TECHDOCS

WAGO I/O System Field

Cybersecurity

765-xxx

Cybersecurity-Handbuch
4446174731 | 2 | de | 2025-07-30 13:13

WAGO GmbH & Co. KG
Hansastraße 27
D - 32423 Minden
Tel: +49 (0) 571/887 – 0
Fax: +49 (0) 571/887 – 844 169
E-Mail: ✉ **info@wago.com**
Web: **www.wago.com**

Technischer Support
Tel: +49 (0) 571/887 – 44555
Fax: +49 (0) 571/887 – 844555
E-Mail: ✉ **support@wago.com**

Es wurden alle erdenklichen Maßnahmen getroffen, um die Richtigkeit und Vollständigkeit der vorliegenden Dokumentation zu gewährleisten. Da sich trotz aller Sorgfalt Fehler nicht vollständig vermeiden lassen, sind wir für Hinweise und Anregungen jederzeit dankbar.

E-Mail: ✉ **documentation@wago.com**

Inhaltsverzeichnis

1 Gültigkeitsbereich

Das vorliegende Dokument gilt für:

Produkte von WAGO I/O System Field (Serie 765).

ⓘ Hinweis

Mitgeltende Dokumente beachten!

Die vollständige Gebrauchsanleitung für das Produkt besteht aus mehreren, mitgeltenden Dokumenten. Das Produkt darf nur gemäß Anweisungen der vollständigen Gebrauchsanleitung installiert und betrieben werden. Kenntnis aller mitgeltenden Dokumente ist Voraussetzung für die bestimmungsgemäße Verwendung. Alle Dokumente und Informationen finden Sie auf der Produktdetailseite.

Alle Dokumente und Informationen finden Sie unter:

www.wago.com/all-765

Die Produktdetailseite können Sie über folgende Möglichkeiten aufrufen:
- Scannen Sie den auf dem Produkt oder dem Beipackzettel aufgedruckten QR-Code.
- Verwenden Sie als Adresseingabe im Internetbrowser:
  www.wago.com/<Artikelnummer>.
  Beispiel: www.wago.com/765-1205/100-000 für den Artikel 765-1205/100-000.
- Besuchen Sie den Onlinekatalog auf: **www.wago.com/** und navigieren Sie zu dem Artikel.

Mitgeltendes Dokument

📖 **Produkthandbuch** des verwendeten Produktes

2 Bedrohungen

2.1 Bedrohung Cybersecurity allgemein

Eintrittswahrscheinlichkeit und Schwere von Ereignissen

Produkte für die industrielle Automatisierung können in sehr unterschiedlichen Anlagen und Anwendungen eingesetzt werden. Je nach Anwendung können die Anforderungen an die **Schutzziele** der Cybersecurity (Integrität, Verfügbarkeit oder Vertraulichkeit von Daten) unterschiedlich hoch sein. Ebenso unterschiedlich sind entsprechend auch die Anreize für potenzielle Angreifer und die Schwere eintretender Ereignisse der Cybersecurity.

Als Hersteller können wir beschreiben, unter welchen Umständen auf welche Datenbereiche, Schnittstellen oder Funktionen unseres Produktes unautorisiert zugegriffen werden kann. Angriffsziele können aus **Produktsicht** betrachtet werden. Als Hersteller können wir Anweisungen geben, wie mit den Cybersecurityfähigkeiten des Produktes die Wahrscheinlichkeit eines unautorisierten Zugriffes reduziert werden kann.

Der Betreiber muss aus **Anwendungssicht** prüfen, welcher Schaden entstehen kann, welches Sicherheitsniveau erforderlich ist und ob zusätzliche Maßnahmen zur Erhöhung der Sicherheit erforderlich sind. Ein Kriterium für die Angemessenheit des Sicherheitsniveaus ist beispielsweise, ob im konkreten Anwendungsfall personenbezogene Daten verarbeitet werden oder nicht. Die tatsächlichen Auswirkungen unautorisierter Zugriffe im jeweiligen konkreten Anwendungsfall kann nur der Betreiber beurteilen.

2.1.1 Angriffsziele aus Produktsicht

Aus Produktsicht können mindestens die folgenden physikalischen oder logischen Objekte ein Angriffsziel darstellen:

- Produktfunktion stören (Verfügbarkeit einschränken).
- Daten manipulieren (auf Auswertungen, Entscheidungen oder Systemverhalten Einfluss nehmen).
- Daten unautorisierten Personen (Dritte) zugänglich machen.
- Zugriff auf verbundene andere Systeme erhalten.

2.1.2 Angriffsvektor aus Produktsicht

Aus Produktsicht können mindestens die folgenden grundlegenden Mechanismen einen Angriffsvektor darstellen:

- Unterbrechung der Spannungsversorgung:
  Einschränkung der Verfügbarkeit (DoS) oder Vorbereitung weiterer Attacken
- Zugriff auf unverschlüsselte Schnittstellen:
  Unautorisierte Betätigung der Schnittstellen; vielfältige Angriffsziele, potenziell auch die Übertragung manipulierter Soft-/Firmware
- Zugriff auf unverschlüsselte Daten:
  Unautorisierte Verwendung, Weitergabe oder Manipulation von Daten
- Veränderung des Aufbaus, der Konfiguration oder der Programmierung des Produktes:
  Vielfältige Angriffsziele, potenziell auch die Kompromittierung weiterer verbundener Systeme

2.2 Cybersecurityspezifische Bedrohungen

Konkrete Bedrohungen können nur bei Kenntnis der jeweiligen Anlage und Anwendung beurteilt werden. Das Beurteilen von Bedrohungen, die sich aus der Bedeutung übertragener Daten ergeben, muss der Betreiber selbst durchführen. Unabhängig von der Beurteilung übertragener Daten können grundlegende Arten von Bedrohungen für den spezifischen Produkttyp benannt werden.

Grundlegende Bedrohungsarten spezifisch für den Produkttyp: WAGO I/O System Field

- Stören der Kommunikation im Netzwerk:
  Indem die Netzwerkadresse des Produktes manipuliert wird, können Adresskonflikte herbeigeführt, die Kommunikation unterbrochen oder Daten fehlgeleitet werden.
- Aneignen von Informationen über Prozesse der Anlage:
  Durch Mitschneiden der Prozesseingangs- oder Prozessausgangsdaten können Informationen zu in der Anlage ablaufenden Prozessen gewonnen werden. Diese Kenntnisse ermöglichen, weitere Schwachstellen für Angriffe der Cybersecurity zu identifizieren.
- Stören von Abläufen oder Verursachen von Schäden in der Anlage:
  Durch Manipulation von Prozesseingangsdaten kann die überlagerte Steuerung zum Erzeugen falscher Vorgabewerte für dezentrale Automatisierungsgeräte veranlasst werden. Durch Manipulation von Prozessausgangsdaten können Aktoren der Feldebene zum Ausführen falscher Vorgänge veranlasst werden.

2.3 Schwachstellenanalyse

Produkte haben aufgrund ihrer Produktfunktionen technische Grenzen. Diese technischen Grenzen können in der Cybersecurity eine Schwachstelle darstellen.

Wenn der Betreiber diese Schwachstellen durch eigene technische oder organisatorische Maßnahmen kompensiert, kann das Produkt dennoch sicher verwendet werden.

Angriffsflächen sind Produkteigenschaften, welche eine bekannte Cybersecurity-Schwachstelle darstellen, falls der Betreiber keine geeigneten Schutzmaßnahmen ergreift.

Hinweis: Der Betreiber ist dafür verantwortlich, alle dokumentierten Angriffsflächen hinsichtlich der Eintrittswahrscheinlichkeit und Schwere von Vorfällen zu bewerten und angemessene Maßnahmen zu ergreifen. Die Schwachstellenanalyse muss auf potentielle Schwachstellen ausgedehnt werden, welche sich aus der Integration in die jeweilige Anlage und Anwendung ergeben.

Die Schwachstellenanalyse unterstützt das Erreichen der Schutzziele Integrität, Verfügbarkeit oder Vertraulichkeit von Daten.

3 Angriffsflächen bei Netzwerkzugang

3.1 Angriffsflächen bei Netzwerkzugang − Überblick

Das Produkt ist für den Einsatz in einem geschützten Netzwerksegment bestimmt.

Folgende Angriffe sind in einem ungeschützten Netzwerksegment durch unautorisierten Zugriff möglich:

Daten können ausgelesen werden. Daten können manipuliert werden. Daten können an unautorisierte Personen (Dritte) weitergegeben werden.

Folgende Daten können beispielsweise betroffen sein:
- Produkt-/Gerätedaten, Prozessdaten, Konfigurationsdaten, Parametrierdaten

Konfigurationen können ausgelesen werden. Konfigurationen können manipuliert werden. Konfigurationen können an unautorisierte Personen (Dritte) weitergegeben werden.

Folgende Konfigurationen können betroffen sein:
- Produkt-/Gerätekonfigurationen, Projektkonfigurationen, Netzwerkkonfigurationen

Soft-/Firmware kann ausgelesen werden. Soft-/Firmware kann manipuliert werden. Soft-/Firmware kann an unautorisierte Personen (Dritte) weitergegeben werden.

Folgende Soft-/Firmware kann betroffen sein:
- Soft-/Firmware des Produktes, Software von Service-/Hilfsmitteln

Systeme können ausgelesen werden. Systeme können manipuliert werden. Systeme können kompromittiert werden.

Folgende Systeme können betroffen sein:
- I/O-System, weitere verbundene Systeme

3.2 Nicht-gesicherter Feldbus

Der Feldbus verbindet leitungsgebunden übergeordnete Steuerungen mit den Produkten des I/O-Systems und dient dem Datenaustausch zwischen den Komponenten.

Ein nicht-gesicherter Feldbus hat keine Cybersecurityfähigkeiten wie Authentifizierung, Integritätsschutz und Verschlüsselung.

Nicht-gesicherte Feldbusse sind beispielsweise: PROFINET, EtherCAT, EtherNet/IP

3.3 Ungeschützter integrierter Webserver

Ein integrierter Webserver dient der Konfiguration eines Produktes. Webseiten, die auf einem Webserver liegen, können über das Internet oder das Netzwerk geöffnet werden.

Ein ungeschützter integrierter Webserver hat keine Cybersecurityfähigkeiten wie Integritätsschutz und Verschlüsselung.

3.4 Engineering-/Service-Zugang

Über den Engineering-/Service-Zugang werden Konfigurationen und Parametrierungen vorgenommen.

Die Protokolle unterstützen keine Authentifizierung oder Verschlüsselung.

Für den Engineering-/Service-Zugang ist die Ausführung eines Engineering-, Konfigurations- und Parametriertools auf ein externes Engineeringgerät (z. B. PC, Laptop oder Smartphone) erforderlich.

Die Cybersecurityfähigkeit eines Engineeringgerätes ist abhängig von vielen Faktoren.

Insbesondere von:
- Dem Betriebssystem
- Den Benutzerrechten
- Der Anbindung in wechselnde Netzwerke (z. B. öffentlich zugängliche)
- Dem Anschluss mobiler Datenträger

Wenn das Engineeringgerät nicht ausreichend gesichert ist, kann über unautorisierte Benutzer und/oder Schadsoftware das Produkt ausgelesen oder manipuliert werden.

4 Angriffsflächen bei physikalischem Zugang

4.1 Angriffsflächen bei physikalischem Zugang − Überblick

Das Produkt ist für den Einsatz in einem physikalisch geschützten Zugangsbereich bestimmt.

Folgende Angriffe sind in einem physikalisch ungeschützten Zugangsbereich durch unautorisierten Zugriff möglich:

Verbindungen und damit die Erreichbarkeit des Produktes können unterbrochen oder ausgesetzt werden.

Folgende Verbindungen können betroffen sein:
- Netzwerkverbindung

Daten können ausgelesen werden. Daten können manipuliert werden. Daten können an unautorisierte Personen (Dritte) weitergegeben werden.

Folgende Daten können beispielsweise betroffen sein:
- Produkt-/Gerätedaten, Prozessdaten, Konfigurationsdaten, Parametrierdaten

Das Produkt kann auf Werkseinstellung zurückgesetzt werden. Dadurch ist ein Zugriff mit dem Standardbenutzernamen und dem Standardpasswort möglich.

Folgende Einstellungen können betroffen sein:
- Produkt-/Geräteeinstellungen

Komponenten des I/O-Systems können ausgetauscht werden. Komponenten, die manipuliert wurden, können in das System eingesetzt werden.

Folgende Komponenten können betroffen sein:
- Komponenten des I/O-Systems

Die Soft-/Firmware kann ausgetauscht werden. Soft-/Firmware, die manipuliert wurde, kann in das System übertragen werden.

Folgende Soft-/Firmware kann betroffen sein:
- Soft-/Firmware der Komponenten des I/O-Systems

4.2 Funktechnologie

Funktechnologie ermöglicht die Diagnose und Konfiguration von Geräten ohne physikalischen Anschluss.

Die Reichweite ist abhängig von der eingesetzten Funktechnologie.

4.3 Netzwerk-Schnittstelle

Die Netzwerk-Schnittstelle verbindet das Produkt physikalisch mit dem Netzwerk. Die Netzwerk-Schnittstelle ermöglicht den Zugriff auf die Prozessdaten und Produktkonfigurationen.

5 Entstehende Angriffsflächen

5.1 Nicht-überwachte Indikatoren

Das Produkt ist für den Einsatz in einer sicheren Betriebsumgebung bestimmt.

Das Produkt verfügt nicht über die Möglichkeiten, Indikatoren für die Vorbereitung oder Durchführung eines Cybersecurityangriffes zu erkennen.

Das Produkt kann bei Auftreten entsprechender Ereignisse oder Vorgänge keine ausreichenden eigenen Gegenmaßnahmen ergreifen. Fehlende Eigendiagnose gibt Angreifern die Möglichkeit, Schwachstellen durch Experimentieren zu finden und auszunutzen.

Beispiele für Indikatoren für die Vorbereitung oder Durchführung eines Cybersecurityangriffes sind:

- Veränderte – meist erhöhte – Netzwerkaktivität
- Veränderte – meist erhöhte – Auslastung der Hardware
- Häufige aufeinander folgende Änderungen der Konfigurationen

6 Härtung und Cybersecurityfähigkeiten

6.1 Defense-in-depth-Prinzip

Das Produkt ist ein Gerät mit offenen Schnittstellen und Ports und ist für den Einsatz in einem geschützten Netzwerksegment bestimmt. Für den Einsatz müssen Schutzmaßnahmen entsprechend des Einsatzbereiches vorgenommen werden.

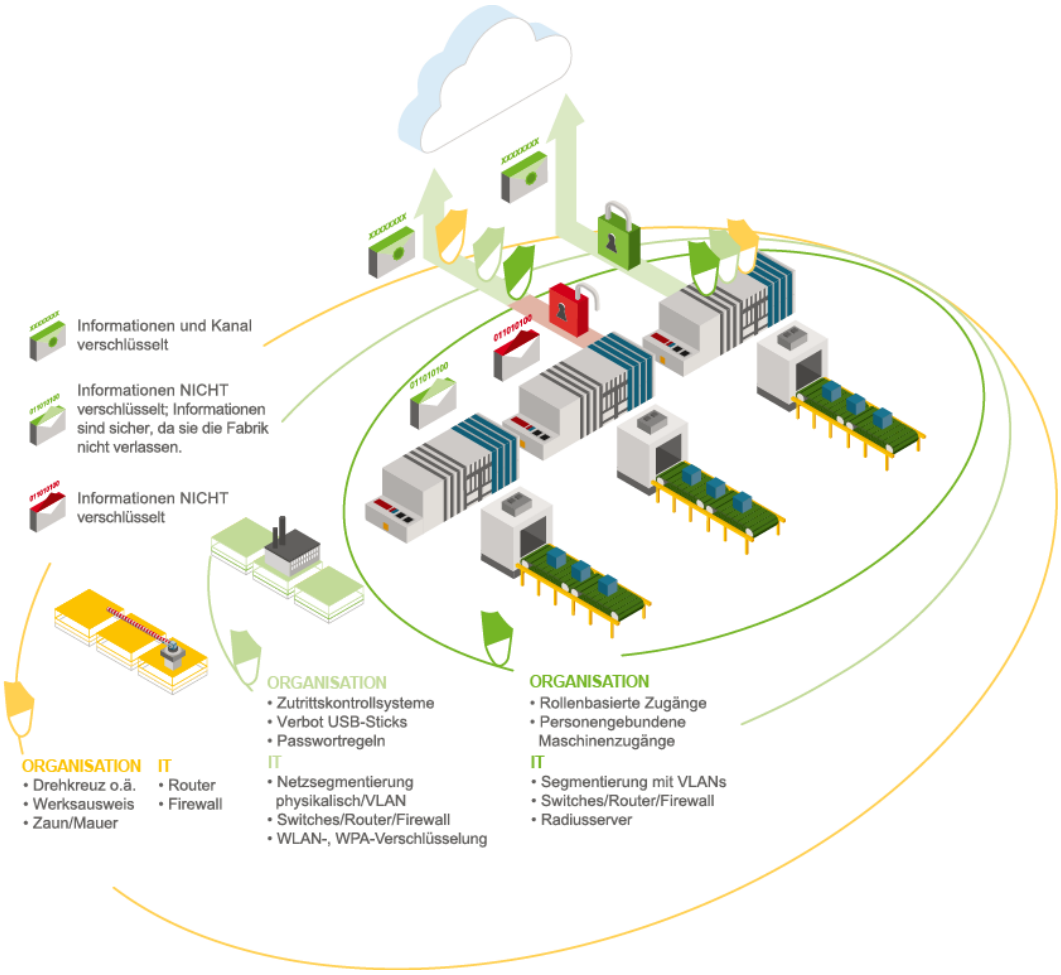

Abbildung 1: Zwiebelschalenmodell (Beispiel)

Der Betreiber einer Anlage muss organisatorische und technische Sicherheitsmaßnahmen miteinander kombinieren, um Bedrohungen der Cybersecurity erfolgreich abzuwehren.

Keine einzelne Sicherheitsmaßnahme bietet umfassenden Schutz. Beispielsweise spielt die Härte einer Tresortür (technische Sicherheitsmaßnahme) keine Rolle, während die Tür zum Einlagern oder Auslagern gerade offen steht (organisatorische Sicherheitsmaßnahme).

Die Funktion mancher Produkte erfordert es, dass innerhalb der Vertrauensgrenzen („Trust Boundaries“) oder innerhalb bestimmter Zeiträume Vorgänge ohne Schutzfunktionen („Tresortür offen“) erfolgen. Im Produkt fehlende Schutzfunktionen müssen dann durch die vom Betreiber verantwortete Einsatzumgebung realisiert werden.

Die getroffenen organisatorischen und technischen Sicherheitsmaßnahmen müssen wie die Schalen einer Zwiebel alle verwundbaren Zugänge oder Übertragungswege umhüllen und Angriffsflächen abdecken. Die getroffenen Sicherheitsmaßnahmen müssen zudem so gestaltet sein, dass bei Überwinden einer Maßnahme die anderen Maßnahmen weiterhin schützend wirken.

Als Hilfestellung für die Auslegung der Sicherheitsarchitektur enthält diese Dokumentation Angaben zu aus Produktsicht erkennbaren, erforderlichen Maßnahmen: **Härtungsmaßnahmen [▶ 12]**.

6.2 Referenzarchitektur

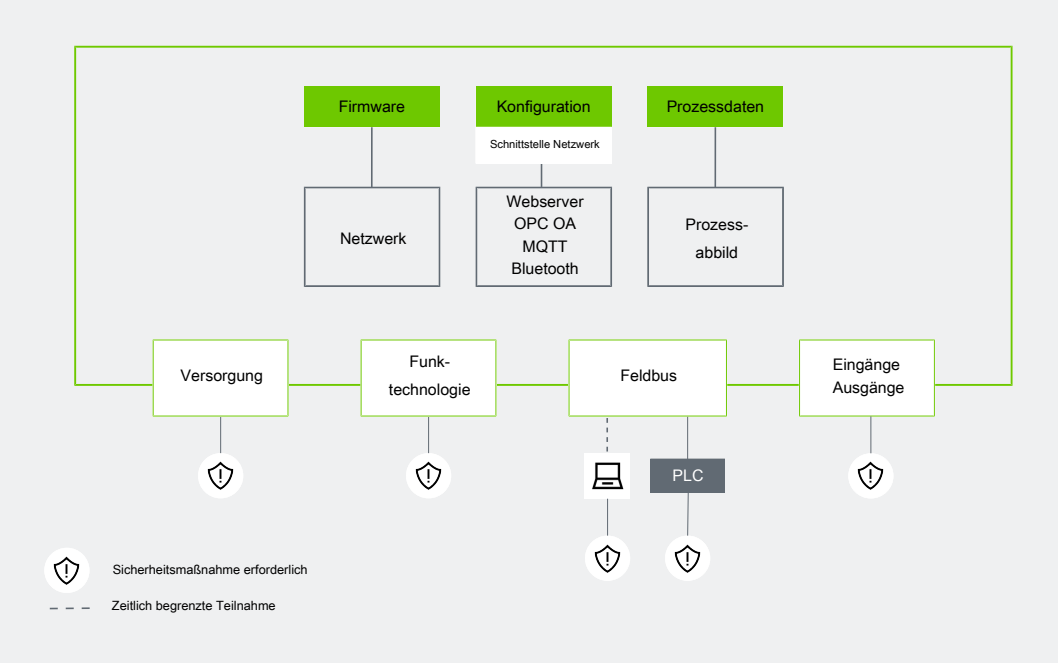

Abbildung 2: Referenzarchitektur

6.3 Härtungsmaßnahmen

Die beschriebenen Härtungsmaßnahmen stellen keine Alternativen zueinander dar. Damit ein guter Schutz gegeben ist, müssen die unterschiedlichen Härtungsmaßnahmen ergänzend zueinander umgesetzt werden.

6.3.1 Sichere Betriebsumgebung

Das Produkt darf nur in einer sicheren Betriebsumgebung betrieben werden. Eine sichere Betriebsumgebung trägt dazu bei, verschiedene Angriffe zu vermeiden. Eine sichere Betriebsumgebung erfüllt mindestens die folgenden Anforderungen:

- Physikalisch geschützter Zugang
- Geschütztes Netzwerksegment

- Protokollierte Zugänge und Zugriffe
- Überwachung auf verdächtige Ereignisse oder Vorgänge

Physikalisch geschützter Zugang

Das Produkt ist ein Gerät mit zugänglichen Anschlüssen.

Es darf nur in geeigneten elektrischen Betriebsräumen eingebaut werden, die mindestens die folgenden Anforderungen erfüllen:
- Zugangsbereich ist geschützt.
- Zugang erfolgt nur autorisiert.

Geschütztes Netzwerksegment

Das Produkt ist ein Gerät mit offenen Schnittstellen und Netzwerkports. Es darf nur in einem geschützten Netzwerksegment eingesetzt werden, das mindestens die folgenden Anforderungen erfüllt:
- Es besteht keine ungeschützte Verbindung zum Internet.
- Es besteht keine ungeschützte Verbindung zu weiteren Netzwerksegmenten.
- Zugriffe erfolgen autorisiert gemäß der Referenzarchitektur.
- Alle Netzwerkteilnehmer befinden sich in einem geschützten Netzwerksegment.

Protokollierte Zugänge und Zugriffe

Das Produkt bedarf in bestimmten Situationen einer zeitlich begrenzten Herabsetzung der Sicherheit. Eine zeitlich begrenzte Herabsetzung der Sicherheit kann beispielsweise bei Engineering-/Servicetätigkeiten oder in einem Fehlerfall notwendig sein.

Eine Protokollierung muss mindestens die folgenden Ereignisse erfassen:
- Verbindung eines Engineeringgerätes
- Zugriff auf das geschützte Netzwerksegment (z. B. Änderung der Grenze des geschützten Netzwerksegmentes, Deaktivieren der Firewall des Netzwerkes)
- Zugang in den physikalisch geschützten Bereich (z. B. Service-Personal)

Überwachung auf verdächtige Ereignisse oder Vorgänge

Eine Überwachung muss mindestens die folgenden Ereignisse und Vorgänge erfassen:
- Veränderte, insbesondere verdächtig erhöhte Netzwerkaktivität

6.3.2 Sichere Inbetriebnahme

Eine sichere Inbetriebnahme des Produktes trägt dazu bei, verschiedene Angriffe zu vermeiden. Eine sichere Inbetriebnahme erfüllt mindestens die folgenden Anforderungen:
- Geänderte Zugangsdaten
- Geschützte Netzwerkzugänge

Zugangsdaten

- Ändern Sie alle frei zugänglich und dokumentierten Zugangsdaten.

Die Zugangsdaten sind im 🕮 **Produkthandbuch** frei zugänglich und dokumentiert.

Die folgenden Einstellungen müssen mindestens erfüllt sein:
- Standardpasswörter/Default-Log-in sind geändert.
- Unbenutzte Netzwerkports sind deaktiviert.

- Die Netzwerkports benutzter Dienste sind geändert, sofern dies am Produkt selbst und auch der Gegenseite sinnvoll umsetzbar ist.
- Unbenutzte Schnittstellen sind deaktiviert.
- Unbenutzte Funktechnologie ist deaktiviert.

Netzwerkzugänge

- Schützen Sie die Netzwerkzugänge.

Die folgenden Anforderungen müssen mindestens erfüllt sein:
- Funktionen für Netzwerkschutz des Produktes werden verwendet, wenn verfügbar (z. B. MAC-Filter).
- Gesichertes Protokoll wird verwendet, wenn verfügbar (z. B. HTTPS, SFTP).
- Nur notwendige Schnittstellen sind aktiviert.
- Nur notwendige Netzwerkports sind aktiviert.
- Nur notwendige Dienste sind aktiviert.

6.3.3 Sicherer Betrieb

Ein sicherer Betrieb des Produktes trägt dazu bei, verschiedene Angriffe zu vermeiden. Ein sicherer Betrieb erfüllt mindestens die folgenden Anforderungen:
- Zeitlich begrenzte physikalische Zugänge bei Engineering-/Servicetätigkeiten oder Fehlerfall
- Zeitlich begrenzte Zugriffe und Zugänge bei Engineering-/Servicetätigkeiten oder Fehlerfall
- Logging von Securityereignissen/-vorgängen
- Handlung nach einem Securityereignis/-vorgang
- System Integritätsprüfungen nach Änderungen
- Verwendung von geprüfter und aktueller Firmware/-Update
- Verwendung von Hilfsmitteln zur Überprüfung der Cybersecurity

Zugriffe und Zugänge bei Engineering-/Servicetätigkeiten oder Fehlerfall

Engineering- oder Servicetätigkeiten erfordern oft Zugang auf Daten oder Konfiguration des Produkts. Daher muss der Betreiber sicherstellen, dass die verwendeten Drittgeräte sowie die zum Produkt hergestellte Verbindung sicher sind.

- Gewähren Sie Zugriffe und Zugänge nur zeitlich begrenzt.

Mindestens die folgenden Zugriffe/Zugänge müssen zeitlich begrenzt werden:
- Zugriff auf Kommunikationssoftware
- Zugriff auf Schnittstellen
- Zugriff mit erhöhten Rechten

Logging Securityereignisse

- Loggen Sie Securityereignisse.

Die folgenden Anforderungen an das Logging von Securityereignissen müssen mindestens erfüllt sein:
- Logging-Funktion des Produktes ist eingerichtet.
- Logging-Maßnahmen für Securityereignisse, die das Produkt nicht loggt, sind eingerichtet.
- Logging-Maßnahmen für das Netzwerk sind eingerichtet.

WAGO empfiehlt die Verwendung von „System Logging Protocol“ (Syslog).

Nach einem Securityereignis

- Handeln Sie nach einem Securityereignis.

Die folgenden Handlungen nach einem Securityereignis müssen mindestens erfüllt werden:
- Ist- und Sollkonfigurationsdaten vergleichen.

Systemintegritätsprüfungen

- Prüfen Sie nach Änderungen die Integrität Ihres Systems.

Die folgenden Prüfungen müssen nach Änderungen der Konfigurationen mindestens durchgeführt werden:
- Prüfung der Firewall

Geprüfte und aktuelle Firmware(-Updates)

- Verwenden Sie nur geprüfte und aktuelle Firmware(-Updates).

Die folgenden Anforderungen sind Merkmale einer geprüften und aktuellen Firmware/-Updates:
- Prüfsumme wurde erfolgreich verifiziert (Integritätsprüfung).

WAGO empfiehlt die Verwendung von aktueller Firmware.

Die aktuelle Version einer Firmware entspricht dem aktuellen Stand der Technik und der Sicherheit. Vorherige Versionen einer Firmware können Schwachstellen in Technik und Sicherheit aufweisen.

Geprüfte und aktuelle WAGO Firmware(-Updates) und Informationen zur Installation erhalten Sie unter:
- **https://downloadcenter.wago.com**

Weitere Informationen erhalten Sie beim:
- **Technischen Support**

Hilfsmittel

- Nutzen Sie weitere Hilfsmittel zur Überprüfung der Security.

Die folgenden Hilfsmittel können zur Überprüfung der Cybersecurity Ihres Systems helfen:
- System Logging Protocol (Syslog)

6.3.4 Sichere Außerbetriebnahme

Eine sichere Außerbetriebnahme des Produktes trägt dazu bei, verschiedene Angriffe zu vermeiden. Eine sichere Außerbetriebnahme erfüllt mindestens die folgenden Anforderungen:
- Gelöschte Daten im Produkt
- Gelöschte Daten des Produktes in der Umgebung

Daten im Produkt

- Löschen Sie alle im Produkt gespeicherten Daten.

Die folgenden Anforderungen müssen mindestens erfüllt sein:
- Produkt ist auf Werkseinstellungen zurückgesetzt.
- Daten, die nicht gelöscht werden können, sind überschrieben (z. B. mit „0“).
- Bei Verdacht auf nicht gelöschte, sensible Daten: Verschrottung durch einen für Cybersecurity qualifizierten Entsorgungsdienstleister veranlassen.

Daten des Produktes in der Umgebung

- Löschen Sie alle vom Produkt gespeicherten Daten in der Umgebung.

Die folgenden Anforderungen müssen mindestens erfüllt sein:
- Konfigurationen des Produktes in der Projektierumgebung sind gelöscht.

6.4 Cybersecurityfähigkeiten

Die vorliegenden Cybersecurityfähigkeiten beschreiben den möglichen Umfang der Cybersecurityfähigkeiten eines Produkttyps. Nicht alle beschriebenen Cybersecurityfähigkeiten gelten für jedes Produkt des Produkttyps. Nicht alle Cybersecurityfähigkeiten eines Produktes des Produkttyps sind in dieser exemplarischen Beschreibung enthalten.

Welche zutreffenden Cybersecurityfähigkeiten ein Produkt hat, finden Sie im: 🕮 **Produkthandbuch**.

Syslog–Protokoll

Das Netzwerkprotokoll Syslog ermöglicht die Übertragung von ereignisgesteuerten Log-Nachrichten in einem IP-basierten Netzwerk. Die Übertragung findet vom Client zum Server über „Transmission Control Protocol“ (TCP) oder „User Datagram Protocol“ (UDP) statt.

Zugriffskontrollen

Eine Zugriffskontrolle steuert und überwacht den Zugriff auf Schnittstellen oder Daten. Nur autorisierte Personen erhalten Zugriff auf bestimmte Schnittstellen oder Daten. Eine Zugriffskontrolle kann über verschiedene Möglichkeiten erfolgen. Beispiele sind:
- Zugriffskontrolle auf das Netzwerk (z. B. MAC-Adressfilter)

Benutzerverwaltung

Der Webserver verfügt über eine rollenbasierte Benutzerverwaltung. Die Benutzverwaltung kann über verschiedene Möglichkeiten erfolgen:
- Vordefinierte Benutzer sind eingerichtet, nur Passwortänderung ist möglich.
- Benutzer können selbst eingerichtet werden.

Anzeige aktiver Ports

Das Anzeigen aktiver Ports ermöglicht die Kontrolle über die Schnittstellen und unterstützt die Erkennung eines unautorisierten Zugriffes. Das Anzeigen aktiver Ports kann erfolgen über:
- Optische Anzeigeelemente am Produkt (LED)

Update-Fähigkeit

Ein Update der Soft-/Firmware kann durch eine Erweiterung der Produkteigenschaft, Verbesserung der Soft-/Firmware oder zur Behebung einer Sicherheitslücke erfolgen.

- Das Produkt hat ab Werk keine automatische Update-Funktion.

6.5 Cybersecurityservice

Aktuelle Sicherheitslücken

- Informieren Sie sich über aktuelle Sicherheitslücken.

Die folgenden Kontaktstellen können zur Information über aktuelle Sicherheitslücken genutzt werden:

- Informationen über bekannte und aktuelle Sicherheitslücken können Sie online einsehen: „Common Vulnerabilities and Exposures (CVE)“, **https://cert.vde.com/de/advisories/vendor/wago/**.
- Informationen zu Schwachstellen von WAGO Produkten erhalten Sie beim WAGO Product Security Incident Response Team **PSIRT**.

Dauer des Service für Cybersecurity

- Informieren Sie sich über die Dauer des Service für Cybersecurity für Ihr Produkt.

Informationen zur Dauer des Service für Cybersecurity finden Sie auf der Produktdetailseite unter: **www.wago.com/**<Artikelnummer>.

Abbildungsverzeichnis

Tabellenverzeichnis

Glossar

Angriffsfläche

Spezifische Schnittstelle eines Produkts, über die Cybersecurity-Angriffe einer grundlegenden Art ausgeführt werden können; Beispiel: Cybersecurity-Angriffe, die als Angriffsvektor physikalischen Zugriff nutzen, können einen Adresswahlschalter nutzen, um das Netzwerk zu stören.

Angriffsvektor

Grundlegender Mechanismus, über den Cybersecurity-Angriffe ausgetragen werden können; Beispiel: physikalischer Zugriff oder Kenntnis von Log-in-Daten

Angriffsziel

Physikalisches oder logisches Objekt, das für Angreifer einen Wert hat; Beispiel: ein Speicherbereich mit aus Betreibersicht schützenswerten Daten

Bedrohung

Möglichkeit der Beeinträchtigung einer Person oder Sache durch Vorfälle der Cybersecurity

Schwachstelle

Eine Angriffsfläche, die nicht oder unzureichend geschützt ist und damit eine Schwachstelle darstellt

Stichwortverzeichnis

WAGO GmbH & Co. KG
Postfach 2880 · D - 32385 Minden
Hansastraße 27 · D - 32423 Minden
✉ **info@wago.com**
www.wago.com

Zentrale	+49 (0) 571/887 – 0
Vertrieb	+49 (0) 571/887 – 44 222
Auftragsservice	+49 (0) 571/887 – 44 333
Fax	+49 (0) 571/887 – 844 169