorisierte Personen sie nicht kopieren oder mitlesen können. Die Kommunikation zwischen Gateway und Server sowie zwischen Server und Dashboard erfolgt zu jeder Zeit verschlüsselt und ist durch das rollenbasierte Berechtigungskonzept abgesichert. Ein Zwischenspeicher auf dem Gateway wirkt dem Verlust von Daten entgegen. Theoretische Angriffsszenarien zur Unterbrechung der verschlüsselten Kommunikation erfordern in der Regel den physischen Zugang zum Gateway. Eine Zutrittsbeschränkung am Einsatzort kann derartige Angriffe von vornherein unterbinden.
Als weiteres Beispiel könnten gezielte Denial-of-Service-Angriffe die Datenintegrität verletzen. Denn während der Dauer des Angriffs ist das Abrufen oder Speichern neuer Daten zumindest zeitweise nicht möglich. Eine Variante eines solchen Angriffs ist zum Beispiel ein Distributed-Denial-of-Service-Angriff. Bei diesem wird ein Netzwerk aus Rechnern verwendet, um das System mit Anfragen zu überlasten. Dies kann zum Ausfall des Servers und dadurch auch zum Ausfall der Datenübertragung vom Server zum Frontend führen. Die verwendete Serverinfrastruktur ist mit gängigen Mechanismen zum Schutz vor derartigen

Angriffen abgesichert. Weiterhin bietet auch der zugrundeliegende Autorisierungsmechanismus eine weitere Schutzebene, da Zugriffe nur für angemeldete Benutzer möglich sind und diese im Falle eines derartigen Angriffs leicht zu identifizieren sind und dann direkt gesperrt werden können.

5.2. Datenintegrität

Die Datenintegrität beschreibt die Korrektheit der Daten. Mit Blick auf das Condition Monitoring könnte eine Manipulation der Zustandsdaten eines Sensors dazu führen, dass der Betreiber einer Anlage den Ausfall eines Sensors nicht mitbekommt und es zu Schäden und Problemen im Prozess kommen kann. Um eine solche Manipulation zu vermeiden, ist es erforderlich, dass die übertragenen Daten weder manipuliert noch künstliche Daten übermittelt werden können.
Auch hier bieten die oben genannten Zugangsbeschränkungen zum Monitoring Box Gateway Schutz vor Manipulation des Gateways. Als zusätzliche Maßnahme ist auch die Kommunikation der Gateways mit einem Berechtigungskonzept ausgestattet. Es stellt sicher, dass Dritte nicht in der Lage sind, falsche Daten für andere Geräte einzuspeisen.
Wir nutzen dafür das Prinzip der Key Rotation.

5.3. Fazit

Mithilfe der zahlreichen erwähnten Maßnahmen und Schutzvorkehrungen bietet Endress+Hauser eine sichere Lösung für Condition Monitoring. Durch das extern durchgeführte Audit wurde der Schutz von unabhängiger Stelle überprüft und für die Applikation verbessert. Die Einführung
kontinuierlicher Überwachungsmechanismen für die verwendete Software und die Applikation führt dazu, dass das Sicherheitssystem der Cloud ständig geprüft, verbessert und auf dem neuesten Stand der Technik gehalten wird.
Durch das Sicherheitsrisiko Mensch ist ein Angriff von außen nie ganz auszuschließen, doch das Risiko für einen Angriff auf die Monitoring Box von Endress+Hauser wird als gering eingeschätzt und der dafür nötige Aufwand ist für potenzielle Angreifer aufgrund der getroffenen Vorkehrungen deutlich erhöht.
Durch unidirektionale Verbindung zwischen Gateway und Sensor ist ein Zugriff durch das System der Monitoring Box auf den Sensor schwer zu erreichen. Das Risiko, dass hier ein Schaden am Sensor oder Kundennetzwerk entsteht, wird als quasi nicht vorhanden eingeschätzt.

5.4. Endress+Hauser PSIRT

Das Endress+Hauser PSIRT ist Bestandteil der unternehmensweiten Cybersecurity-Politik von Endress+Hauser und dient in Bezug auf die Cybersecurity von Endress+Hauser-Lösungen Kunden, Behörden, Lieferanten, Sicherheitsforschern und anderen Anspruchsgruppen als Kontakt- und Informationsstelle. Für einen einheitlichen und koordinierten Umgang mit Cybersecurity-Schwachstellen betreibt das Endress+Hauser PSIRT ein zentrales Schwachstellen- und Incident-Management.

Headquarters

Endress+Hauser
Instruments International AG
Kaegenstraße 2
4153 Reinach
Switzerland

Tel +41 61 715 8100
Fax +41 61 715 2500
info@ii.endress.com
www.ii.endress.com

WP01272K/90/DE/01.25-00
(8031495 / EN / V1-2)

Endress+Hauser

People for Process Automation