Richtlinie zur Meldung von IT-Sicherheitslücken (Coordinated Vulnerability Disclosure Policy)

Dokument: CVD-Richtlinie / Single Point of Contact (SPoC)
Version: 1.0
Gültig ab: 11.09.2026
Verantwortlich: BHS Control Systems GmbH
Freigabe: Geschäftsführung

Inhalt

1. Zweck

Die BHS Control Systems GmbH entwickelt und liefert kundenspezifische Automatisierungs- und Softwarelösungen für industrielle Anlagen, insbesondere:

- SPS-Software
- WinCC Unified Anwendungen
- WinCC OA Anwendungen
- SCADA-Systeme
- Prozessleitsysteme
- Fernwartungs- und Kommunikationslösungen
- Individuelle Softwarekomponenten für industrielle Automatisierungssysteme

Diese Richtlinie beschreibt den Prozess zur verantwortungsvollen Meldung von Sicherheitslücken in von **BHS Control Systems** entwickelten Produkten und Lösungen.

Ziel ist es, Schwachstellen schnell zu identifizieren, zu bewerten und angemessen zu beheben, bevor sie zu einer Gefährdung von Kundenanlagen oder Produktionsprozessen führen.

2. Geltungsbereich

Diese Richtlinie gilt für:

- von BHS Control Systems entwickelte SPS-Programme
- WinCC Unified Projekte
- WinCC OA Projekte
- Kommunikationsschnittstellen
- Datenbankanbindungen
- Remote-Service-Lösungen
- sonstige digitale Komponenten, die von BHS Control Systems entwickelt oder wesentlich verändert wurden

Nicht erfasst sind Produkte Dritter, soweit diese **nicht** durch BHS Control Systems entwickelt oder verändert wurden.

3. Single Point of Contact (SPoC)

Sicherheitsmeldungen können an folgende zentrale Kontaktstelle übermittelt werden:

E-Mail: security@bhs-control-systems.com

Security.txt:
https://www.bhs-control-systems.com/.well-known/security.txt

Die Kontaktstelle wird während der üblichen Geschäftszeiten überwacht.

4. Erwünschte Meldungen

BHS Control Systems begrüßt Hinweise auf:

- Authentifizierungsfehler
- Rechteeskalationen
- Schwachstellen in Benutzer- und Rollenverwaltung
- Unsichere Kommunikationsschnittstellen
- Schwachstellen bei Fernzugriffen
- Unsichere Datenspeicherung
- Offenlegung vertraulicher Informationen
- Manipulationsmöglichkeiten von Prozessdaten
- Umgehung von Sicherheitsfunktionen
- Denial-of-Service-Schwachstellen
- Schwachstellen mit Auswirkungen auf Verfügbarkeit, Integrität oder Vertraulichkeit

5. Inhalt einer Meldung

Meldungen sollten möglichst folgende Informationen enthalten:

- Beschreibung der Schwachstelle
- Betroffene Software oder Anlage
- Versionsstand
- Zeitpunkt der Feststellung
- Schritte zur Reproduktion
- Mögliche Auswirkungen
- Screenshots, Logdateien oder sonstige Nachweise
- Kontaktdaten des Meldenden

6. Umgang mit Meldungen

Nach Eingang einer Meldung erfolgt:

6.1 Eingangsbestätigung

Innerhalb des nächsten Arbeitstages

6.2 Erste Bewertung

Die Meldung wird hinsichtlich folgender Kriterien bewertet:

- Plausibilität
- Betroffenheit
- Kritikalität
- Ausnutzbarkeit
- Auswirkungen auf Kundenanlagen

Zur Bewertung kann die Methodik des

CVSS v4.0

verwendet werden.

6.3 Bearbeitung

Je nach Kritikalität werden Maßnahmen eingeleitet:

Kritikalität	**Zielzeit für Bewertung**
Kritisch	24 Stunden
Hoch	5 Arbeitstage
Mittel	10 Arbeitstage
Niedrig	Nach Aufwand

7. Vertraulichkeit

BHS Control Systems behandelt eingehende Meldungen vertraulich.

Informationen werden ausschließlich an Personen weitergegeben, die unmittelbar an der Analyse und Behebung beteiligt sind.

Personenbezogene Daten werden gemäß den geltenden Datenschutzvorschriften verarbeitet.

8. Verantwortungsvolle Offenlegung

Meldende werden gebeten:

- keine Produktionsanlagen zu beeinträchtigen
- keine Daten unbefugt zu verändern
- keine personenbezogenen Daten auszulesen
- keine Verfügbarkeit von Systemen zu beeinträchtigen
- Schwachstellen nicht öffentlich zu machen, bevor eine Bewertung erfolgt ist

BHS Control Systems strebt eine koordinierte Offenlegung gemeinsam mit dem Meldenden an.

9. Cyber Resilience Act (CRA)

Diese Richtlinie unterstützt die Anforderungen des europäischen

Cyber Resilience Act

zur koordinierten Offenlegung von Schwachstellen (Coordinated Vulnerability Disclosure).

BHS Control Systems unterhält hierzu einen Single Point of Contact zur Annahme und Bearbeitung von Sicherheitsmeldungen.

10. Dokumentation

Alle eingehenden Meldungen werden dokumentiert.

Erfasst werden insbesondere:

- Ticketnummer
- Eingangsdatum
- Betroffene Lösung
- Risikoeinstufung
- Bearbeitungsstatus
- Umgesetzte Maßnahmen
- Abschlussdatum

Die Dokumentation wird mindestens für die Dauer der gesetzlichen Aufbewahrungsfristen aufbewahrt.

11. Kontakt

BHS Control Systems GmbH & Co. KG
Security Response Team (SRT)
E-Mail: security@bhs-control-systems.com