

Politik zur koordinierten Offenlegung von Schwachstellen

Coordinated Vulnerability Disclosure Policy

Dokument	POL-CRA-02 – CVD-Policy
Version / Stand	1.0 · 08.09.2026
Rechtsgrundlage	Verordnung (EU) 2024/2847 (Cyber Resilience Act), Anhang I Teil II Nr. 4, 5 und 6, Anhang II Nr. 2, Art. 13 Abs. 17
Orientierung	ISO/IEC 29147 (Offenlegung von Schwachstellen), ISO/IEC 30111 (Bearbeitung von Schwachstellen)
Meldeadresse	product_security@hargassner.at
Veröffentlichung	https://www.hargassner.com/agb
Verantwortlich	CISO, HARGASSNER Ges mbH
Freigabe	Christoph Buchbauer (CFO, 23.09.2026)

1 Unser Standpunkt

Auch sorgfältig entwickelte Produkte enthalten Fehler. Wir halten es für richtig, dass Menschen, die eine Sicherheitslücke in einem unserer Produkte finden, einen klaren und verlässlichen Weg haben, uns davon zu erzählen – ohne rechtliches Risiko und ohne ins Leere zu laufen.

Diese Politik beschreibt diesen Weg. Sie richtet sich an Sicherheitsforscherinnen und -forscher, an Kunden und Fachpartner, an Lieferanten und an alle, denen an unseren Anlagen etwas auffällt. Sie ist zugleich unsere Politik zur koordinierten Offenlegung von Schwachstellen im Sinne von Anhang I Teil II Nr. 5 des Cyber Resilience Act.

**HARGASSNER GES MBH**

Anton Hargassner Str. 1
A-4952 Weng
+43 7723 5274-0
office@hargassner.at
hargassner.com

2 Geltungsbereich

2.1 Erfasste Produkte und Dienste

Diese Politik gilt für alle Produkte mit digitalen Elementen und alle zugehörigen Dienste, die HARGASSNER unter eigenem Namen oder eigener Marke bereitstellt:

Bereich	Umfasst insbesondere
Kesselsteuerungen	BCE31, BCE53, Touch-Steuerungen und die zugehörige Steuerungssoftware
Linux-Light-Steuerungen	Smart-HV, Smart-PK, Smart-Duo
Regelungskomponenten	Heizkreisregler HKR und HKM, Fernbedienungen, Zubehörsteuerungen
Konnektivität und Cloud	Serviceportal, Webportal, Hargassner App, Fernwartung, Datenerfassung (DAQ)
Werkzeuge im Feld	Service-, Diagnose-, Update- und Parametrierwerkzeuge, Lizenz- und Dongle-Verwaltung
Web-Auftritte	Von HARGASSNER betriebene Domains und die darüber erreichbaren Anwendungen

Erfasst sind ausdrücklich auch ältere Produkte, die bereits im Feld stehen – nicht nur aktuelle Baureihen.

2.2 Nicht erfasst

- Fremde Produkte, die lediglich an eine Hargassner-Anlage angeschlossen sind (Wechselrichter, Fremdregelungen, Gebäudeleittechnik, Router und Netzwerktechnik der Betreiber).
- Systeme und Netzwerke unserer Fachpartner, Installateure und Kunden.
- Angriffe auf Personen: Social Engineering, Phishing gegen unsere Mitarbeiter, physischer Zutritt zu unseren Standorten.
- Denial-of-Service-Tests, Lasttests und alles, was den Betrieb einer realen Heizanlage stören kann.
- Reine Konfigurationsempfehlungen ohne konkrete Ausnutzbarkeit (etwa fehlende HTTP-Header, unterstützte TLS-Ciphersuiten, Ergebnisse automatisierter Scanner ohne belegte Auswirkung).
- Funktionsstörungen ohne Sicherheitsbezug. Diese richten Sie bitte an den Kundendienst.

**HARGASSNER GES MBH**

Anton Hargassner Str. 1
A-4952 Weng
+43 7723 5274-0
office@hargassner.at
hargassner.com

3 So melden Sie eine Schwachstelle

3.1 Kontakt

E-Mail	product_security@hargassner.at
Telefon	+43 7723 5274-0 (Zentrale, Montag bis Freitag) – bitten Sie um das CRA-Team
Post	HARGASSNER Ges mbH, Anton Hargassner Str. 1, A-4952 Weng, Österreich, z. Hd. GF / CRA – vertraulich

Sie können frei wählen, auf welchem Weg Sie uns erreichen; wir beschränken die Meldung nicht auf ein Formular oder ein automatisiertes Werkzeug. Vertrauliche Inhalte verschlüsseln Sie bitte mit unserem PGP-Schlüssel.

3.2 Was wir für eine schnelle Bearbeitung brauchen

- Betroffenes Produkt, Baureihe und – wenn bekannt – Software- oder Firmwarestand
- Beschreibung der Schwachstelle und ihrer möglichen Auswirkung
- Nachvollziehbare Schritte zur Reproduktion, gerne mit Bildschirmfotos, Logauszügen oder einem Proof of Concept
- Wie und wann Sie die Schwachstelle gefunden haben
- Ob die Schwachstelle Ihres Wissens bereits ausgenutzt wird oder öffentlich bekannt ist
- Ihre Kontaktdaten und ob Sie namentlich genannt werden möchten
- Ob und wann Sie selbst zu veröffentlichen beabsichtigen

Auch eine unvollständige Meldung ist uns willkommen – wir fragen dann nach. Wir nehmen Meldungen auf Deutsch und Englisch entgegen.

**HARGASSNER GES MBH**

Anton Hargassner Str. 1
A-4952 Weng
+43 7723 5274-0
office@hargassner.at
hargassner.com

4 Was Sie von uns erwarten können

Schritt	Frist	Was passiert
Eingangsbestätigung	3 Werktage	Sie erhalten eine Bestätigung mit einer Vorgangsnummer, unter der Sie jederzeit nachfragen können.
Erste inhaltliche Rückmeldung	10 Werktage	Wir sagen Ihnen, ob wir die Schwachstelle nachvollziehen konnten, wie wir sie einstufen und wie es weitergeht.
Statusmeldung	alle 14 Tage	Solange der Fall offen ist, hören Sie regelmäßig von uns – auch dann, wenn es nichts Neues gibt.
Behebung	nach Schweregrad	Kritisch: Sicherheitsupdate binnen 7 Tagen. Hoch: binnen 30 Tagen. Mittel: mit dem nächsten Release, spätestens 90 Tage.
Veröffentlichung	siehe Abschnitt 6	Wir informieren Sie vor der Veröffentlichung und stimmen den Zeitpunkt mit Ihnen ab.

Diese Fristen sind unsere Selbstverpflichtung. Sollten wir sie einmal nicht halten können, sagen wir Ihnen das aktiv und nennen einen neuen Termin – wir lassen Sie nicht ohne Antwort.

5 Regeln für gutgläubige Sicherheitsforschung

5.1 Unsere Zusage an Sie

Wenn Sie sich an die Regeln in Abschnitt 5.2 halten, gilt Ihre Untersuchung für uns als autorisiert und gutgläubig. In diesem Fall:

- leiten wir keine zivil- oder strafrechtlichen Schritte gegen Sie ein und stellen keinen Strafantrag,
- unterstützen wir Sie, falls ein Dritter aufgrund Ihrer Untersuchung an unseren Produkten gegen Sie vorgeht, mit einer Bestätigung, dass die Untersuchung im Rahmen dieser Politik erfolgte,
- behandeln wir Ihre Meldung und Ihre Person vertraulich und geben Ihren Namen nur mit Ihrer Zustimmung weiter.

**HARGASSNER GES MBH**

Anton Hargassner Str. 1
A-4952 Weng
+43 7723 5274-0
office@hargassner.at
hargassner.com

5.2 Was wir von Ihnen erwarten

- Sie testen ausschließlich an Anlagen und Konten, die Ihnen gehören oder für die Ihnen der Betreiber ausdrücklich eine Erlaubnis erteilt hat.
- Sie greifen nicht auf Daten Dritter zu und verändern oder löschen keine fremden Daten. Stoßen Sie versehentlich auf personenbezogene Daten, brechen Sie ab, löschen Sie das Material und teilen Sie uns das mit.
- Sie stören den Betrieb nicht: keine Denial-of-Service-Tests, keine Lasttests, kein Eingriff in eine laufende Feuerung oder Sicherheitskette.
- Sie beschränken sich auf das Maß an Nachweis, das zum Beleg der Schwachstelle nötig ist, und weiten den Zugriff nicht weiter aus als erforderlich.
- Sie halten die Schwachstelle bis zur abgestimmten Veröffentlichung vertraulich und geben sie nicht an Dritte weiter, auch nicht an Broker.
- Sie melden uns die Schwachstelle unverzüglich und vollständig.
- Sie halten geltendes Recht ein.

5.3 Grenzen dieser Zusage

Unsere Zusage bindet nur uns. Sie ersetzt keine Erlaubnis Dritter – insbesondere nicht die des Betreibers einer fremden Anlage – und schließt Ansprüche Dritter oder Ermittlungen von Behörden nicht aus. Erpressung, die Forderung einer Zahlung für die Nichtveröffentlichung sowie die Weitergabe oder der Verkauf der Schwachstelle an Dritte sind vom Schutz dieser Politik ausdrücklich nicht erfasst.

6 Koordinierte Offenlegung**6.1 Regelfrist**

Wir streben an, eine gemeldete Schwachstelle innerhalb von 90 Kalendertagen ab Eingang Ihrer Meldung zu beheben und anschließend gemeinsam mit Ihnen zu veröffentlichen. Bis dahin bitten wir Sie um Vertraulichkeit.

6.2 Verlängerung

Manche Schwachstellen lassen sich nicht in 90 Tagen schließen – etwa wenn ein Update auf Geräten ohne Netzanbindung nur über einen Kundendienstesatz ausgerollt werden kann oder wenn ein Zulieferer erst eine Komponente korrigieren muss. In solchen Fällen bitten wir Sie rechtzeitig, begründet und mit konkretem Zeitplan um eine Verlängerung. Die Entscheidung liegt bei Ihnen.

**HARGASSNER GES MBH**

Anton Hargassner Str. 1
A-4952 Weng
+43 7723 5274-0
office@hargassner.at
hargassner.com

6.3 Vorzeitige Veröffentlichung

Wird die Schwachstelle nachweislich angegriffen oder anderweitig öffentlich, veröffentlichen wir früher – notfalls vor der Verfügbarkeit eines vollständigen Updates, dann mit einer Anleitung zur Risikominderung. Wir informieren Sie darüber.

6.4 Was wir veröffentlichen

Wir veröffentlichen unter <https://www.web.hargassner.at> ein Security Advisory. Es enthält betroffene Produkte und Versionsstände, eine Beschreibung der Schwachstelle und ihrer Auswirkung, die CVSS-Bewertung, die Korrekturmaßnahme mit Bezugsweg sowie – sofern Sie zustimmen – Ihre Nennung. Wo es sinnvoll ist, beantragen wir eine CVE-Kennung. Angriffsdetails, die eine Ausnutzung erleichtern würden, halten wir zurück, bis das Update im Feld angekommen ist.

Diese Veröffentlichung erfüllt zugleich unsere Pflicht aus Anhang I Teil II Nr. 4 CRA, Informationen über behobene Schwachstellen bereitzustellen.

7 Schwachstellen in Komponenten Dritter

Viele unserer Produkte enthalten Software Dritter. Betrifft Ihre Meldung eine solche Komponente, gehen wir so vor:

- Wir prüfen anhand unserer Software-Stückliste (SBOM), welche unserer Produkte die Komponente einsetzen.
- Wir informieren den Hersteller oder das Projekt, das die Komponente pflegt, und stellen ihm die Erkenntnisse zur Verfügung.
- Wir stimmen den Zeitpunkt der Veröffentlichung mit dem Upstream und mit Ihnen ab.
- Bis eine Korrektur vorliegt, prüfen wir eigene Übergangsmaßnahmen für unsere Produkte.

Umgekehrt bitten wir unsere Lieferanten, uns Schwachstellen in gelieferten Komponenten unverzüglich an product_security@hargassner.at zu melden.

**HARGASSNER GES MBH**

Anton Hargassner Str. 1
A-4952 Weng
+43 7723 5274-0
office@hargassner.at
hargassner.com

8 Gesetzliche Meldepflichten

Nach Art. 14 des Cyber Resilience Act sind wir verpflichtet, eine aktiv ausgenutzte Schwachstelle und jeden schwerwiegenden Sicherheitsvorfall innerhalb von 24 Stunden nach Kenntnis an das österreichische CSIRT (CERT.at) und die ENISA zu melden, gefolgt von einer ausführlichen Meldung nach 72 Stunden und einem Abschlussbericht.

Das kann bedeuten, dass wir Ihre Meldung an eine Behörde weitergeben müssen, bevor die mit Ihnen abgestimmte Offenlegungsfrist abgelaufen ist. Wir geben dabei nur die Angaben weiter, die für die Meldung erforderlich sind, und nennen Sie nicht namentlich, sofern Sie dem nicht zugestimmt haben. Wir informieren Sie, wenn wir eine solche Meldung abgesetzt haben.

9 Anerkennung

Wir nennen Sie auf Wunsch im Security Advisory und in unserer Danksagungsliste unter <https://www.web.hargassner.at> – mit Namen, Handle oder Organisation, ganz wie Sie es möchten. Sie können auch anonym bleiben.

Kein Bug-Bounty-Programm

HARGASSNER zahlt derzeit keine Prämien für gemeldete Schwachstellen. Eine Meldung begründet keinen Anspruch auf Vergütung. Wir sagen das offen, damit niemand mit einer anderen Erwartung Arbeit investiert.

10 Umgang mit Ihren Daten

Wir verarbeiten die Angaben aus Ihrer Meldung ausschließlich zur Bearbeitung des Falls, zur Rückfrage bei Ihnen und zur Erfüllung unserer gesetzlichen Melde- und Nachweispflichten. Rechtsgrundlage ist unser berechtigtes Interesse an der Sicherheit unserer Produkte sowie die Erfüllung rechtlicher Verpflichtungen. Die Fallakte bewahren wir entsprechend den Vorgaben des Cyber Resilience Act auf. Sie können jederzeit unter product_security@hargassner.at Auskunft über die zu Ihrer Person gespeicherten Daten verlangen.

11 Kein Kanal für Störungen und Service

Bitte beachten

Die Adresse product_security@hargassner.at ist ausschließlich für Meldungen zu Sicherheitslücken bestimmt und wird auf enge Fristen hin überwacht.

Störungsmeldungen, Ersatzteilbestellungen, Servicetermine und allgemeine Produktfragen richten Sie bitte an Ihren Fachpartner oder an den Hargassner-Kundendienst. Anfragen dieser Art können wir hier nicht bearbeiten.

**HARGASSNER GES MBH**

Anton Hargassner Str. 1
A-4952 Weng
+43 7723 5274-0
office@hargassner.at
hargassner.com

12 Geltung und Änderungen

Diese Politik gilt ab dem Datum der Freigabe und wird mindestens jährlich sowie anlassbezogen überprüft. Die jeweils gültige Fassung steht unter <https://www.hargassner.com/security>. Maßgeblich ist immer die dort veröffentlichte Version; ausgedruckte Exemplare sind unkontrollierte Kopien.

Version	1.0
Stand	08.09.2026
Nächste Prüfung	September 2027
Kontakt	product_security@hargassner.at
Anschrift	HARGASSNER Ges mbH, Anton Hargassner Str. 1, A-4952 Weng, Österreich

