

Cyberangriff auf Raumfahrtfirma Beyond Gravity

Stand 18.10.2026 11:20 · Sendung: – · Belegstärke: **bestätigt** · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

Wissensstand

■ Wissen 41 % ■ Wahrscheinlich 25 % ■ Nicht bekannt 34 %

Zeitpunkt, Ermittler (BACS, Mandiant) und Datenabfluss sind durch Agenturmeldungen, SRF und eine Aussage der GPK-Präsidentin gut belegt und von beiden Recherchen bestätigt. Der China-Verdacht stützt sich auf SRF-Quellen, eine offizielle Zuschreibung fehlt. Täter, Angriffsweg, Art der Daten und mögliche Folgen für die Fertigung sind offen. Eine Originalmitteilung der Firma wurde online nicht gefunden.

1. Was ist passiert, und warum?

WISSEN

- Beyond Gravity hat am 12. August 2026 erste Hinweise auf „möglicherweise schädliche Aktivitäten“ in der eigenen IT-Umgebung erhalten und spricht von einem gezielten Angriff durch einen mutmaßlich „hochprofessionellen Akteur“. (100 %)

[<https://www.blick.ch/politik/cyberangriff-auf-raumfahrtunternehmen-beyond-gravity/s56k68q>]

- Laut Keystone-SDA/AWP läuft die Untersuchung gemeinsam mit dem Bundesamt für Cybersicherheit (BACS) und der IT-Sicherheitsfirma Mandiant; die englische Keystone-SDA-Meldung vom 03.10. nennt beide ebenfalls. Laut SRF untersucht auch das VBS zusammen mit dem BACS. (100 %) [<https://www.inside-it.ch/beyond-gravity-meldet-cyberangriff-20261005> ; <https://www.swissinfo.ch/eng/space-research/space-company-beyond-gravity-was-the-target-of-a-cyberattack/92160616>]
- Laut SRF gehen Beyond Gravity und der Bund nach Aussage mehrerer Beteiligten intern davon aus, dass China dahintersteckt. Firma und VBS bestätigen das offiziell nicht. (100 %) [<https://www.srf.ch/news/schweiz/schweizer-weltraumkonzern-nach-cyberattacke-auf-beyond-gravity-verdacht-faellt-auf-china>]
- Die Firma schreibt: „Die Herkunft des Angreifers ist nach wie vor nicht bestätigt und bleibt Gegenstand laufender Abklärung.“ (100 %)

[<https://www.netzwoche.ch/news/2026-10-06/beyond-gravity-wird-opfer-eines-cyberangriffs>]

- Die Firma hat bei der Staatsanwaltschaft Bern Strafanzeige gegen Unbekannt gestellt. Die für Spionage zuständige Bundesanwaltschaft war laut SRF bis zum 15.10. nicht tätig geworden. (100 %) [<https://www.srf.ch/news/schweiz/schweizer-weltraumkonzern-nach-cyberattacke-auf-beyond-gravity-verdacht-faellt-auf-china>]
- Die FDP spricht von einem „Angriff auf die Schweiz“ und vermutet einen staatlichen Akteur. Das ist eine politische Einschätzung. (100 %)

[<https://www.20min.ch/story/bundesunternehmen-angriff-auf-die-schweiz-cyberattacke-auf-beyond-gravity-103643156>]

NICHT BEKANNT

- Wer der Täter ist (keine offizielle Zuschreibung)
- Wie die Angreifer hineingekommen sind
- Seit wann die Angreifer vor dem 12. August schon im Netz waren
- Ob die Angreifer vollständig entfernt sind
- Ob ein Ermittlungsverfahren der Bundesanwaltschaft folgt

WAHRSCHEINLICH (Einschätzung)

- Ziel war Spionage (Technologie-, Programm- oder Kundenwissen) und keine Erpressung mit Ransomware. (80 %) – Kein Bericht über Lösegeld oder verschlüsselte Systeme, Datenabfluss laut GPK, China-Verdacht laut SRF, lange stille Forensik und Kunden wie ESA/Ariane und NASA. Beide Recherchen kommen zum selben Schluss.

- Hinter dem Angriff steht ein staatlicher oder staatsnaher Akteur. (73 %) – Mehrere Beteiligte nennen gegenüber SRF China, die Firma spricht von einem hochprofessionellen Akteur, Mandant ist hinzugezogen. Eine offizielle technische Zuschreibung fehlt, deshalb nicht höher.
- Die Angreifer waren schon vor dem 12. August im Netz. (60 %) – Bei Spionagekampagnen liegt zwischen Erstzugriff und Entdeckung oft längere Zeit, im RUAG-Fall 2014 bis 2016 rund eineinhalb Jahre. Für Beyond Gravity gibt es dazu keine Angaben.

2. Was ist die Auswirkung?

WISSEN

- GPK-Präsidentin Maya Graf: „Die Geschäftsprüfungskommissionen von National- und Ständerat haben vom Datenabfluss Kenntnis erhalten.“ Die Kommissionen haben einen Bericht bekommen. (100 %) [<https://www.srf.ch/news/schweiz/schweizer-weltraumkonzern-nach-cyberattacke-auf-beyond-gravity-verdacht-faellt-auf-china> ; <https://www.inside-it.ch/china-steckt-moeglicherweise-hinter-cyberattacke-auf-beyond-gravity-20261015>]
- Welche Informationen abgeflossen sind und wie sensibel sie sind, ist laut Berichten unbekannt. (100 %) [<https://www.20min.ch/story/schweizer-raumfahrtfirma-steckt-china-hinter-dem-hackerangriff-auf-beyond-gravity-103650057>]
- Laut Firma ist die IT-Umgebung betroffen. Die IT wird stärker überwacht, Fachleute suchen nach Angreifer-Aktivitäten, betroffene Geräte werden forensisch untersucht, die Sicherheitsmaßnahmen wurden ausgebaut. (100 %)
[<https://www.blick.ch/politik/cyberangriff-auf-raumfahrtunternehmen-beyond-gravity/s56k68q> ; <https://www.inside-it.ch/beyond-gravity-meldet-cyberangriff-20261005>]
- Die zuständige Untergruppe der Kommissionen prüft, ob weiterer Handlungsbedarf besteht. (100 %) [<https://www.inside-it.ch/china-steckt-moeglicherweise-hinter-cyberattacke-auf-beyond-gravity-20261015>]
- Beyond Gravity beliefert das europäische Ariane-Programm und die NASA; in Emmen entstehen Nutzlastverkleidungen für Trägerraketen. (100 %) [<https://www.srf.ch/news/schweiz/schweizer-weltraumkonzern-nach-cyberattacke-auf-beyond-gravity-verdacht-faellt-auf-china>]

NICHT BEKANNT

- Welche Daten abgeflossen sind (Konstruktion, Kunden, Personal)
- Ob Kunden wie ESA, Arianespace oder NASA direkt betroffen sind
- Ob Produktion oder Lieferungen beeinträchtigt sind
- Wie hoch der finanzielle Schaden ist

WAHRSCHEINLICH (Einschätzung)

- Der größte Schaden ist ein Abfluss von Know-how und kein Stillstand. (72 %) – Datenabfluss ist durch die GPK-Präsidentin belegt, Ausfälle oder Lieferverzug werden in rund sechs Wochen Berichterstattung nirgends erwähnt.
- Größere Produktionsausfälle hat es wegen des Angriffs nicht gegeben. (70 %) – Kein Bericht nennt Ausfälle, bei einem Stillstand in einem bundeseigenen Werk wäre das wahrscheinlich bekannt geworden, und Spionageakteure vermeiden auffällige Störungen. Die Firma hat sich dazu aber nicht geäußert.
- Die Firma muss Kunden und Partner informieren und Risiken in der Lieferkette prüfen. (72 %) – Bei Datenabfluss in Raumfahrtprogrammen mit ESA- und NASA-Bezug sind vertragliche Informationspflichten üblich; öffentlich belegt ist das nicht.

3. Wie lange dauert es digital (Wiederherstellung IT)?

WISSEN

- Laut Firma ist die Untersuchung wegen der Komplexität des Angriffs „äußerst zeitintensiv“ und läuft mit dem BACS und externen Forensik-Spezialisten. (100 %)
[<https://www.blick.ch/politik/cyberangriff-auf-raumfahrtunternehmen-beyond-gravity/s56k68q>]
- Ein Sprecher begründete die knapp zwei Monate bis zur Veröffentlichung mit „Gründlichkeit vor Schnelligkeit“; eine voreilige Mitteilung hätte die Forensik gefährden können. (100 %)
[<https://www.inside-it.ch/beyond-gravity-meldet-cyberangriff-20261005>]

NICHT BEKANNT

- Ob die Angreifer vollständig aus dem Netz entfernt sind
- Ob Systeme neu aufgesetzt werden mussten
- Ob es überhaupt IT-Ausfälle gab oder die IT eingeschränkt läuft
- Wann die Untersuchung abgeschlossen sein soll

WAHRSCHEINLICH (Einschätzung)

- Bereinigung, Härtung und Threat Hunting dauern insgesamt noch Wochen bis mehrere Monate. (74 %) – Nach Spionageangriffen mit staatlichem Verdacht muss man mit versteckten Backdoors rechnen; im RUAG-Fall 2016 lief allein die Beobachtung von Januar bis Mai, die Analyse zog sich über Monate.
- Der normale Bürobetrieb läuft weitgehend, im Vordergrund steht die Forensik und nicht die Wiederherstellung. (60 %) – Keine Berichte über Ausfälle; bei Spionage bleiben Systeme oft in Betrieb, damit die Forensik die Angreifer beobachten kann, und die stille Untersuchung über sieben Wochen passt dazu.

4. Ist in der Anlage etwas kaputt, das lange dauert?

WISSEN

- Die Firma spricht nur von Aktivitäten in der IT-Umgebung; zu Produktion oder OT gibt es keine Angaben. (100 %) [<https://www.blick.ch/politik/cyberangriff-auf-raumfahrtunternehmen-beyond-gravity/s56k68q> ; <https://www.inside-it.ch/beyond-gravity-meldet-cyberangriff-20261005>]
- Auch die Berichte vom 15.10. (SRF, Inside IT, swissinfo) nennen keine Schäden an Fertigungs- oder Prüfanlagen. (100 %)
- [<https://www.inside-it.ch/china-steckt-moeglicherweise-hinter-cyberattacke-auf-beyond-gravity-20261015> ; <https://www.swissinfo.ch/eng/foreign-affairs/china-suspected-in-cyberattack-on-swiss-space-company/92221479>]
- In Emmen werden Verkleidungen für Trägerraketen gefertigt, die Satelliten schützen; Kunden sind unter anderem NASA und ESA. (100 %) [<https://www.srf.ch/news/schweiz/schweizer-weltraumkonzern-nach-cyberattacke-auf-beyond-gravity-verdacht-faellt-auf-china>]
- Am Standort Berndorf (AT) fertigt Beyond Gravity thermische Isolationen und Mechanismen für Satelliten und Trägerraketen. (100 %)

[<https://www.vienna.at/austrias-largest-space-company-invests-millions-in-berndorf/10266524>]

NICHT BEKANNT

- Ob die Fertigungsnetze (OT) von der Büro-IT getrennt sind
- Ob Konstruktions-, Maschinen- oder Prüfdaten abgeflossen oder verändert wurden
- Ob Lieferungen an Raketenprogramme verzögert sind

WAHRSCHEINLICH (Einschätzung)

- Physische Schäden an Fertigungsanlagen hat es nicht gegeben. (78 %) – Spionageakteure wollen unentdeckt bleiben, Sabotage würde sie verraten; kein Bericht deutet auf Anlagenschäden oder Verzug hin.
- Fertigungs- und Prüfdaten müssen auf Integrität geprüft werden. (58 %) – Bei Raumfahrtbauteilen hängt die Freigabe an Prüfprotokollen und sauberer Dokumentation; ist unklar, worauf die Angreifer Zugriff hatten, ist eine Prüfung naheliegend. Öffentlich bestätigt ist sie nicht.
- Fertigungsdaten (Konstruktionsdaten, Maschinenprogramme, Prüfprotokolle) waren über die IT für die Angreifer erreichbar. (40 %) – In vielen Fertigungsbetrieben liegen solche Daten auf IT-Servern (PLM, Fileserver); für Beyond Gravity gibt es dazu keine Angaben.

5. Wie viele solcher Ziele gibt es?

WISSEN

- RUAG International (operativ Beyond Gravity) hatte Ende 2025 1.926 Vollzeitstellen (FTE) und 2025 einen Nettoumsatz von 412,0 Mio. CHF (widersprüchlich: A nennt laut vienna.at rund 402 Mio. CHF Umsatz 2025 / B laut Geschäftsbericht 412,0 Mio. CHF; übernommen ist der Geschäftsbericht). (100 %) [<https://annualreport.ruag.com/en/node/411> ;

<https://www.vienna.at/austrias-largest-space-company-invests-millions-in-berndorf/10266524>]

- Beyond Gravity ist an 12 Standorten in sechs Ländern tätig (Schweiz, Schweden, Österreich, USA, Finnland, Portugal). Die Angaben zur Belegschaft schwanken je nach Quelle zwischen rund 1.600 und 1.900 Mitarbeitenden (Stellenanzeigen: rund 1.800; vienna.at, Juni 2026: rund 1.900). (100 %) [https://www.stepstone.at/jobs/in-berndorf_nieder%C3%B6sterreich ;

[<https://www.vienna.at/austrias-largest-space-company-invests-millions-in-berndorf/10266524>]

- Die Mutter RUAG war 2014 bis 2016 Opfer von Spionage mit Malware der Turla-Familie; mindestens 23 GB Daten flossen ab. (100 %) [https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/fachberichte/technical%20report%20ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf]

- 2019 wurden laut AFP vier Airbus-Zulieferer angegriffen; Quellen vermuteten Gruppen mit Verbindung zu chinesischen Nachrichtendiensten. (100 %)

[<https://securityaffairs.com/91744/hacking/airbus-suppliers-attacks.html>]

- Die chinesische Gruppe RedNovember hat 2024 bis 2025 Rüstungs-, Luft- und Raumfahrt- und Hightech-Fertiger angegriffen, vor allem über Edge-Geräte. (100 %)

[<https://www.securityweek.com/chinese-cyberspies-hacked-us-defense-contractors/>]

- In der Schweiz gingen 2025 beim BACS 222 Pflichtmeldungen zu Cyberangriffen auf kritische Infrastrukturen ein. (100 %)

[<https://www.blick.ch/digital/bund-zieht-bilanz-cyberangriffe-fast-jeden-tag-trifft-es-kritische-infrastruktur-id21705130.html>]

- Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Schweiz: 51672 gesamt (DNP3 15837, ProConOS 14468, EtherNet/IP 14205, Modbus 1881, Siemens S7 645, OPC UA 411) (100 %)

NICHT BEKANNT

- Wie viele Raumfahrt- und Rüstungszulieferer es in der Schweiz, in Österreich und Deutschland genau gibt (nicht recherchiert)

- Ob dieselbe Kampagne weitere Firmen der Branche getroffen hat

WAHRSCHEINLICH (Einschätzung)

- Andere europäische Raumfahrt- und Rüstungszulieferer stehen im Visier derselben oder ähnlicher Akteure. (78 %) – Muster aus RUAG 2016, Airbus-Zulieferern 2019 und RedNovember 2024 bis 2025; der Weltraum ist laut Politologe Ralph Weber seit langem ein Ziel von Geheimdiensten.

- Genau dieselben Angreifer haben weitere Firmen der europäischen Raumfahrt- und Rüstungslieferkette angegriffen. (60 %) – Staatliche Spionagekampagnen laufen meist gegen mehrere Ziele einer Branche, wie bei RedNovember dokumentiert; für diesen Fall gibt es keinen Beleg.

- Kleinere Zulieferer in der Kette sind ein häufigerer Einstieg als die großen Hersteller. (50 %) – Der Airbus-Fall 2019 lief über Zulieferer; für den aktuellen Fall gibt es dazu keine Angaben.

6. Kann das wieder passieren?

WISSEN

- Die Firma hat ihre Sicherheitsmaßnahmen nach eigenen Angaben ausgebaut. (100 %)

[<https://www.swissinfo.ch/eng/space-research/space-company-beyond-gravity-was-the-target-of-a-cyberattack/92160616>]

- Bei RUAG 2014 bis 2016 konnte der Erstzugang nicht geklärt werden; das Verfahren wurde 2018 eingestellt, weil die Täter nicht ermittelt werden konnten. (100 %) [https://www.ncsc.admin.ch/dam/ncsc/en/dokumente/dokumentation/fachberichte/technischer_bericht_apr_case_ruag_summary.pdf.download.pdf/TR-ZF-e.pdf ; <https://www.srf.ch/news/schweiz/schweizer-weltraumkonzern-nach-cyberattacke-auf-beyond-gravity-verdacht-faellt-auf-china>]

- Exploits waren laut Mandiant 2025 im sechsten Jahr in Folge der häufigste Einstieg (32 % der Fälle), Voice-Phishing kam auf 11 %. (100 %)

[<https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026>]

- Recorded Future erwartet, dass chinesische Gruppen weiterhin Edge-Geräte angreifen und Schwachstellen kurz nach Bekanntwerden ausnutzen. (100 %)

[<https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-cn-2025-0924.pdf>]

NICHT BEKANNT

- Welche Lücke diesmal ausgenutzt wurde
- Ob die Ursache gefunden und geschlossen ist
- Welche Maßnahmen konkret umgesetzt wurden

WAHRSCHEINLICH (Einschätzung)

- Beyond Gravity und vergleichbare Firmen bleiben dauerhaft Ziel staatlicher Spionage, es wird weitere Versuche geben. (86 %) – Zweiter bekannter Fall in der Firmengeschichte, Programme wie Ariane und NASA-Lieferungen bleiben interessant, die Firma ist politisch exponiert (Verkaufsdebatte). Beide Recherchen schätzen das sehr hoch ein.
- Die Angreifer versuchen nach der Bereinigung, wieder Zugang zu bekommen. (62 %) – Typisch für langfristig angelegte Spionage, für diesen Fall aber nicht belegt.

Lage

Beyond Gravity, der bundeseigene Schweizer Hersteller von Bauteilen für Trägerraketen und Satelliten mit Sitz in Zürich, hat am 12. August 2026 schädliche Aktivitäten in seiner IT-Umgebung bemerkt und den gezielten Angriff am 2./3. Oktober öffentlich gemacht. Laut Keystone-SDA/AWP untersucht die Firma den Vorfall mit dem Bundesamt für Cybersicherheit (BACS) und Mandiant. Seit dem 15.10. berichtet SRF, dass Firma und Bund intern China verdächtigen, und laut GPK-Präsidentin Maya Graf wissen die Geschäftsprüfungskommissionen beider Räte von einem Datenabfluss. Offiziell bestätigt sind weder Täter noch Umfang, und zu Produktion oder OT gibt es bisher keine Angaben.

Angriff	Gezielter Cyberangriff auf die IT-Umgebung mit laut GPK abgeflossenen Daten; laut Firma ein mutmaßlich hochprofessioneller Akteur, Muster passt zu Spionage.
Wann / Status	Erste Hinweise am 12.08.2026, öffentlich ab 02./03.10.2026 · unklar
Täter	Offiziell unbekannt; laut SRF gehen Firma und Bund intern von China aus – berichtet
Betreiber / Branche	Beyond Gravity (RUAG International AG, im Besitz des Schweizer Bundes) · Raumfahrtzulieferer (Strukturen und Komponenten für Trägerraketen und Satelliten, Mechanismen, Isolation); Kunden u. a. ESA/Ariane und NASA
Anlage / Alter	Fertigung von Raumfahrtkomponenten, z. B. Verbundstrukturen und Nutzlastverkleidungen in Emmen, thermische Isolation und Mechanismen in Berndorf (AT) · unbekannt (Fertigung in Emmen seit Ende der 1970er-Jahre)
Region	Hauptsitz Zürich; Standorte u. a. Emmen (CH), Berndorf und Wien (AT), Linköping (SE), Decatur (US), Finnland, Portugal

Angriffsvektor

Noch nicht bekannt – Hypothesen (Einschätzung):

- Hypothese: Ausnutzung einer Schwachstelle in einem Edge-Gerät mit Verbindung ins Internet (VPN, Firewall, Remote-Access-Gateway) (): Exploits sind laut Mandiant M-Trends 2026 seit sechs Jahren der häufigste Einstieg (32 %). Die chinesische Gruppe RedNovember kam 2024 bis 2025 bei Rüstungs- und Luftfahrtfertigern vor allem über Edge-Geräte hinein, und Recorded Future erwartet das weiter. Für Beyond Gravity selbst gibt es keinen Beleg. Gegenmaßnahme: CC5 Risk-Based Vulnerability Management und CC4 Secure Remote Access.
- Hypothese: Phishing oder Voice-Phishing gegen Mitarbeitende, um Zugangsdaten zu erbeuten (): Voice-Phishing war laut Mandiant 2025 in 11 % der Fälle der Einstieg; bei gezielter Spionage gegen Hightech-Firmen ein üblicher Weg. Kein Hinweis im konkreten Fall.
- Hypothese: Einstieg über einen Zulieferer, Partner oder Fernwartungszugang in der Lieferkette (): Bei Airbus liefen die Angriffe 2019 über Zulieferer. Zu Beyond Gravity gibt es keine Angaben zu Partnerzugängen, deshalb eher unwahrscheinlich, aber nicht auszuschließen.

Gegenmaßnahme: CC4 Secure Remote Access und CC2 Defensible Architecture.

Früherer Stand: Erstmeldung (04.10.2026 10:56)

Wissen 15 % · wahrscheinlich 10 % · nicht bekannt 75 %

Beyond Gravity ist ein Schweizer Hersteller von Bauteilen für Satelliten und Trägerraketen und gehört dem Bund. Die Firma meldet einen gezielten Cyberangriff durch mutmaßlich einen hochprofessionellen Akteur; erste schädliche Aktivitäten in der IT fielen am 12.08.2026 auf, öffentlich wurde der Fall erst knapp zwei Monate später. Laut SDA/AWP (cash.ch, swissinfo) untersucht die Firma den Fall mit dem Bundesamt für Cybersicherheit (BACS) und Mandiant und hat Strafanzeige gestellt. Wer dahintersteckt, ob Daten abgeflossen sind und ob Produktion oder OT betroffen sind, ist öffentlich nicht bekannt.

Früherer Stand: Nach 24 Stunden (05.10.2026 11:13)

Wissen 42 % · wahrscheinlich 28 % · nicht bekannt 30 %

Beyond Gravity ist der bundeseigene Schweizer Raumfahrtzulieferer und ging 2022 aus dem Rüstungskonzern RUAG hervor. Am 12. August 2026 fielen der Firma erste mögliche schädliche Aktivitäten in ihrer IT-Umgebung auf, öffentlich machte sie den Angriff am 02.10.2026. Sie hat Strafanzeige gestellt und spricht von einem mutmaßlich hochprofessionellen Akteur. Laut Keystone-SDA/AWP (swissinfo) untersucht sie den Vorfall mit dem BACS und Mandiant. Täter, Ziel, Datenabfluss und mögliche Folgen für Produktion oder OT sind öffentlich nicht bekannt, und seit dem 03.10. sind keine neuen Fakten dazugekommen.

Früherer Stand: Nach 72 Stunden (07.10.2026 11:02)

Wissen 40 % · wahrscheinlich 27 % · nicht bekannt 33 %

Die bundeseigene Schweizer Raumfahrtfirma Beyond Gravity ging 2022 aus RUAG hervor. Sie bemerkte am 12. August 2026 möglicherweise schädliche Aktivitäten in ihrer IT-Umgebung und machte den Angriff am 2. Oktober öffentlich. Laut Firma steckt mutmaßlich ein hochprofessioneller Akteur dahinter. Nach Angaben eines Firmensprechers gegenüber AWP läuft die Untersuchung mit dem BACS und Mandiant. Wer der Täter ist, wie die Angreifer hineinkamen und ob Daten abgeflossen sind, ist öffentlich nicht bekannt. Dasselbe gilt für mögliche Folgen für Produktion oder OT.

Öffentliche Einschätzung von OT-Cyber auf Basis öffentlicher Quellen. Prozent = Einschätzung: 100 % bestätigt, 0 % sicher falsch. Fachliche Einschätzung, keine Schuldzuweisung.