Leitfaden zum Umgang mit Sicherheitslücken

Vulnerability Handling Guideline

Der sichere und verantwortungsvolle Umgang mit Sicherheitslücken ist ein zentraler Bestandteil unserer Produkt- und Informationssicherheit. Dieser Leitfaden beschreibt die grundlegenden Prinzipien, Verantwortlichkeiten und Abläufe, die sicherstellen, dass Schwachstellen in unseren Produkten, Systemen sowie OT- und IT-Umgebungen schnell, strukturiert und gesetzeskonform behandelt werden.
Er dient allen Mitarbeitenden als Orientierung und bildet die Basis für unsere PSIRT-Prozesse, die koordinierte Offenlegung (CVD) sowie die Erfüllung der Meldepflichten nach dem Cyber Resilience Act (CRA).

1.Grundprinzipien

Unser Umgang mit Sicherheitslücken folgt fünf zentralen Leitlinien:
Schnelligkeit Sicherheitslücken werden unverzüglich bewertet und bearbeitet, um Risiken frühzeitig zu minimieren.
Transparenz Alle Schritte – von der Meldung bis zur Behebung – werden nachvollziehbar dokumentiert.
Sicherheit Alle Maßnahmen dienen dem Schutz unserer Systeme, Produkte und Kunden.
Verantwortung Jede Person, die eine Schwachstelle erkennt, meldet diese sofort über die vorgesehenen Kanäle.
Compliance Wir erfüllen alle gesetzlichen Vorgaben, insbesondere CRA und relevante ISO-Normen.

Meldewege

Sicherheitslücken dürfen ausschließlich über definierte Kanäle gemeldet werden:

PSIRT-E-Mail: psirt@trsystems.de
Internes Ticketsystem: OTOBO (Ticket-ID)
Direkte Meldung an PSIRT-Ansprechpartner

Externe Sicherheitsforscher nutzen die CVD-Kontaktadresse und den veröffentlichten PGP-Key (Pretty Good Privacy) zur verschlüsselten Kommunikation.

Nach der Meldung. Beginnt die Klassifizierung. Jede Meldung wird als eine der folgenden Kategorien eingestuft:

- **Schwachstelle** (Vulnerability)
- **Sicherheitsvorfall** (Incident)
- **Änderungswunsch** (Change Request)

Schwachstellen und Vorfälle werden durch das PSIRT priorisiert und bewertet. Die Bewertung erfolgt anhand folgender Kriterien

- Ausnutzbarkeit (CVSS)
- Schweregrad
- Betroffene Produkte
- Hinweise auf aktive Ausnutzung
- CRA-Relevanz (Meldepflicht)

Die Erstbewertung erfolgt innerhalb von 24 Stunden nach Eingang der Meldung. Außerdem wird für jede bestätigte Schwachstelle ein Maßnahmeplan erstellt.
Dieser umfasst:

- Sofortmaßnahmen
- technische Behebung
- Validierung
- Dokumentationsanpassungen
- Kommunikationsmaßnahmen

Der Maßnahmenplan stellt sicher, dass die Schwachstelle strukturiert, vollständig und nachvollziehbar behoben wird. Die Kommunikation erfolgt abhängig von Schweregrad und Ausnutzung:

- Interne Information relevanter Stellen
- Kundeninformation (z. B. PCN)
- Veröffentlichung eines Security Advisories
- Meldung an ENISA oder BSI, wenn die Schwachstelle aktiv ausgenutzt wird
- Koordination mit externen Sicherheitsforschern (CVD)

Transparente Kommunikation ist ein wesentlicher Bestandteil des sicheren Schwachstellenmanagements.
Nach Umsetzung aller Maßnahmen erfolgt die:

- Abschlussbewertung durch das PSIRT
- Vollständige Dokumentation im Ticketsystem
- Durchführung von Lessons Learned und die
- Ableitung von Prozessverbesserungen

Damit wird sichergestellt, dass wir nicht nur Schwachstellen beheben, sondern auch unsere Prozesse kontinuierlich verbessern.

Die Verantwortlichkeiten , was macht wer ?

PSIRT: Bewertung, Koordination, Freigabe und Kommunikation
Die Fachabteilungen: Analyse, technische Umsetzung sowie Tests
Stakeholder: Meldung von Schwachstellen
Management: Bereitstellung von Ressourcen und Freigaben

Unser Vorgehen orientiert sich dabei an folgenden Standards und gesetzlichen Anforderungen:

- Cyber Resilience Act (CRA)
- ISO/IEC 30111 – Vulnerability Handling
- ISO/IEC 29147 – Vulnerability Disclosure
- ISO/IEC 27001 – Informationssicherheit
- Interne PSIRT-Prozesse und Richtlinien

Dieser Leitfaden bietet eine klare Orientierung darüber, wie Sicherheitslücken in unserem Unternehmen erkannt, bewertet, behandelt und kommuniziert werden.
Er schafft Transparenz, stärkt die Sicherheit unserer Produkte und stellt sicher, dass wir alle gesetzlichen Anforderungen erfüllen.