Cybersecurity Database

Report

ARTEX, das KI-gesteuerte Angriffswerkzeug, vor dem FBI und CERT-EU warnen (2026)

ARTEX entstand als Open-Source-Werkzeug für automatisierte, von Sprachmodellen gesteuerte Penetrationstests, doch seit August 2026 setzen kriminelle und staatliche Gruppen es gegen Organisationen in aller Welt ein. CERT-EU warnte am 5. November, das FBI am 13. November; am 19. November bestätigte die Europäische Kommission eine mit einem KI-Werkzeug geführte Cyberkampagne, bei der laut Kommission vom 23. November Daten von Nutzern der EU Academy gestohlen wurden. Was bekannt ist, welche Regeln und Normen zählen und was jetzt zu tun ist.

Ausgabe Datenstand: 27. November 2026

Stets aktuelle Fassung https://www.cybersecuritydatabase.org/de/reports/artex-ai-hacking-tool/

Lizenz CC BY 4.0: freie Weiterverwendung mit Quellenangabe

Für wen: Für Journalisten und für alle, die in den betroffenen Sektoren arbeiten: die von amtlichen Quellen bestätigten Fakten, die zugehörigen Gesetze und Normen und die von den Behörden empfohlenen Maßnahmen.

> ARTEX ist eine „autonome“ Plattform für Penetrationstests: Der Nutzer beschreibt das Ziel in Worten, und ein Team von Agenten auf Basis von Sprachmodellen führt Aufklärung, Ausnutzung von Schwachstellen und Datenabfluss selbstständig durch. Im Juli 2026 für autorisierte Tests auf GitHub veröffentlicht, wird sie seit August von Kriminellen und staatlichen Gruppen genutzt: Laut FBI gelangten manche Angriffe vom ersten Kontakt in weniger als drei Stunden zu Administratorrechten. Das Repository wurde am 8. Oktober entfernt, doch Kopien, Varianten und eine kommerzielle Version sind weiter im Umlauf. CERT-EU am 5. November und das FBI am 13. November warnten, dass ihre Verbreitung Angriffe auf aus dem Internet erreichbare Systeme beschleunigt. Am 19. November bestätigte die Europäische Kommission, seit Oktober Ziel einer „KI-generierten Cyberkampagne“ gewesen zu sein; am 23. November bestätigte sie, dass Namen und E-Mail-Adressen von Nutzern der Plattform EU Academy abgeflossen sind. Am 24. November bestätigte auch die Schweiz erste erfolgreiche Angriffe mit KI-Agenten auf kritische Infrastrukturen, und am 26. November warnte das BSI, dass diese Werkzeuge inzwischen reif für den breiten Einsatz sind.

< 3 h
vom ersten Kontakt bis zu Administratorrechten, bei manchen Angriffen (FBI)

1600+
aus dem Internet erreichbare ARTEX-Konsolen Anfang November (FBI)

2250+
nachgelagerte Kunden, die beim Lieferkettenangriff über ConnectWise ins Visier gerieten (FBI)

Was jetzt zu tun ist

Die Empfehlungen von FBI und CERT-EU, um das Risiko eines Angriffs mit ARTEX oder ähnlichen Werkzeugen zu verringern.

1. Alles inventarisieren, was aus dem Internet erreichbar ist, auch Partner-und Lieferantenportale, Backends mobiler Apps, von einzelnen Abteilungen erstellte Anwendungen und Altsysteme, und abschalten, was nicht gebraucht wird.
2. Administrationskonsolen für Cloud und Netz, Backup-Plattformen und andere sensible Dienste nur aus vertrauenswürdigen Netzen oder über eigene Kanäle erreichbar machen, nicht aus dem Internet.
3. Notfall-Patches auf exponierten Systemen einspielen und als gering eingestufte Schwachstellen nicht liegen lassen: Ein automatisches Werkzeug verkettet sie.
4. Mehr-Faktor-Authentifizierung und minimale Rechte für Konten und Anwendungen nutzen und neue Zugangsdaten, Rechtezuweisungen und Anmeldungen aus unbekannten Netzen überwachen.
5. Nicht authentifizierten Nutzern keine detaillierten Fehlermeldungen zeigen, im Code und in Pipelines verbliebene Zugangsdaten suchen und ersetzen, Rate-Limits für APIs und Portale setzen.

6. Anmelde-und Audit-Protokolle aufbewahren, den Einsatz von KI-Werkzeugen im eigenen Netz überwachen und einen Verdacht auf einen ARTEX-Vorfall den Behörden melden (in Europa dem nationalen CSIRT, in den Vereinigten Staaten IC3).

Chronologie

Datum	Was geschah	Quellen
8. Oktober 2026	Der Entwickler „Autumn-27“, der ARTEX im Juli auf GitHub veröffentlicht und als nur für autorisierte Tests bestimmt bezeichnet hatte, macht das Repository nach Berichten über Missbrauch durch Angreifer unzugänglich. Laut FBI bleibt das Werkzeug über Forks, archivierte Kopien und eine kommerzielle Version, ARTEX PRO, verfügbar; Angriffe mit ARTEX werden seit mindestens August 2026 beobachtet.	[1]
5. November 2026	CERT-EU, der Cybersicherheitsdienst der EU-Institutionen, veröffentlicht die Analyse „Beware of ARTEX“: Mehrere Bedrohungsakteure weltweit nutzen das Werkzeug, und CERT-EU hat gegen die von ihm geschützten Institutionen ähnliche, KI-gesteuerte Aktivitäten beobachtet, die sehr wahrscheinlich mit ARTEX ausgeführt wurden. Die öffentliche Verfügbarkeit des Werkzeugs werde seine Verbreitung beschleunigen, warnt CERT-EU.	[2]
13. November 2026	Das FBI veröffentlicht die FLASH-Warnung FLASH-20261113-001 zu ARTEX mit beobachteten Techniken, Kompromittierungsindikatoren und Empfehlungen. Die betroffenen Sektoren reichen von Finanzdienstleistungen über Verwaltung und Verteidigung bis zu Halbleitern, Energie und Gesundheit; unter den genannten Kampagnen sind ein Angriff auf südkoreanische Finanzinstitute und die Kompromittierung der Lieferkette von ConnectWise Cloud Backup. Das FBI bittet, Vorfälle mit ARTEX an IC3 zu melden.	[1]
19. November 2026	Beim Mittagsbriefing bestätigt der Sprecher der Europäischen Kommission eine „Cyberkampagne“ gegen die Kommission, entdeckt am 22. Oktober und nach ersten Prüfungen am 26. Oktober bestätigt: Vorsorglich wurden mehrere Anwendungen abgeschaltet, die meisten sind inzwischen wiederhergestellt. Es war eine „KI-generierte“ Kampagne mit einem öffentlich verfügbaren KI-Werkzeug; bisher keine Hinweise auf eine Verletzung der Daten des gesamten Personals und keine bekannte Lösegeldforderung. Die Kommission steht mit CERT-EU und dem Europäischen Datenschutzbeauftragten in Kontakt und nennt keinen Verantwortlichen.	[5]
23. November 2026	Die Kommission bestätigt, dass die Kampagne auch die Plattform EU Academy traf, die externen Nutzern Online-Kurse zur EU-Politik anbietet: Personenbezogene Daten der Nutzer, darunter Namen und E-Mail-Adressen, sind abgeflossen. Das Ausmaß wird noch untersucht; der öffentliche Zugang zur Plattform wurde gesperrt, die Nutzer wurden per Hinweis auf der Website informiert und der Europäische Datenschutzbeauftragte wurde benachrichtigt. Keine Zuschreibung, solange die Untersuchung nicht abgeschlossen ist.	[6]

Datum	Was geschah	Quellen
24. November 2026	Das Nationale Zentrum für Cybersicherheit der Schweiz (NCSC/BACS) bestätigt die ersten Fälle in der Schweiz, in denen Angriffe mit KI-Agenten („Agentic Offensive Frameworks“) gegen Unternehmen und Betreiber kritischer Infrastrukturen aus mindestens zwei Sektoren geführt wurden: In allen bekannten Fällen gelang den Angreifern die Kompromittierung der Systeme. Laut NCSC hat sich die Zahl der über das Internet erreichbaren KI-Agenten wie ARTEX oder CyberStrikeAI seit Oktober 2026 fast verdoppelt; es empfiehlt, kritische Updates für exponierte Systeme innerhalb von 24 Stunden einzuspielen.	[3]
26. November 2026	Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt, dass „Agentic Offensive Frameworks“ wie ARTEX, CAIRN oder PentAGI vom Experiment in den produktiven Einsatz übergegangen sind, und bestätigt aufgrund eigener Erkenntnisse ihren hohen Reifegrad. Sie funktionieren auch mit frei zugänglichen Modellen und senken die nötigen Fachkenntnisse deutlich; das BSI erwartet eine deutliche Zunahme von Qualität und Quantität der Angriffe und geht davon aus, dass aus dem Internet erreichbare Infrastrukturen kompromittiert werden, wenn auf Schwachstellen nicht reagiert wird. Es fordert, schwache oder Standardpasswörter und ungeschützte Schnittstellen zu beseitigen, einen Notfallplan bereitzuhalten und die einfachsten Angriffswege sofort zu schließen.	[4]

Betroffene Länder und Stand der EU-Regeln

Land	Gemeldete Fälle	NIS 2	CER
Europäische Union	CERT-EU hat gegen die Organe, Einrichtungen und Agenturen der EU KI-gesteuerte Aktivitäten beobachtet, die sehr wahrscheinlich mit ARTEX ausgeführt wurden. Die Europäische Kommission bestätigte eine am 22. Oktober entdeckte „KI-generierte“ Kampagne mit einem öffentlich verfügbaren KI-Werkzeug, ohne es zu nennen; laut Presse erkannte CERT-EU darin ARTEX. Mehrere interne Anwendungen wurden vorsorglich abgeschaltet (laut Presse mehr als zehn Tage lang die Systeme für Gehälter, Urlaub und Arztkostenerstattung sowie die Übersetzungsdienste: The Record, 19. November). Am 23. November bestätigte die Kommission den Diebstahl von Namen und E-Mail-Adressen externer Nutzer der Plattform EU Academy, die nun für die Öffentlichkeit geschlossen ist. [2] [5] [6] [7]	–	–

Land	Gemeldete Fälle	NIS 2	CER
Südkorea	Laut FBI führten finanziell motivierte Angriffe mit ARTEX auf südkoreanische Finanzinstitute zum Abfluss personenbezogener Daten von rund 67.000 Menschen. [1]	–	–
Schweiz	Das Schweizer NCSC hat erste Meldungen über Angriffe mit KI-Agenten gegen Organisationen und Betreiber kritischer Infrastrukturen aus mindestens zwei Sektoren erhalten, die alle erfolgreich waren; es teilt mit den Betreibern kritischer Infrastrukturen technische Indikatoren, um sie zu erkennen. [3]	–	–
Deutschland	Das BSI berichtet von sich häufenden Sicherheitsvorfällen, bei denen der Einsatz solcher Tools vermutet und zum Teil nachgewiesen wurde, und bestätigt aufgrund eigener Erkenntnisse den hohen Reifegrad von „Agentic Offensive Frameworks“. [4]	■ Umgesetzt, in Kraft	■ Umgesetzt, in Kraft

Der Stand von NIS 2 und CER stammt aus den Umsetzungsseiten der Website und wird mit den Daten aktualisiert.

Wie ARTEX funktioniert

Laut FBI ist ARTEX eine in Go geschriebene Multi-Agenten-Plattform, die in natürlicher Sprache beschriebene Ziele in Befehle übersetzt, die spezialisierte Agenten ausführen, mit minimalem menschlichem Eingriff nach der Zielvorgabe. Sie enthält kein eigenes Modell, sondern bindet externe Sprachmodelle an, kommerzielle oder quelloffene. In den vom FBI untersuchten, von Angreifern kontrollierten Instanzen überwiegen Modelle chinesischer Herkunft, gewählt wegen Kosten und Fähigkeiten und weil sichtbare Schutzmechanismen fehlen, wenn die Anfrage als Penetrationstest dargestellt wird.

Das Werkzeug ist besonders wirksam bei Randsystemen: Partner-und Lieferantenportale, Backends mobiler Apps, Mitarbeiteranwendungen, Altsysteme, Drittanbieter-Integrationen. Zu den vom FBI beobachteten Techniken gehören die Nutzung offengelegter Cloud-Zugangsdaten, unsignierte SAML-Assertions, XXE-und SSRF-Schwachstellen, im Code hinterlegte Administratorpasswörter und der Weg von einem kompromittierten Lieferanten zu dessen Kunden über Vertrauensbeziehungen.

Entscheidend ist für FBI und CERT-EU nicht eine neue Schwachstelle, sondern die Geschwindigkeit: Eine kleine Gruppe mit wenig Fachwissen kann mehrere Angriffe gleichzeitig führen und abschließen, bevor die Verteidiger reagieren, auch wenn der erzeugte Datenverkehr auffällig ist und Alarme auslösen kann.

Warum darüber gesprochen wird

Es ist einer der ersten von Behörden mehrerer Länder dokumentierten Fälle, in denen ein für alle verfügbarer KI-Agent in großem Umfang für echte Angriffe genutzt wird, und der erste, der die Europäische Kommission direkt trifft. Für Organisationen ändert sich der Zeitmaßstab: Bekannte, aber nicht behobene Schwachstellen und vergessene, aus dem Internet erreichbare Systeme werden in Stunden statt Wochen gefunden und ausgenutzt.

Der Fall belebt auch die Debatte über Dual-Use-Werkzeuge: ARTEX wurde für autorisierte Tests entwickelt, und dieselbe Art der Automatisierung hilft Verteidigern, die eigenen Schwächen zuerst zu finden. Deshalb empfiehlt CERT-EU, die Nutzung von KI-Werkzeugen im eigenen Netz im Blick zu behalten und als gering eingestufte Schwachstellen nicht liegen zu lassen.

Was die Regeln sagen

Die Rechtsakte der Datenbank, die die Sicherheit der EU-Institutionen, KI-Systeme und das Management von Cyberrisiken betreffen.

Verordnung (EU, Euratom) 2023/2841 zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union

Die Verordnung über Cybersicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union: Sie verpflichtet jede Stelle zu Risikomanagementmaßnahmen und zur Meldung erheblicher Vorfälle an CERT-EU, das als gemeinsamer Dienst fungiert. Sie ist der Rahmen für den Angriff auf die Kommission und die Warnung von CERT-EU.

Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie)

Für Unternehmen und Einrichtungen in wesentlichen und wichtigen Sektoren verlangt NIS 2 Schwachstellenmanagement, Sicherheit der Lieferkette und schnelle Meldung von Vorfällen (Art. 21 und 23): genau die Maßnahmen, die ARTEX mit Angriffen von wenigen Stunden auf die Probe stellt.

Verordnung (EU) 2024/1689 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Verordnung über künstliche Intelligenz)

Die KI-Verordnung verpflichtet Anbieter von KI-Modellen mit allgemeinem Verwendungszweck und systemischem Risiko, systemische Risiken zu bewerten und zu mindern und ein angemessenes Cybersicherheitsniveau zu gewährleisten (Art. 55); als systemisches Risiko nennt Erwägungsgrund 110 offensive Cyberfähigkeiten wie das Aufspüren und Ausnutzen von Schwachstellen. Der Fall zeigt, warum sie zählen.

Die maßgeblichen Normen

Die Normen der Datenbank, die zur Verkleinerung der Angriffsfläche und zur Steuerung des KI-Einsatzes am nützlichsten sind.

CIS Controls v8.1 – Kritische Sicherheitskontrollen des CIS

Die Controls 1 und 2 (Inventar von Systemen und Software), 7 (kontinuierliches Schwachstellenmanagement) und 12 (Verwaltung der Netzinfrastruktur) sind die erste Verteidigung gegen ein Werkzeug, das gerade vergessene Systeme sucht.

OWASP Top 10:2025 – OWASP Top 10:2025 – Die zehn kritischsten Sicherheitsrisiken für Webanwendungen

Die laut FBI von ARTEX ausgenutzten Schwachstellen (Zugriffskontrolle, Fehlkonfigurationen, SSRF, Zugangsdaten im Code) sind Kategorien der OWASP Top 10: eine Liste zur Prüfung exponierter Portale und Webanwendungen.

NIST CSF 2.0 – Cybersecurity Framework (CSF) 2.0 des NIST

Der Rahmen zur Organisation der Verteidigung: Inventar und Lieferantenmanagement (Govern und Identify), Schutz der Zugänge sowie schnelle Erkennung und Reaktion (Detect und Respond), die bei Angriffen von wenigen Stunden bereits stehen müssen.

NIST AI RMF 1.0 – Rahmenwerk für das Risikomanagement künstlicher Intelligenz (AI RMF 1.0)

Der Rahmen des NIST für das Management von KI-Risiken: nützlich für alle, die KI-Agenten entwickeln oder einsetzen, auch für Sicherheitstests, um zulässige Nutzungen, Kontrollen und Verantwortlichkeiten festzulegen.

ISO/IEC 42001:2023 – Informationstechnik – Künstliche Intelligenz – Managementsystem

Das KI-Managementsystem: interne Regeln, welche KI-Werkzeuge von wem und mit welchen Kontrollen genutzt werden dürfen, wie es CERT-EU mit der Empfehlung verlangt, den KI-Einsatz im eigenen Netz zu überwachen.

Quellen der Analyse

1. **Amtliche Quellen:** Federal Bureau of Investigation (FBI), FLASH-20261113-001 – Threat Overview of ARTEX Autonomous Penetration Testing Framework ↗, 13. November 2026.https://www.ic3.gov/csa/2026/261113.pdf
2. CERT-EU, From Penetration Testing to Cyber Threat: Beware of ARTEX ↗, 5. November 2026.https://cert.europa.eu/blog/from-penetration-testing-to-cyber-threat-beware-of-artex
3. National Cyber Security Centre (NCSC), Switzerland, Cyberattacks involving AI agents: First confirmed cases in Switzerland ↗, 24. November 2026.https://www.bacs.admin.ch/en/26-ki-agenten-1-en
4. Bundesamt für Sicherheit in der Informationstechnik (BSI), Hoher Reifegrad von Agentic Offensive Frameworks verschärft Bedrohungslage ↗, 26. November 2026.https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Offensive-agentische-KI_261115.html
5. European Commission – Audiovisual Service, EC Midday press briefing of 19/11/2026 – Cybersecurity: Cyber campaign against the European Commission, Q&A ↗, 19. November 2026.https://audiovisual.ec.europa.eu/en/media/video/I-298222
6. European Commission – Audiovisual Service, EC Midday press briefing of 23/11/2026 – Cybersecurity: Cyber campaign against the European Commission, Q&A ↗, 23. November 2026.https://audiovisual.ec.europa.eu/en/media/video/I-298395
7. **Presse:** The Record (Recorded Future News), European Commission confirms cyberattack, says hackers used AI tool ↗, 19. November 2026.https://therecord.media/european-commission-confirms-cyberattack-using-ai

Für eine praktische Antwort

- Wem und wie schnell ein Vorfall zu melden ist, Land für Land
- Die nationalen Behörden und CSIRTs jedes Landes
- Die Seite Ihres Sektors: EU-Gesetze, spezifische Rechtsakte und Normen

Quellen und Daten

„Was bekannt ist“ auf Grundlage der FLASH-Warnung des FBI, der Analyse von CERT-EU, der Erklärungen des Sprechers der Europäischen Kommission bei den Mittagsbriefings vom 19. und 23. November sowie, wo angegeben, von Medienberichten. Stand zum angegebenen Datum. Maßgeblich sind die zitierten Quellen.

- Interaktive Seite: NIS 2 https://www.cybersecuritydatabase.org/de/transposition/nis2/
- Interaktive Seite: CER https://www.cybersecuritydatabase.org/de/transposition/cer/
- Interaktive Seite: Normen und Frameworks https://www.cybersecuritydatabase.org/de/standards/
- Offene Daten (JSON): documents.json https://www.cybersecuritydatabase.org/api/v1/documents.json

Zitiervorschlag

Cybersecurity Database, „ARTEX, das KI-gesteuerte Angriffswerkzeug, vor dem FBI und CERT-EU warnen (2026)“, Datenstand 27. November 2026, https://www.cybersecuritydatabase.org/de/reports/artex-ai-hacking-tool/. Lizenz CC BY 4.0.