MIT HONEYWELL-GASMESSGERÄTEN IMMER AUF DER SICHEREN SEITE

Wenn Sie mit ihrem Handy oder Laptop Geldgeschäfte tätigen, vertrauen Sie darauf, dass sicherheitsrelevante Daten nicht beeinflusst werden und das Gerät nicht gehackt werden kann. Sollten Sie solche Anforderungen nicht auch an die eingesetzte Messtechnik stellen, die letztlich die Geldmaschine ihres Unternehmens ist?

Honeywell legt als eines der führenden Technologie-Unternehmen großen Wert auf das Thema Cyber-Sicherheit und hat daher sowohl den Entwicklungs- und Pflege-Prozess seiner Produkte als auch zum Teil die Produkte selbst entsprechend zertifizieren lassen.

CYBER SECURITY BY DESIGN

Für die Entwicklung und Pflege der Produkte haben wir einen „Security Development Lifecycle Process“ eingeführt. Dieser ist zertifiziert gemäß den relevanten Anforderungen von ISASecure® Security Development Lifecycle Assurance (SDLA) 3.0.0 und IEC/ANSI/ISA-62443-4-1-2018 Secure product development lifecycle requirements.

Damit gewährleistet Honeywell, dass Sicherheitsaspekte von Anfang an in die Produktentwicklung integriert und nicht erst nachträglich berücksichtigt werden – Sicherheitsmechanismen und Kontrollen werden im Entwicklungsprozess genauso behandelt wie andere Elemente.

Darüber hinaus definiert der Prozess ebenso die durchzuführenden Maßnahmen bei der Behebung von Produktanomalien.

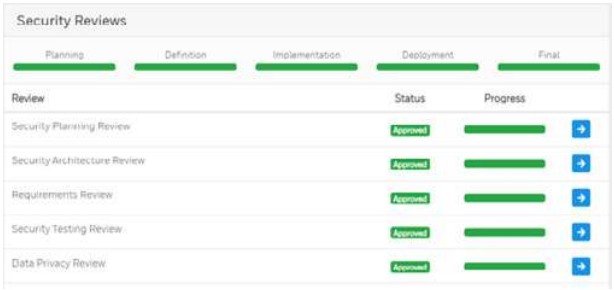
SECURITY DEVELOPMENT LIFECYCLE PROCESS

Durchgeführte Arbeiten nach Lebenszyklusphasen

Der “Security Development Lifecycle Process“ definiert im Detail, welche Arbeiten in welcher Phase des Entwicklungsprozesses durchzuführen sind:

- Konzept: Während der Festlegung des Projektumfangs werden die Sicherheitsanforderungen ermittelt und in die Anforderungen des Projekts aufgenommen.
- Entwurf: Hauptziele in dieser Phase sind die Minimierung kritischer technischer Risiken und die Entwicklung einer geeigneten Architektur.
- Konstruktion: Beim Entwurf und bei der Implementierung wurden möglicherweise Maßnahmen ermittelt, die in dieser Phase umgesetzt werden.
- Produkteinführung: Um sicherzustellen, dass der Endbenutzer die Integrität und Authentizität des Produkts überprüfen kann, werden die Produktpakete und Komponenten mit einem Zertifikat signiert.

Wird eine Produktanomalie behoben, erfolgt zu jedem Zeitpunkt eine Überprüfung, ob die Behebung die Sicherheit des Produkts beeinträchtigen könnte. Ist dies der Fall, werden die Anomalie und ihre Behebung analysiert, um festzulegen, wie etwaige Sicherheitsprobleme zu behandeln sind.



Rollen im Entwicklungsprozess
Zur Umsetzung der genannten Aufgaben sind zusätzlich zu den üblichen Rollen in einem Entwicklungsprojekt weitere sicherheitsspezifische Rollen definiert:

- Security Architect (Projektrolle): Er leitet das Team bei der Festlegung der Architekturanforderungen unter Sicherheitsaspekten an und stellt auf der Grundlage der Cyber-Sicherheit Leitlinien für den Entwurf bereit.
- Security Tester (Projektrolle): Der Security Tester besitzt ein hohes Verständnis von potenziellen Cyber-Sicherheitsangriffen und hat eine spezielle Ausbildung in der Verwendung von Sicherheitstools.
- Master Security Architect (Organisatorische Rolle): Er ist verantwortlich für die Beratung und Betreuung des Security Architects, für die endgültige Genehmigung von Bedrohungsanalysen und für die Festlegung von Lösungen für nicht behobene Sicherheitsprobleme, auf die der Security Architect stößt.
- Master Security Tester (Organisatorische Rolle): Diese Rolle ist verantwortlich für die Beratung und Betreuung von Security Testern und den verwendeten Testtools.

Ergebnisse im Entwicklungsprozess
Während des Entwicklungsprozesses werden eine Reihe von Dokumenten erstellt, die zur Überprüfung der Ergebnisse und zur abschließenden Genehmigung herangezogen werden. Dies sind unter anderem:

- Anforderungs-Repository: Sammlung von Sicherheitsanforderungen und nicht-funktionalen Anforderungen, die auf den Master Security Requirements (MSR) basieren. Die für das Projekt relevanten Sicherheitsanforderungen werden ausgewählt und in das Anforderungs-Repository des Projekts aufgenommen.
- Softwarearchitektur: Das Dokument enthält Informationen darüber, wie die Systemarchitektur aufgebaut ist, um Sicherheitsanforderungen zu erfüllen, die in der Architektur besonders behandelt werden müssen.
- Bedrohungsmodell: Analyse und Bewertung des Risikoniveaus der Anwendung mit den Angaben zu
  - Schwachstellen: Definition der potenziellen Angriffspunkte.
  - Bedrohungen: Identifikation möglicher Szenarien, wie das System missbraucht werden könnte.
  - Maßnahmen: Mechanismen zur Risikominimierung der möglichen Bedrohungen; zusätzliche Anforderungen oder Architekturelemente, die implementiert und getestet werden müssen.

Zusätzliche Dokumente wie Berichte der statischen Code-Analyse, ein Plan für die Sicherheitstests oder auch eine Checkliste, mit der die erforderlichen Sicherheitsinformationen für die Benutzerdokumentation überprüft werden, vervollständigen die geforderten Arbeitsergebnisse.

Genehmigung durch den Chief Technology Officer (CTO)
Die Einhaltung des Prozesses und die Überprüfung der Arbeitsergebnisse wird durch entsprechende Tools überwacht. Nach Durchführung und Dokumentation der einzelnen Prozessschritte wird eine abschließende Überprüfung durchgeführt und dem CTO zur Genehmigung vorgelegt.

Alle Produkte, die Software oder Firmware enthalten, müssen abschließend vom CTO im Hinblick auf die Cyber-Sicherheitsanforderungen genehmigt werden, bevor sie in die Serienproduktion gehen.

Sicherheitsanforderungen an Komponenten von Lieferanten
Die hohen Sicherheitsanforderungen an den zertifizierten Entwicklungsprozess gelten natürlich nicht nur für die bei Honeywell entwickelten Produkte, sondern in gleicher Weise für die Produktentwicklungsprozesse bei Lieferanten, die Komponenten für Honeywell entwickeln. Aufgabe des Security Architect ist es sicherzustellen, dass die ausgewählten Lieferanten die definierten Sicherheitsanforderungen erfüllen, bevor er sie mit der Entwicklung beauftragt werden.

Schwachstellen-Management (Vulnerability Management)
Cyber-Sicherheitsschwachstellen werden über interne und externe Quellen gemeldet:

- Interne Prozesse: Diese sind Sicherheitsbewertungen oder Sicherheitstests, Bedrohungsmodelle, statische Code-Analysen und Code-Reviews oder Design- oder Architektur-Reviews.
- Externe Mitteilungen wie Black Hat oder White Hat Hacker, Kunden, Sicherheitsorganisationen (z.B. NIST, BSI), etc.

Gemeldete Schwachstellen werden über entsprechende Berichte in Honeywell Fehlerverwaltungssystemen erfasst und nach Prioritäten geordnet, um die Version zu ermitteln, in der die Behebung verfügbar sein wird.

KOMPONENTEN-ZERTIFIZIERUNG NACH IEC 62443

Wie zu Beginn des Artikels erwähnt, ist ein zweiter Aspekt neben dem zertifizierten Entwicklungs- und Pflege-Prozesses die Zertifizierung des Produkts selbst. Dies wir von immer mehr Kunden und Behörden gefordert, wobei oftmals nicht im Detail spezifiziert wird, welche Zertifizierung gewünscht ist.

Auf Basis unserer Erfahrungen im Bereich der Industrieautomatisierung haben wir als Hersteller entschieden, eine Komponenten-Zertifizierung nach IEC 62443 (sichere Industrielle Automatisierungs- und Steuerungssysteme) für die Gasmessgeräte anzustreben.

Die internationale Normenreihe IEC 62443 befasst sich mit der Cyber-Sicherheit von „Industrial Automation and Control Systems" (IACS) und verfolgt dabei einen ganzheitlichen Ansatz für Betreiber, Integratoren und Hersteller.

Cyber-Sicherheit nimmt einen immer größeren Stellenwert bei der Bewertung von Gasmessgeräten ein. Wir bei Honeywell sind uns unserer Verantwortung seit langem bewusst und haben entsprechende Maßnahmen bei der Entwicklung und Pflege unserer Produkte implementiert. Eine Produkt-Zertifizierung folgt.

Mit Honeywell-Produkten bleiben Sie auf der sicheren Seite!

Bernhard Thomas
bernhard.thomas@honeywell.com