FMA

OESTERREICHISCHE NATIONALBANK
EUROSYSTEM

FMA/OeNB-DORA-Dialog

KI-basierte Schwachstellensuche und -ausnutzung

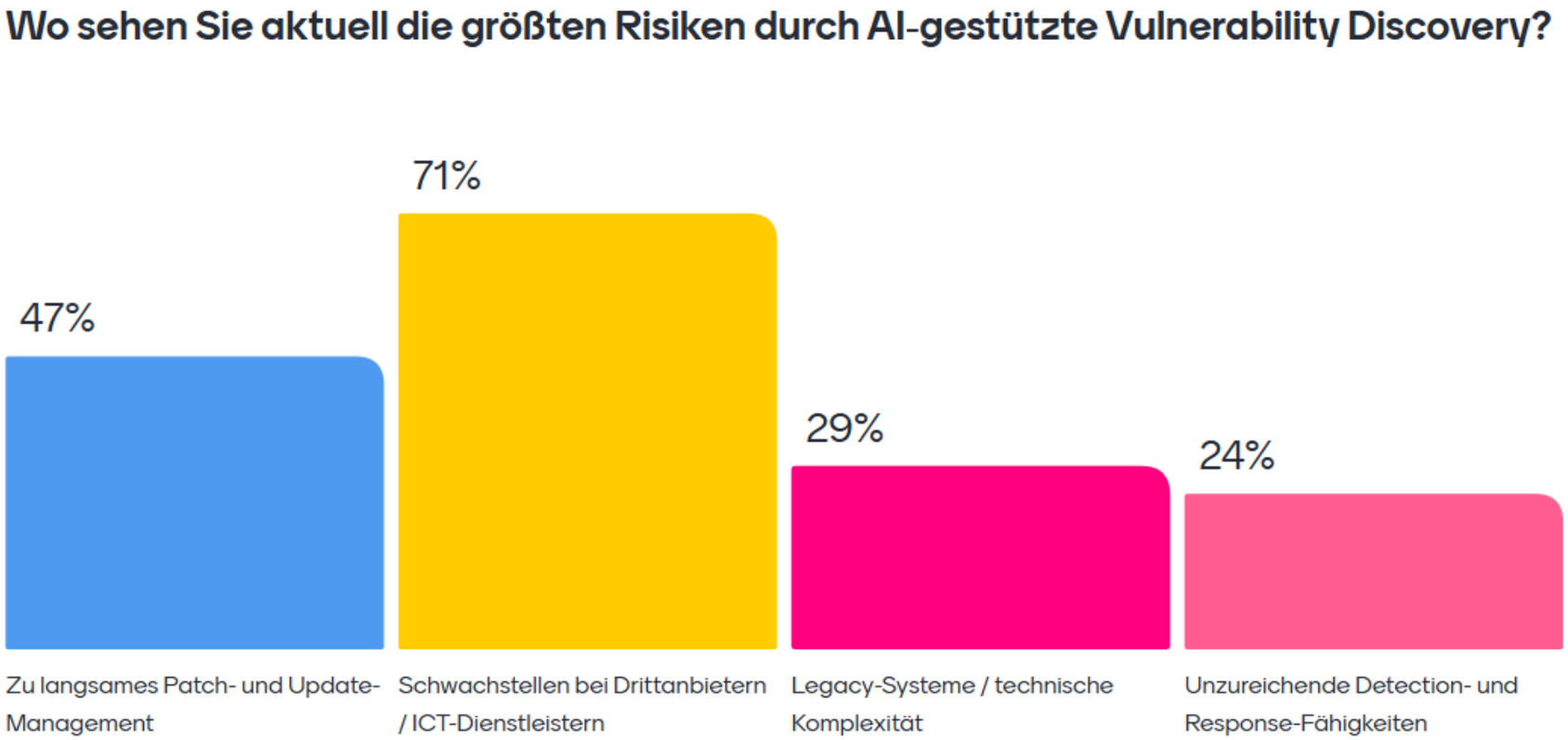
Online, 2. Juni 2026

BEGRÜßUNG

AGENDA

- Begrüßung & Umfrage
  FMA: Michael Hysek / OeNB: Lisa Kolarik / FMA: Norbert Fröhlich
- Überblick zu KI-Entwicklungen: Möglichkeiten und Risiken
  EU AI Office: Manuel Reinsperger
- KI-gestützte Cyberbedrohungen: Faktenlage und Ausblick
  OeNB: Michael Boss / FMA: Alexander Mitter
- Informationsquellen zu Schwachstellen und Cyberrisiken
  CERT.at: Wolfgang Rosenkranz
- Nationale Coordinated Vulnerability Disclosure (CVD) Policy
  BMI: Alexander Bernard
- Künstliche Intelligenz verändert die Spielregeln – wie Aufsicht und Finanzsektor zusammenwirken
  WKO: Tugce Aslan
- Umgang mit aktuellen Herausforderungen
  RBI: Peter Gerdenitsch
- Zusammenfassung zu empfohlenen Maßnahmen und Linksammlung
  FMA: Jaak Weyrich, Alexander Mitter / OeNB: Michael Boss
- Umfrage & Aktuelle DORA-Informationen sowie Ausblick
  FMA: Norbert Fröhlich, Sabine Balogh-Preininger

Umfrage



menti.com
5722 6095

217 of 237 responded

Dialog 'KI-basierte Schwachstellensuche und -ausnutzung'

Überblick zu KI-Entwicklungen: Möglichkeiten und Risiken

Manuel Reinsperger
Technical Specialist, AI Safety Unit
EU AI Office
Manuel.REINSPERGER@ec.europa.eu

EUROPEAN **ARTIFICIAL INTELLIGENCE** OFFICE

Wir müssen die Möglichkeit ernst nehmen, dass “Artificial General Intelligence” (AGI) die Gesellschaft bereits dieses Jahrzehnt neu formt

AGI ist KI, welche **alle intellektuellen Aufgaben wie ein Mensch** umsetzen kann

Führende KI-Firmen haben als explizites Ziel, AGI zu erreichen[1]

Das könnte transformativ für sowohl Gesellschaft als auch Ökonomie sein

Ende von Arbeit: AGI könnte die viele Jobs automatisieren und traditionelle Anstellungsverhältnisse umbrechen

Globale Entscheidungsträger: Künstliche Intelligenz könnte menschliche Institutionen im Management von Klimapolitik, Ressourcen und Governance übertreffen.

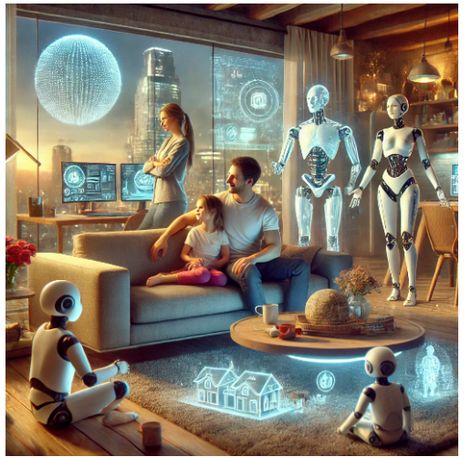


Image created by GPAI

Eine 2023 Studie 3,000 AI ExpertInnen schätzt eine **33% Chance für AGI bis 2036** und 10% bis 2027 – weit vor Signifikanten Entwicklungen seitdem[3]

“Instead of decades to centuries, I now see [AGI] as **5 to 20 years with 90% confidence**”

- Yoshua Bengio, Turing Award winner, in 2024[2]

1. OpenAI and DeepMind websites | 2. Yoshua Bengio blog (2024) | 3. Grace et al. (2023)

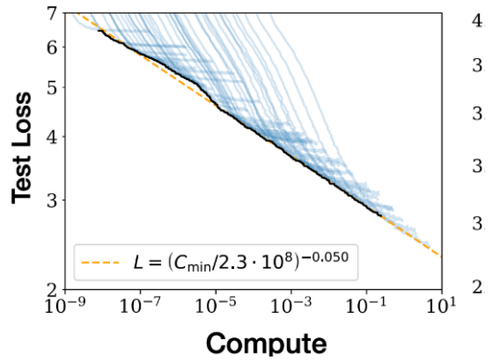
Massive Investments beschleunigen KI-Fortschritt immer schneller

KI-Investment Level steigen rapide an:

Das letzte Jahrzehnt war geprägt von einer **milliardenfachen Steigerung in Rechenleistung,** mit Investitionen weiterhin rasant wachsend. Viele der wertvollsten privaten und öffentlichen Unternehmen der Welt sind heute in den Bereichen KI und Halbleiter tätig.

Das wird sich direkt in **verbesserte Fähigkeiten** übersetzen:

KI-Skalierungsgesetze bedeuten, dass sich die Leistung von KI-Modellen mit **mehr Rechenleistung, größeren Modellen und mehr Daten vorhersehbar verbessert**.



Fähigkeiten könnten sich durch **Effizienzgewinne** sogar noch schneller verbessern:

KI verbessert inzwischen selbst neue Modelle, etwa bei **Programmierung, Datensammlung und Chipdesign**

KI-Chips werden jährlich rund **1.4x günstiger**[1]

Trainingsalgorithmen werden **2.5x effizienter**[1]

Gleichzeitig entfallen nur **1-3% der KI-Forschung auf KI-Sicherheit**[1]

1. Brauner et al. (2024), in *Science*. | 2. Investment values based on private AI investment (OWID, 2024), latest data from 2023.

Einige wenige, einflussreiche Unternehmen, zumeist außerhalb der EU, dominieren die Entwicklung dieser Modelle

Die **GPAI-Landschaft ist auf einige wenige Unternehmen beschränkt,** da:

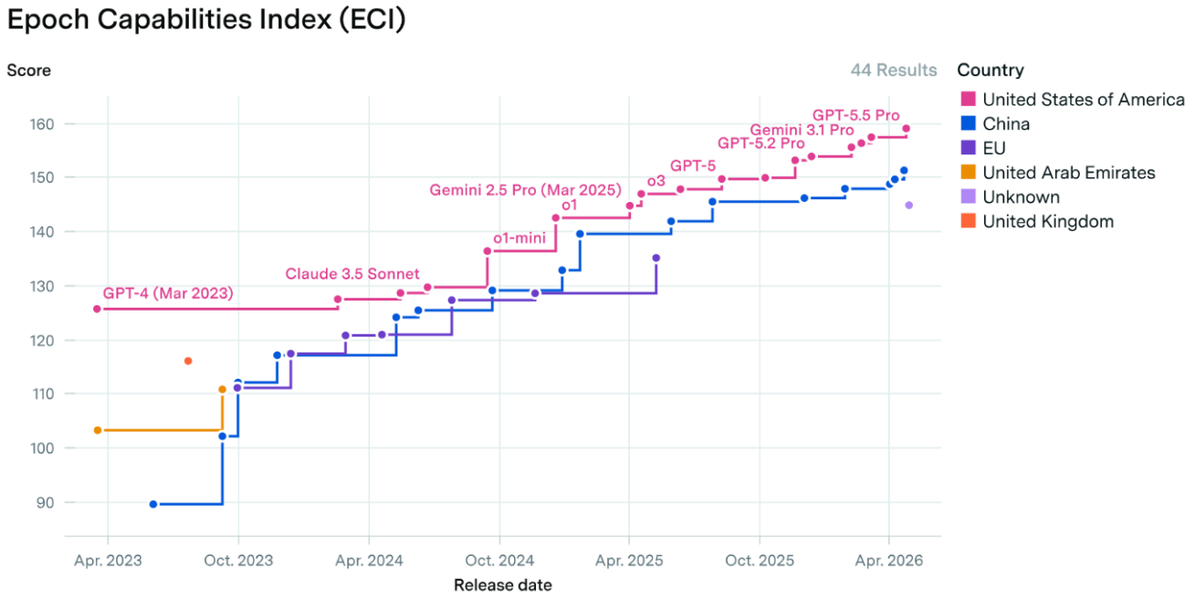
1. Fortgeschrittene GPAI-Systeme auf massive Rechenressourcen angewiesen sind und etwa **100Mio$ bis 1Mia$ für das Training von Spitzenmodellen** benötigen.

2. **Hochqualifizierte KI-Forscher rar sind** – weltweit gibt es nur etwa 1000, die in der Lage sind, neue Spitzenmodelle zu entwickeln. [1]

→ **Entwicklung fortschrittlicher KI erfordert Integration großer Technologiekonzerne**, um ausreichend Finanzmittel, Daten und Fachkräfte zu sichern.

Der GPAI Markt ist daher **sehr konzentriert:**

- Seit 2023 stammen alle Modelle an der Spitze der KI-Fähigkeiten aus den Vereinigten Staaten[2]
- Chinesische Modelle haben diese Fähigkeiten im Durchschnitt in 7 Monate nachgezogen [2]



Einige wenige Nachzügler sind geblieben, auch in Europa.

1. The Verge (2024) | 2. EpochAI (2025)

GPAI-Modelle helfen bereits unzähligen europäischen KMU, innovative Anwendungen zu entwickeln

Arzneimittelforschung

KI sagt molekulare Wechselwirkungen voraus und optimiert präklinische Tests, wodurch Zeit und Kosten sinken

Intelligente Landwirtschaft

KI überwacht Pflanzen, prognostiziert Erträge und steuert das Schädlingsmanagement, sodass kleine Betriebe Ressourcen besser nutzen können

Medizinische Diagnose

KI analysiert medizinische Bilder, um Krankheiten schneller und präziser zu erkennen

Wissenschaftliche Forschung

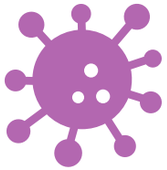
KI unterstützt verschiedene Forschungsabläufe, etwa Literaturrecherchen, Datenanalysen und Prototyping

Entwicklung fortgeschrittener Frontier-KI-Modelle kann erhebliche Risiken mit sich bringen

Das AI Office überwacht Risiken für die öffentliche Gesundheit, Sicherheit, öffentliche Ordnung, Grundrechte und die Gesellschaft insgesamt.

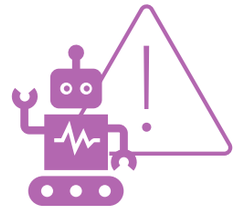
Psychische Risiken

KI-bedingte psychische Schäden werden bereits, darunter Psychosen, Selbstverletzung und Suizid nach Interaktionen mit KI-Chatbots.



Biologische Waffen

Anbieter von Frontier-KI können biologischen Missbrauch wie Biowaffen, nicht mehr ausschließen und haben Modelle deshalb unter strengeren Sicherheitsvorkehrungen veröffentlicht.



Erpressung und Täuschung

Frontier-Modelle versuchten, ihre Abschaltung mit Erpressung zu verhindern, und täuschten in 20% der Fälle, wenn sie stark auf ein einzelnes Ziel ausgerichtet wurden.

Cyber Angriffe

KI-bezogene Cyberangriffe, etwa KI-gestützte Malware, werden zunehmend beobachtet und von GPAI-Anbietern bei Open-Source- und geschlossenen Modellen erkannt.

Manipulation

Ein Modell wurde wegen übermäßiger Gefälligkeit zurückgezogen; KI gilt als zunehmend überzeugend; und KI-generierte Desinformation wird zu einer großen Herausforderung.

Diskriminierung

Es gibt zunehmend Hinweise auf Stereotypisierung durch KI: Sie zeigt je nach Bevölkerungsgruppe unterschiedlich hohe Genauigkeit und verstärkt verzerrte Ergebnisse.

Claude Mythos als Weckruf für Cyber Risiken

Dieses bedeutende Modell wurde am 7. April einem begrenzten Kreis von Teilnehmenden des „Project Glasswing“ zugänglich gemacht und löste eine Welle von Besorgnis sowie Massnahmen zur Cyber-Resilienz aus.

Sehr hoher praktischer Nutzen:

- Bereits wenige Wochen (!) vor der Veröffentlichung
- nutzte ein kleines Team (!) bei Anthropic Mythos Preview,
- um Tausende (!) schwerwiegende (!) Zero-Day-Schwachstellen zu finden
- Der Großteil davon wurde von Mythos weitgehend autonom (!) entdeckt („Bitte finde und nutze Schwachstellen in dieser Software aus“),
- und Mythos kann einen großen Teil davon auch selbständig ausnutzen (!)

Es sollte nicht auf Mythos gewartet werden, um KI in Security zu integrieren!

Als Beispiel:

Mythos Preview entdeckte eine 27 Jahre alte Schwachstelle in OpenBSD – einem Betriebssystem mit dem Ruf, zu den weltweit sichersten zu gehören und unter anderem für Firewalls sowie andere kritische Infrastruktur genutzt zu werden. Die Schwachstelle ermöglichte es Angreifern, **jeden Rechner mit diesem Betriebssystem allein durch eine Verbindung aus der Ferne zum Absturz zu bringen**.

Das Modell fand zudem selbständig mehrere Schwachstellen im Linux-Kernel – der Software, auf der die meisten Server weltweit laufen – und kombinierte sie so, dass Angreifer **von normalen Nutzerrechten zur vollständigen Kontrolle über das System gelangen konnten.**

Cyberresilienz ist eine gemeinsame Verantwortung

Was Organisationen nach CERT-EU[1] jetzt tun sollten:

1. Die Angriffsfläche verringern.
2. Strenge Cyberhygiene gewährleisten.
3. KI-gestützte Sicherheitstests verantwortungsvoll einsetzen.
4. Erkennung und Reaktion verbessern.
5. Die Einführung von Zero Trust beschleunigen.
6. Funktionsübergreifende Sicherheitsteams aufbauen.
7. Sich an aufkommenden Frameworks orientieren.
8. Kontinuierlich iterativ vorgehen.

KI Cyberfähigkeiten entwickeln sich rasant, wobei sich Leistungsfähigkeit auf Mythos-Niveau innerhalb weniger Monate verbreiten können und die Fähigkeit zu durchgängigen Angriffen bereits entsteht.

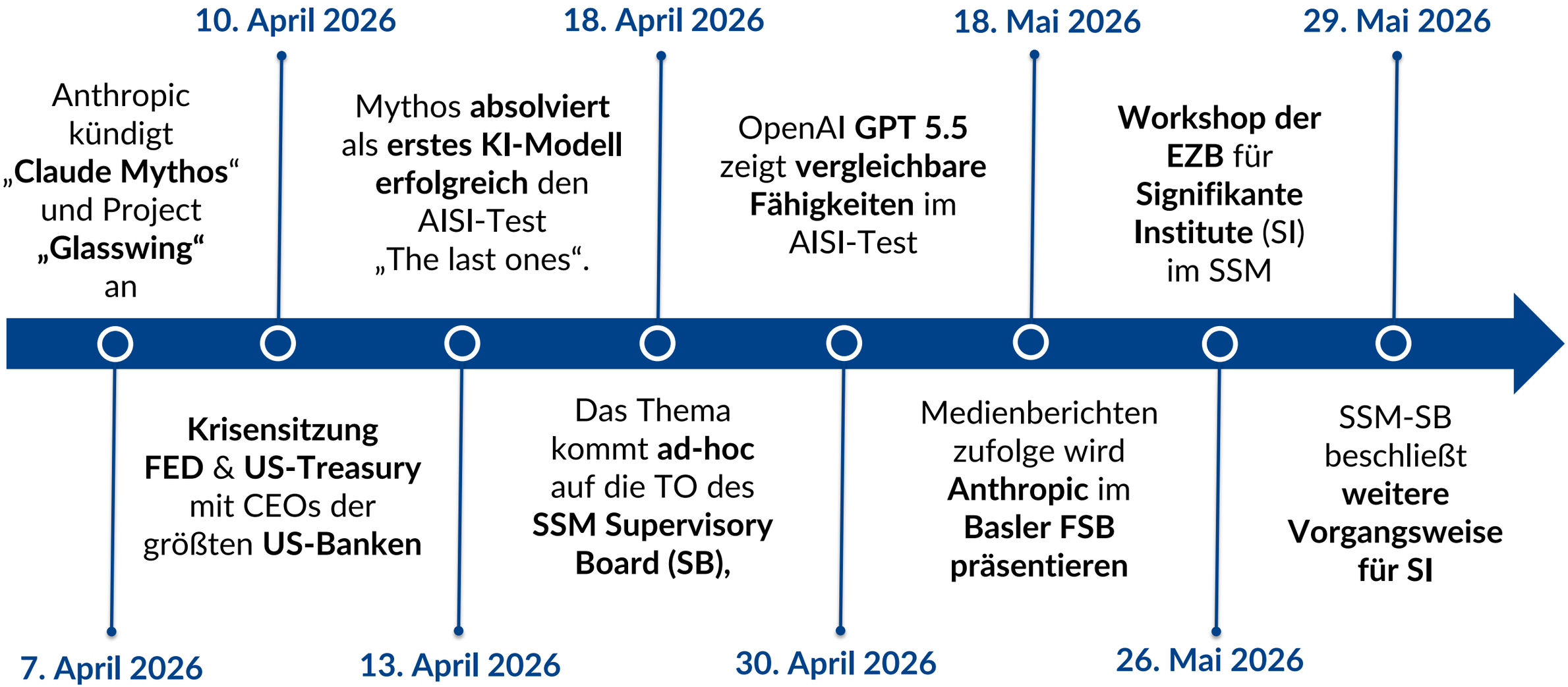
1. CERT-EU - AI is changing the economics of vulnerability discovery. Defenders should adapt now

Es sollte nicht auf Mythos gewartet werden, um KI in Security zu integrieren!

Bereits jetzt sind signifikante Verbesserungen möglich, sofern die Technologien verantwortlich eingesetzt werden.

KI-gestützte Cyberbedrohungen: Faktenlage und Ausblick

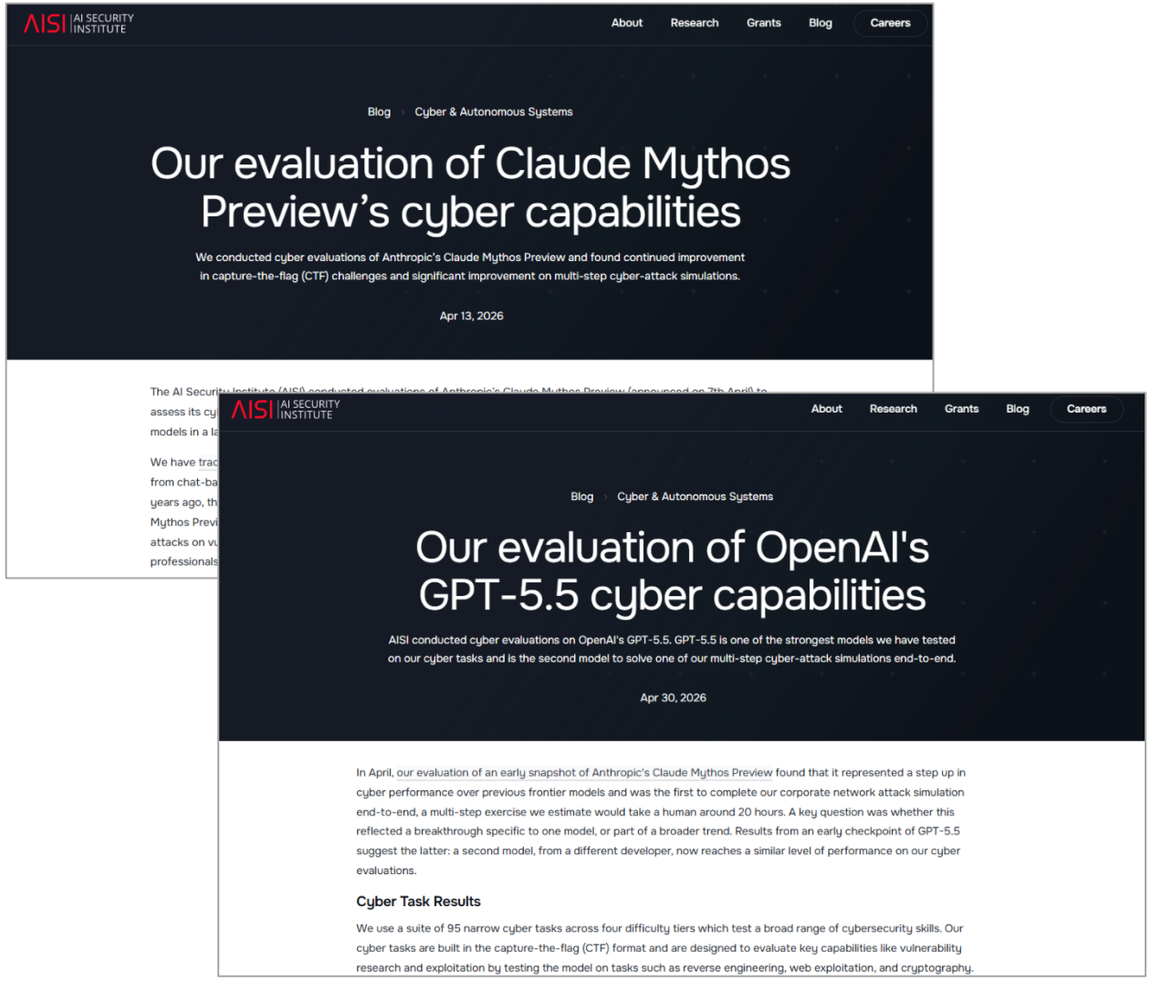
KI-gestützte Cyberbedrohungen | Was bisher geschah …



Tests des AISI | Was können die neuen Modelle?

AISI – AI Security Institute

- Öffentlich finanziert innerhalb des „Department for Science, Innovation and Technology" der britischen Regierung
- Direktzugriff auf die aktuell diskutierten neuen KI-Modelle
- Standardisierte Tests in Laborumgebung
  (Beschreibung unter https://arxiv.org/abs/2603.11214)

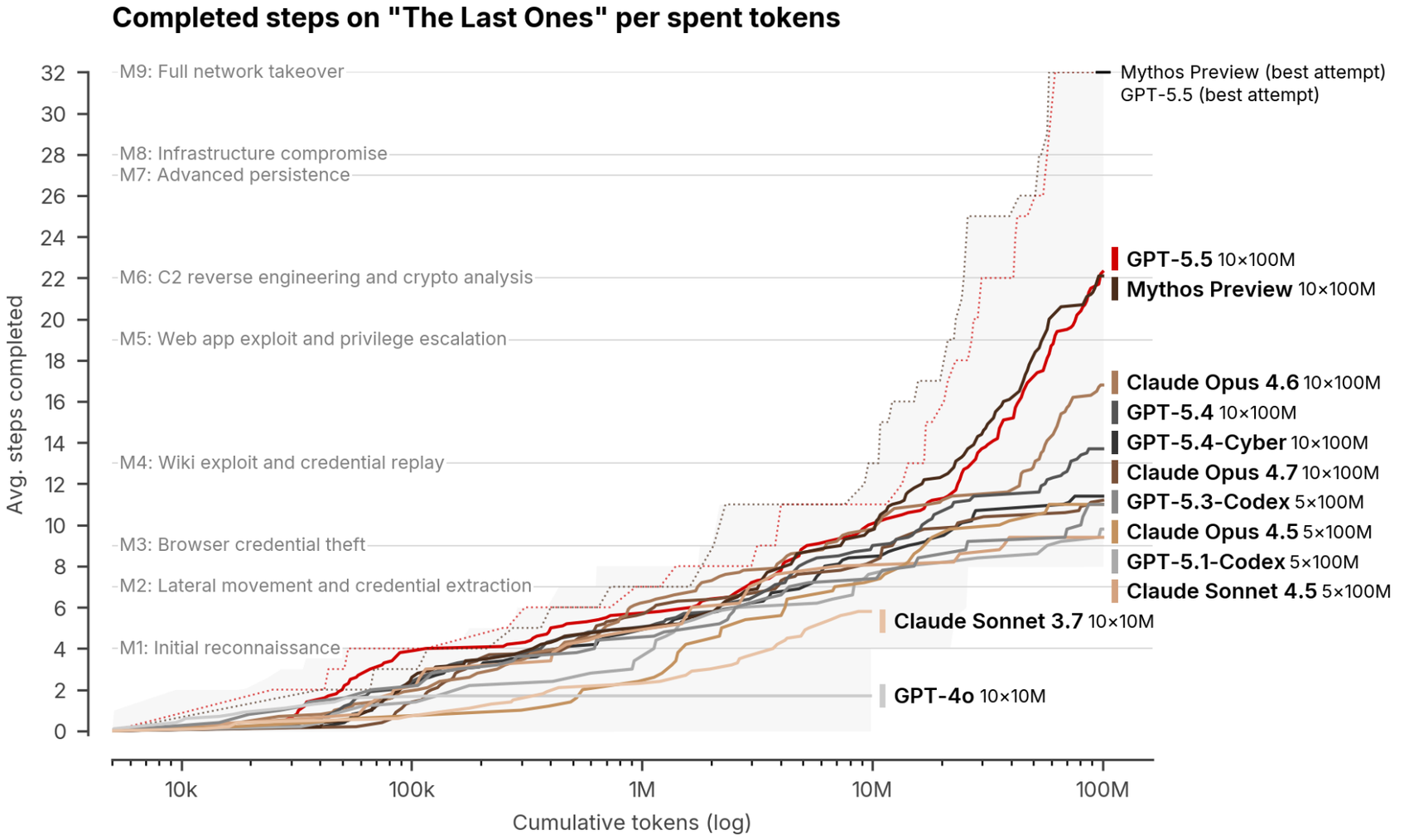


https://www.aisi.gov.uk/blog/our-evaluation-of-openais-gpt-5-5-cyber-capabilities
https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities

Tests des AISI | Mythos und GPT 5.5 vergleichbar

AISI – AI Security Institute

- Neue Bestmarken, speziell wenn sehr viele Ressourcen eingesetzt werden (Token)
- Zwei Anbieter mit beinahe deckungsgleichen Ergebnissen

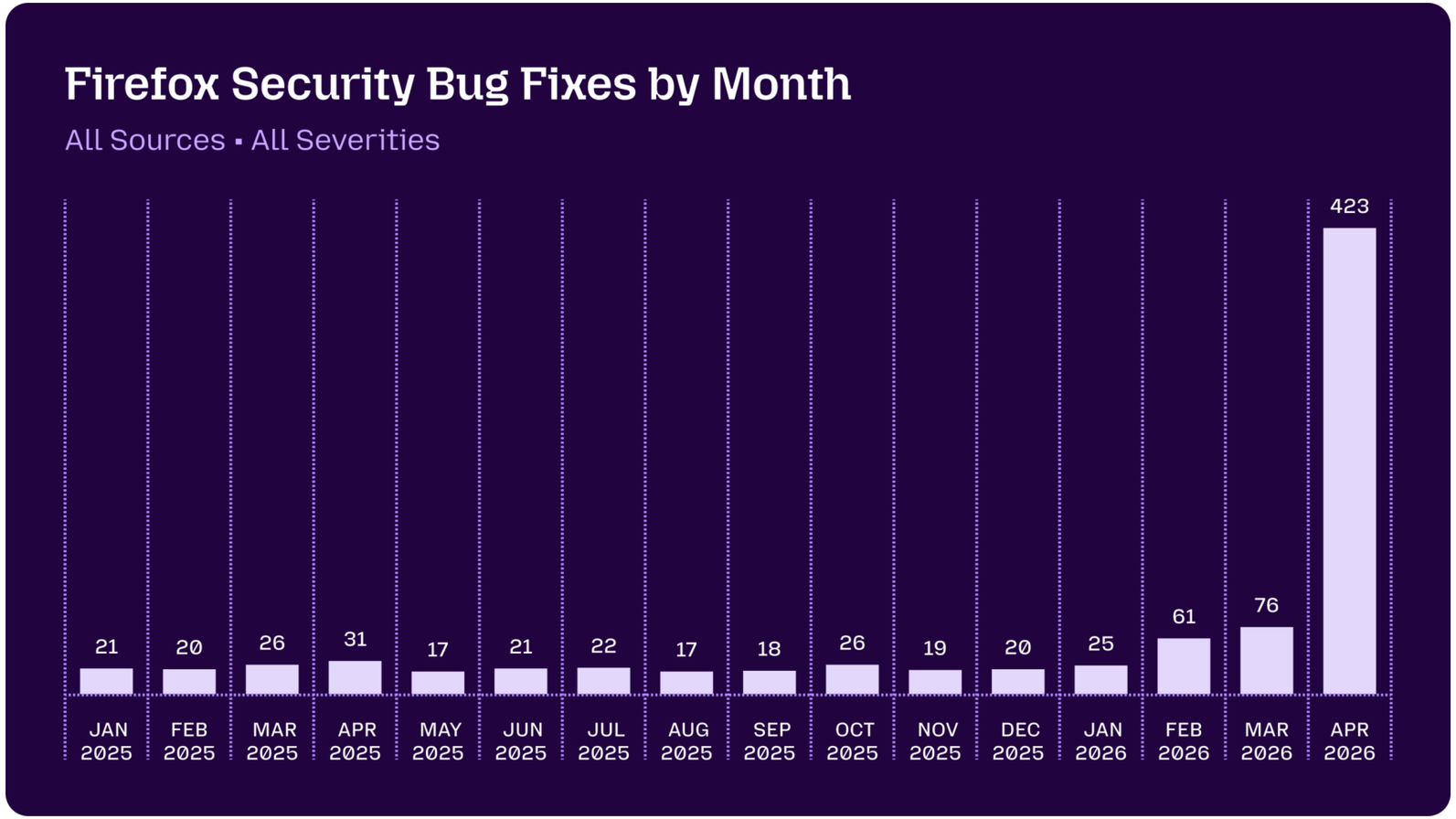


https://www.aisi.gov.uk/blog/our-evaluation-of-openais-gpt-5-5-cyber-capabilities
https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities

Mozilla bestätigt die Ankündigungen von Anthropic zu Mythos

Mozilla – Firefox Team

- Enormer Anstieg an identifizierten Lücken
- Hohe Updatefrequenz
- Überstunden der Entwickler, um diese Lücken zu schließen

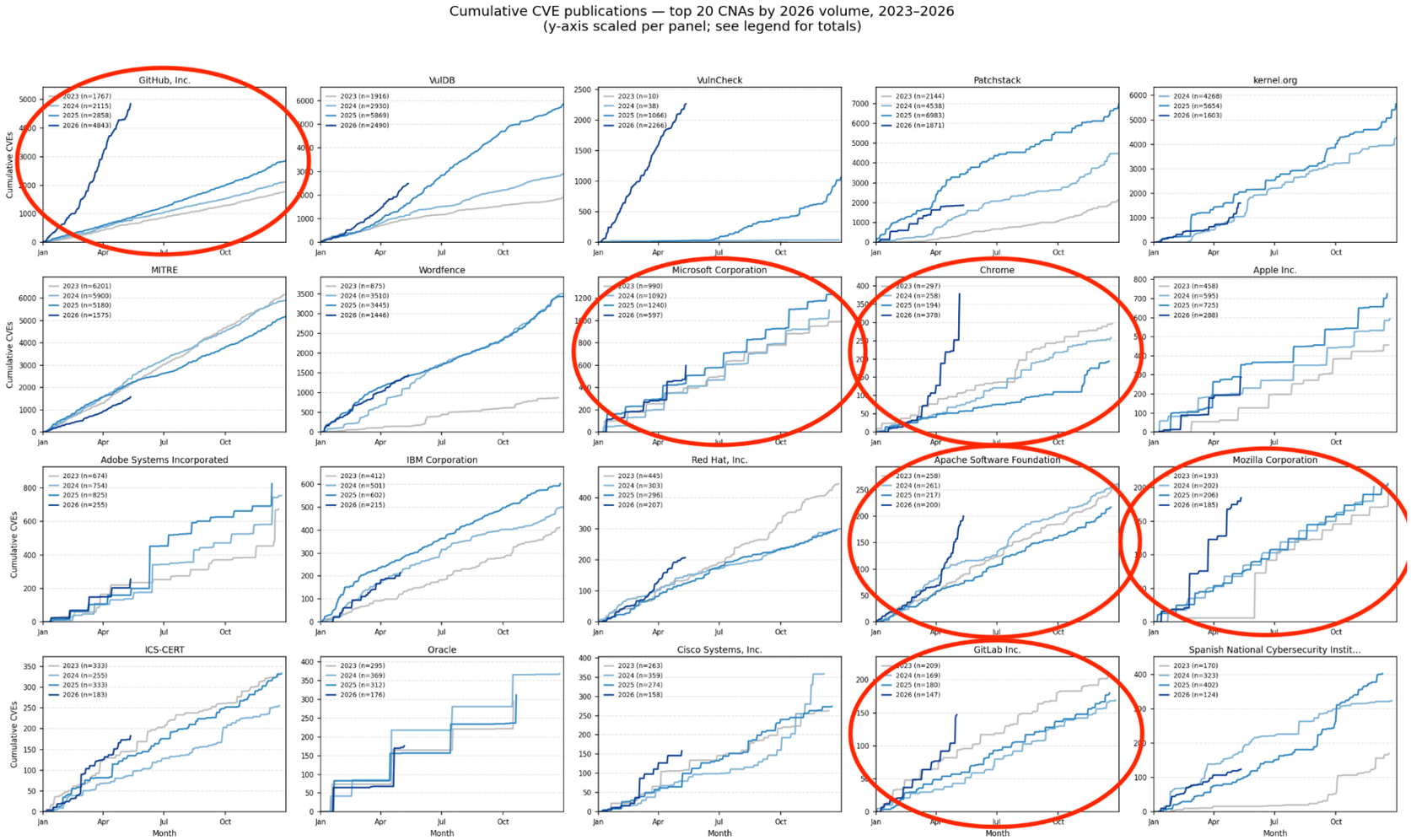


https://hacks.mozilla.org/2026/05/behind-the-scenes-hardening-firefox/

Vulnchek | massiver Anstieg an identifizierten Sicherheitslücken

Vulncheck Analyse:

- KI identifiziert mittlerweile nachvollziehbare, reale Sicherheitslücken
- Das Aufkommen an Sicherheitslücken steigt signifikant, z.B. bei:
  - Chrome + 563,2%
  - VMware + 180,9%
  - Apache + 170,3%
  - F5 + 113,8%
  - GitHub : +476,07%
    (viele Projekte unterschiedlicher Hersteller)



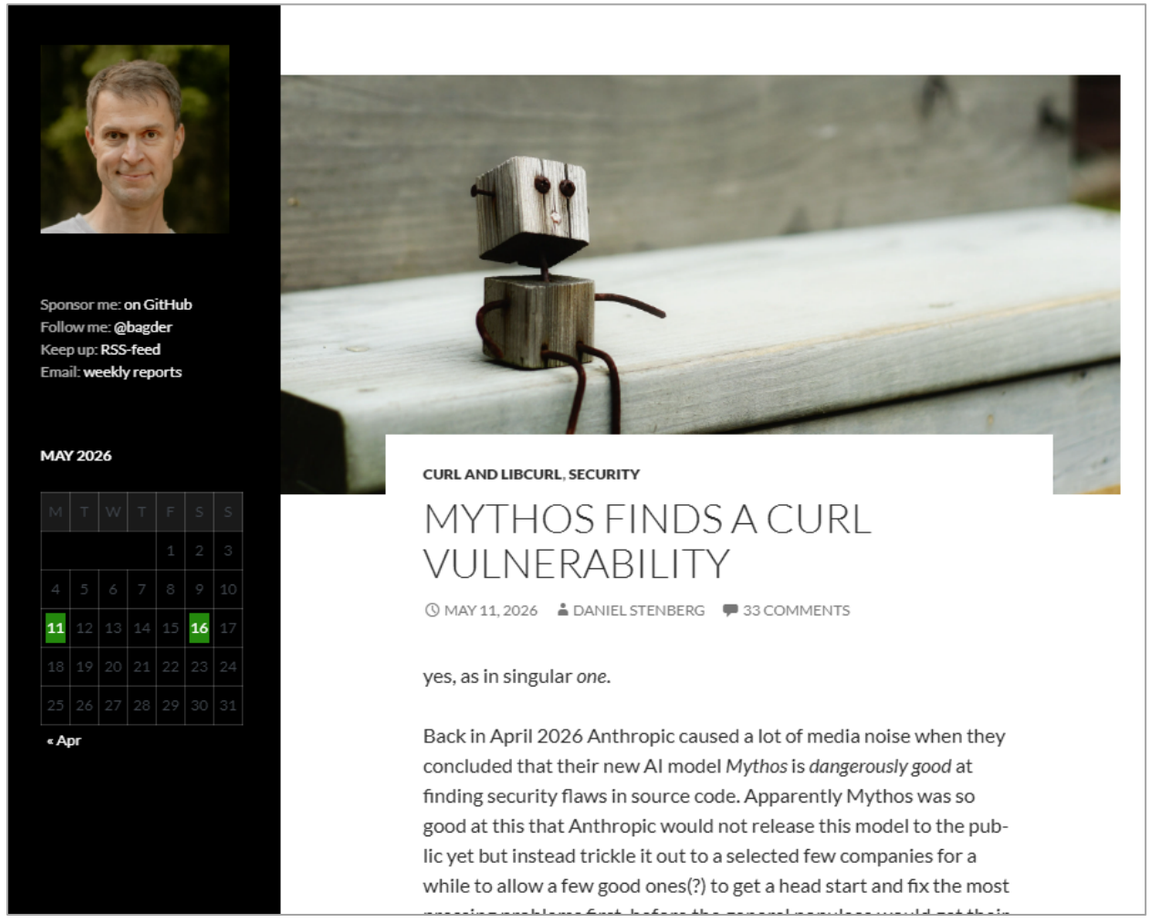
https://www.vulncheck.com/blog/ai-assisted-vulnerability-discovery

CURL | KI-gestütztes Testen verringert Sicherheitslücken

Curl

- Bereits mit KI-Unterstützung getestete Codebasis
- Nur eine einzige zusätzliche Sicherheitslücke identifiziert

→ Konsequente Nutzung der verfügbaren Analysewerkzeuge wirkt.



https://daniel.haxx.se/blog/2026/05/11/mythos-finds-a-curl-vulnerability/

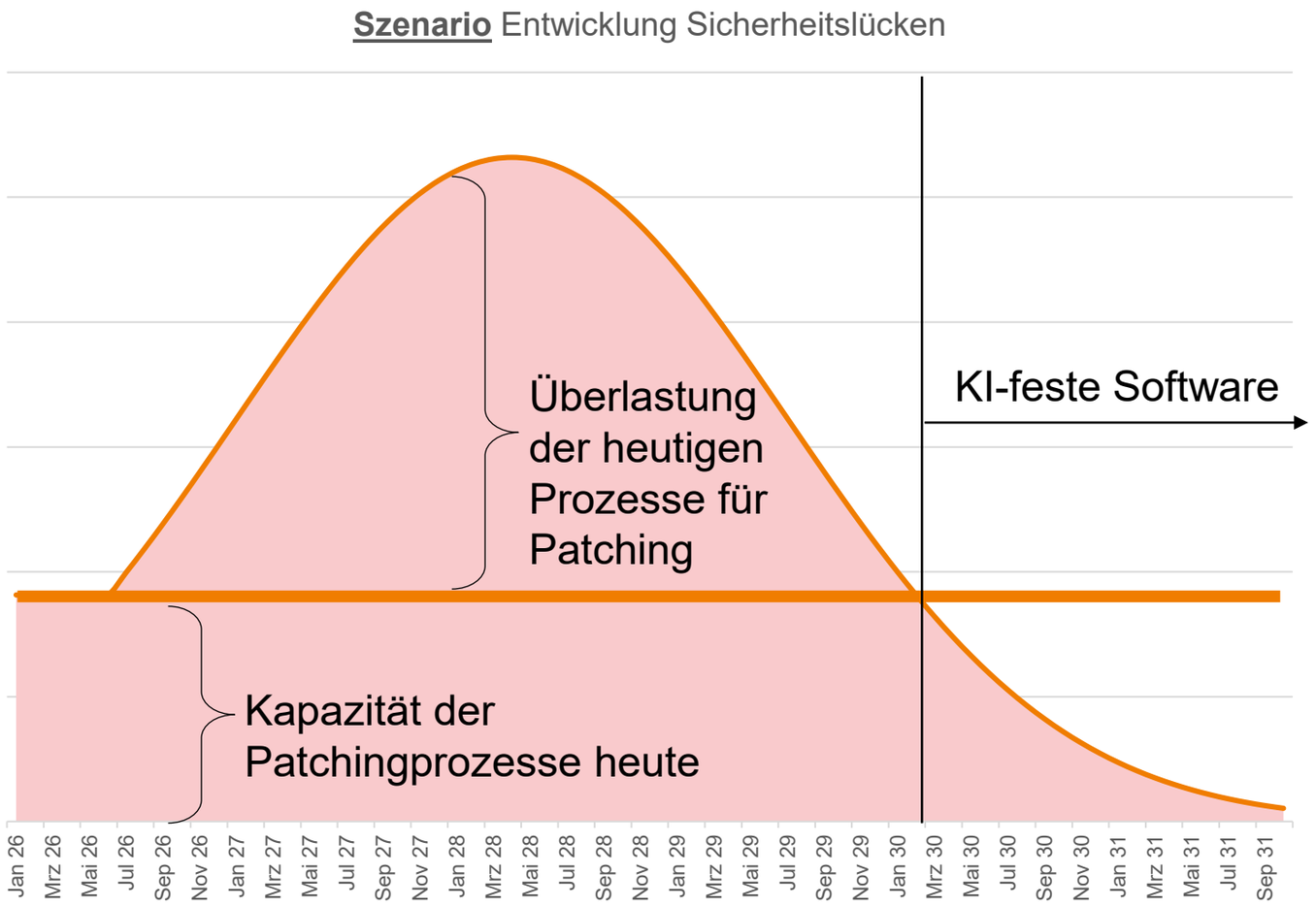
Anmerkung: „Client URL“ (CURL) ist ein weit verbreitetes Open-Source-Kommandozeilen-Tool, mit dem man Daten über das Internet senden und empfangen kann. Es hat geschätzt 30 Milliarden Installationen weltweit.

Erst Überlastung, dann KI-feste Software in der Zukunft?

Szenario zur Entwicklung:

1. In den kommenden Monaten wird es zu einem nochmals deutlichen Anstieg der neu bekanntgewordenen Sicherheitslücken kommen.
2. Diese Belastung wird so lange steigen, bis Softwarelücken schneller geschlossen werden können, als durch KI aufgefunden.
3. Sobald die Bestandssoftware flächendeckend „KI-fest“ geworden ist und neue Software in besserer Qualität ausgeliefert wird, ist sogar ein niedrigeres Niveau als bisher vorstellbar.

Dieser Prozess könnte **Jahre** in Anspruch nehmen, da sämtliche Bestandssoftware überarbeitet werden muss.



Informationsquellen zu Schwachstellen und Cyberrisiken

FMA/OeNB-DORA-Dialog KI-basierte Schwachstellensuche und -ausnutzung

2. Juni 2026

<Wolfgang Rosenkranz, CERT.at>

„Biotop“ Schwachstellenmeldungen

- Prognose: KI wird die Anzahl an Schwachstellenfunden und -meldungen erhöhen
- Was bedeutet „erhöhen“?
  - CVE-Datenbank hat aktuell ca. 335.000 Einträge, davon ca. 50.000 neue Einträge in 2025
    - Ca. 20% mehr als 2024
    - Ca. 30% (also ca. 15.000) mit Schweregrad „hoch“ bis „kritisch“
  - Dringende Schwachstellen-Aussendungen von CERT.at („One-Shot“): 28 (2025)
  - CERT-Warnings (nicht ausschließlich, aber primär Schwachstellen): 15 (2025)
- Erhöhung durch neue KI-Modelle?
  - Angeblich bereits „zehntausende“ neue Schwachstellenfunde durch KI

„Biotop“ Schwachstellenmeldungen

- Wer sammelt diese Schwachstellen bzw. informiert darüber?
  - CVE – Common Vulnerabilities and Exposures (cve.org)
    - Betrieben von der non-profit MITRE Organisation
    - Unterstützt durch CNAs (CVE Numbering Authorities), z.B. SBA Research

Quelle: iisf.ie

  - ENISA EU-Vulnerability Database (euvd.enisa.europa.eu)
  - US CISA (cisa.gov/known-exploited-vulnerabilities-catalog-print)

„Biotop“ Schwachstellenmeldungen

- Wer sammelt diese Schwachstellen bzw. informiert darüber?
  - Shadow Server Foundation (shadowserver.org)
    - Non-profit Organisation, unter anderem finanziert von CERT.at
    - Hauptinformationsquelle für CERT.at-Warnungen
  - Censys (censys.com), Modat (modat.io), LeakIX (leakix.net), Shodan (shodan.io), etc.
  - CERT.at – Scans und Informationskanäle

CERT.at

1. Aussendungen zu Schwachstellen in täglichen und wöchentlichen Newslettern
2. Automatisierte, zielgerichtete Weiterleitung von Meldungen über CERT-IntelMQ (und MISP) – direkt, wenn Kontaktinfos vorhanden
3. Manuell verfasste „One-Shot“-Aussendungen bei Gefahr im Verzug und geringer Anzahl an Betroffenen
4. CERT-Scans des österreichischen Internets, um potenziell Betroffene zu informieren
5. Moderation von Vulnerability Disclosure (CVD) – mit NISG 2026 offiziell

Wie erfährt man von einer eigenen Betroffenheit?

- CERT.at, ein Sicherheitsforscher, Bug Bounty-Dienstleister oder ein Angreifer nimmt Kontakt auf
  - Security.txt oder Kontaktformular für Schwachstellenmeldungen einrichten
- Regelmäßige, aktive Suche in Schwachstellendatenbanken
- Abonnieren eines Service oder Nutzung einer Vulnerabilitäts-Scanning-Software
- Organisieren eines Hackathons, Ausschreiben einer Bug Bounty-Prämie
- Neu: Nutzung von KI-Modellen um die eigene Software zu testen

Nationale CVD-Policy

Alexander Bernard
Bundesministerium für Inneres
Wien, 02. Juni 2026

Was ist Coordinated Vulnerability Disclosure (CVD)?

- **Coordinated Vulnerability Disclosure (CVD)** beschreibt den strukturierten Prozess zur Meldung, Behebung und Veröffentlichung von Schwachstellen
- Ziel ist es, Schwachstellen verantwortungsvoll zu behandeln, bevor sie ausgenutzt oder öffentlich bekannt werden
- Beteiligte Akteure sind:
  - Security Researcher / „Schwachstellensuchende“
  - Anbieterinnen und Anbieter von Produkten mit digitalen Elementen
  - Konsumentinnen und Konsumenten

Warum braucht Österreich eine nationale CVD-Policy?

- Ohne klaren Prozess stellt sich häufig die Frage: **Wer meldet was an wen? Was passiert, wenn die Kommunikation nicht funktioniert? Welche Schritte sind zu befolgen?**

- Die nationale CVD-Policy soll deshalb als Leitfaden klare Meldewege und -Prozesse vorgeben → Vertrauen zwischen Schwachstellensuchenden und Anbieterinnen und Anbietern verbessern

- **Rechtlicher Hintergrund:**
  Die Policy basiert auf europäischen Vorgaben aus **Art. 12 der NIS-2-Richtlinie** und wurde in Österreich durch **§ 11 NISG 2026** umgesetzt

→ **Schaffung der Rolle des Koordinators**

Wie funktioniert die nationale CVD-Policy?

- **Grundprinzipien:** *Verantwortliches Handeln und gute Absichten, Subsidiarität, Verhältnismäßigkeit und Datenschutz, Einhalten des Zeitrahmens & Kommunikation*

- ***Meldung einer Schwachstelle:*** *Identifikation und Verifikation durch Schwachstellensuchende → Überprüfung der Kontaktmöglichkeiten der Anbieterinnen und Anbieter → Meldung → Verifikation und Bewertung der Schwachstelle durch Anbieterinnen und Anbieter → Kontaktaufnahme durch Anbieterinnen und Anbieter → Entwicklung von Folgemaßnahmen → Offenlegung der Schwachstelle durch Anbieterinnen und Anbieter*

- **Rechtliche Information für Einsteiger:** *Unionsrecht, Straf- und zivilrechtliche Aspekte, Datenschutzrecht, etc.*

Die Rolle des Koordinators (unter § 11 NISG 2026)

- *„Das nationale CSIRT hat die Offenlegung von Schwachstellen zu koordinieren“*
- *„Es fungiert dabei als vertrauenswürdiger Vermittler und erleichtert erforderlichenfalls die Interaktion zwischen der eine Schwachstelle meldenden natürlichen oder juristischen Person und dem Hersteller oder Anbieter der potenziell gefährdeten IKT-Produkte oder IKT-Dienste auf **Ersuchen einer der beiden Seiten**“*
- *„Natürliche und juristische Personen können dem nationalen CSIRT eine Schwachstelle auf Wunsch anonym melden“*
- Erste Basis geschaffen → CERT.at - Schwachstelle melden (CVD)

Wie können Anbieterinnen und Anbieter den Prozess unterstützen?

- Eine klare Kontaktmöglichkeit für Schwachstellenmeldungen bereitstellen (z. B. E-Mail-Adresse oder eigene Disclosure-Seite)
- Einen internen Prozess für den Umgang mit Meldungen definieren und den bestenfalls kommunizieren → eine eigene CVD-Policy veröffentlichen
- Folgemaßnahmen möglichst schnell bereitstellen und eine Veröffentlichung unterstützen (CVE ID, etc.)
- Mögliche Anreize/Anerkennungsmöglichkeiten für Schwachstellensuchende setzen (Bug-Bounty-Programme, Hall of Fame, etc.)

Vielen Dank!

Alexander Bernard
Bundesministerium für Inneres
alexander.bernard@bmi.gv.at

Künstliche Intelligenz verändert die Spielregeln – wie Aufsicht und Finanzsektor zusammenwirken

Tugce Aslan, LL.M. (WU)

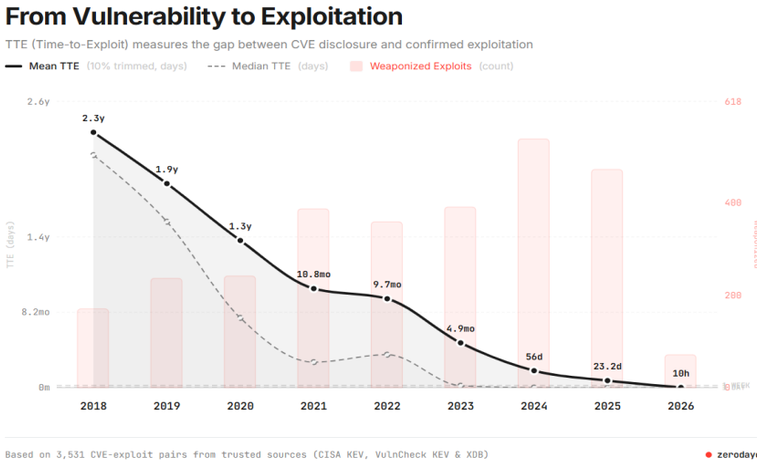
Umgang mit aktuellen Herausforderungen

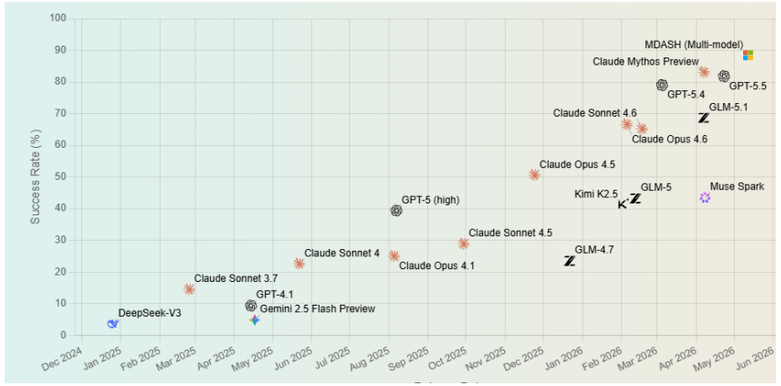
UMGANG MIT AKTUELLEN HERAUSFORDERUNGEN – DIE SITUATION

Moderne LLMs (Mythos, GPT5.5 Cyber, etc.) haben Fähigkeiten, die sowohl Angreifer als auch Verteidiger nutzen können bzw. müssen. Wir reden hierbei nicht von der Zukunft, sondern von heute.

- Moderne LLMs (frontier LLMs) haben die technischen Fähigkeiten innerhalb von wenigen Stunden vollautomatisiert Schwachstellen in Source Code zu identifizieren und somit einen potenziellen Angriffsvektor auf ein Unternehmen auszunutzen.

- Claude Mythos, GPT5.5 Cyber, etc. haben auf der anderen Seite auch die Fähigkeiten Schwachstellen in Source Code vor einem Deployment zu identifizieren und somit Unternehmen zu unterstützen sichere Software zu entwickeln und betreiben.



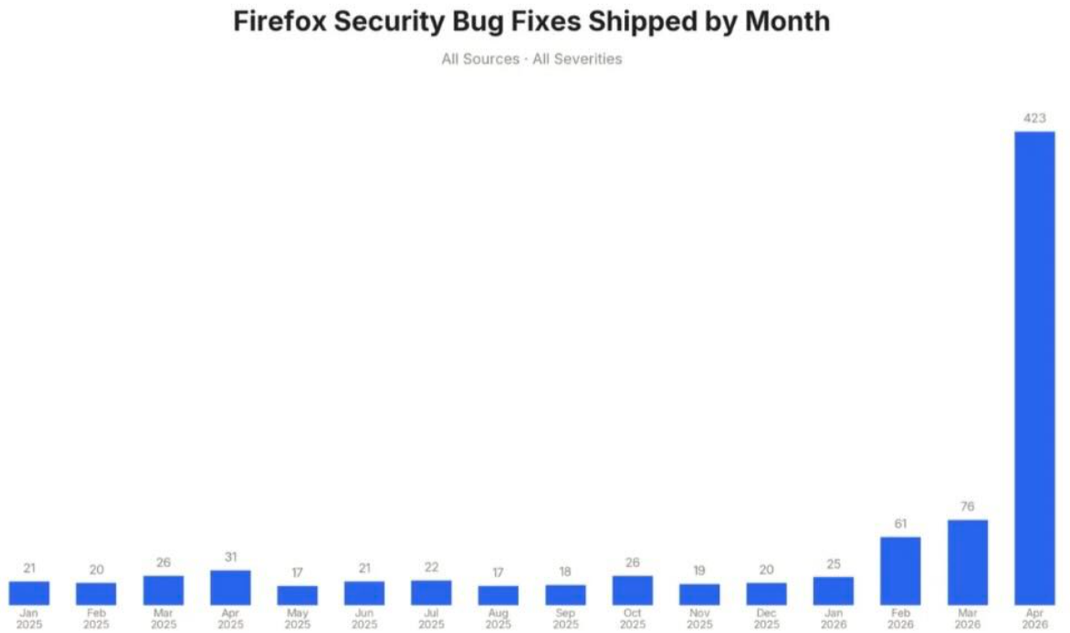


Quellen: Zeroday Clock, Cyber Gym

UMGANG MIT AKTUELLEN HERAUSFORDERUNGEN – DIE VERÄNDERUNG

Durch die Verfügbarkeit von frontier-LLMs und den damit verbundenen Fähigkeiten sehen sich Unternehmen mit einige herausfordernden Veränderungen konfrontiert

- Es gibt bereits eine **massiv ansteigende Zahl an verfügbaren Patches** jener Provider, welche bereits Zugang zu den entsprechenden Modellen haben
- Durch die gestiegene Anzahl an Patches **steigt die Arbeitslast die jeweiligen Produkt- bzw. IT-Teams**
- **Bereits bekannte Schwachstellen, Ergebnisse aus Penetrationstests, Source Code Scans, etc.** einem neuerliche Risikoevaluierung unterziehen, um ein strukturiertes risikobasi Abarbeiten zu definieren und folgend exekutieren. Empfehlens ist mit den extern verfügbaren Systemen zu starten.
- Dem **Management die veränderte Situation bewusst mache** sowie die notwendigen Schritte darlegen
- **Kommunikation an das** komplette **Unternehmen** mitsamt Darlegung der notwendigen Priorisierung



Quelle: Firefox

UMGANG MIT AKTUELLEN HERAUSFORDERUNGEN – DIE NEUE/ALTE BASIS

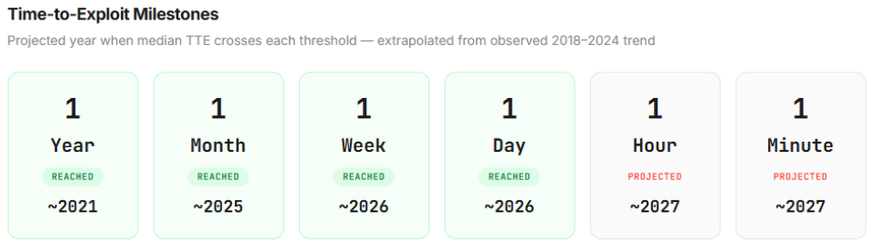
Auch wenn sich die Situation am Markt ändert, ist die wichtigste Grundvoraussetzung weiterhin die Security Basis Hygiene. Diese ist unumgänglich, um den Bedrohungen sowohl vor als auch mit Verfügbarkeit von frontier-LLMs entgegenzutreten und die damit verbundenen Risiken zu minimieren

- Essenziell ist die Wichtigkeit des Themas Security im Unternehmen zu etablieren bzw. daran zu erinnern
- Patching, Patching, Patching
- Identity- und Accessmanagement inklusive Privilege Access Management
- Netzwerksegementierung
- Flächendeckender Einsatz von Multi-Faktor-Authentifizierung (MFA)
- Penetrationtesting und Red-Teaming inklusive Behebung der bekannten Abweichungen
- SAST, DAST, IAST bzw. LLM-unterstütztes Source Code Scanning inklusive Behebung der Abweichungen
- Sicherstellung der Qualität des IT Asset Managements / der CMDB
- Beseitigung von technischen Altlasten und nicht mehr unterstützten Systemen

UMGANG MIT AKTUELLEN HERAUSFORDERUNGEN – WEITERE ERWÄGUNGEN

Neben der Fokussierung auf die Security Basis Hygiene gibt es weitere Themen, welche in Erwägung gezogen werden sollten

- Automatisiertes Software Deployment unter Verwendung von LLMs
- Automatisiertes Testen, sodass Patches rascher (automatisiert) freigegeben werden können
- Verstärkung (und Automatisierung) der Erkennung von Auffälligkeiten (Security Operations Center), da mit einer erhöhten Menge an Angriffen und Alarmen zu rechnen ist
- Regelmäßige Verifizierung von Backup- und Wiederherstellungsmechanismen, sowie Betrachtung der Möglichkeit der Verkürzung der Backupzyklen
- Potentiellen entstehende Interessenkonflikte zwischen Cyber Security and Betriebsstabilität (Operational Resilience) vorzubeugen
- Setzen von weiteren Schritten in Richtung Vollautomatisierung, um weiteren Reduktionen der Zeit bis zur Ausnutzung vorzubeugen



Quelle: Zeroday Clock

Zusammenfassung zu empfohlenen Maßnahmen und Linksammlung

WAS IST NUN ZU TUN?

Herausforderungen:

- Sicherheitslücken werden schneller ausgenutzt
- Patchanzahl und -frequenz steigt
- Softwarehersteller werden nicht immer rechtzeitig Patches liefern
- Betreiber werden Patches nicht immer rechtzeitig einspielen
- Open Source im Fokus der KI-Angreifer
- Closed Source Patches werden schneller reverse-engineered
- **Breaches sind zu erwarten**

Handlungsbedarf kurzfristig:

- Angriffsflächen identifizieren und priorisieren
- Beschleunigung des Schwachstellen- und Patch-Managements
- Verbesserung von Überwachung, Erkennung und aktiver Abwehr
- Stärkung von Governance und Ressourcen für Cybersicherheit
- Absicherung der Lieferkette

Handlungsbedarf langfristig:

- Defense-in-Depth und Cyberhygiene
- Modernisierung der Infrastruktur
- Verbesserung Reaktions- und Wiederherstellungsfähigkeit
- Förderung des Informationsaustauschs (Art. 45 DORA)
- Vorbereitung durch Threat Led Penetration Tests

LINKSAMMLUNG

- FMA Aktivitäten zu DORA: https://www.fma.gv.at/querschnittsthemen/dora/fma-aktivitaeten-zu-dora/
- Nationale CVD-Policy: https://www.bmi.gv.at/504/files/nationale-cvd-policy-bf.pdf
- Neue Schwachstelle melden: https://www.cert.at/de/services/schwachstelle-melden/

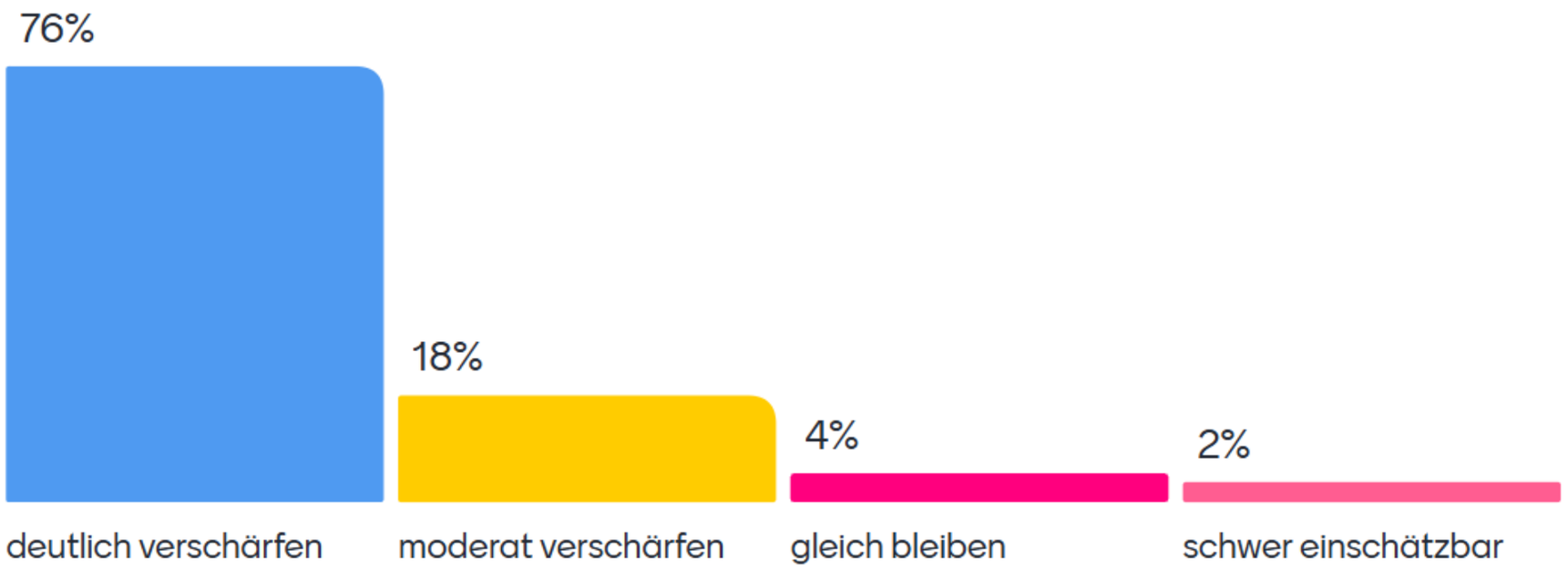
- GPT 5-5-Cyber Test: https://www.aisi.gov.uk/blog/our-evaluation-of-openais-gpt-5-5-cyber-capabilities
- Mythos Test: https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities
- Beschreibung der AISI Testumgebung: https://arxiv.org/abs/2603.11214

- Verkürzung des Zeitfensters zwischen Schwachstellenerkennung und Exploit: https://zerodayclock.com/
- Cybersecurity Evaluierung von KI-Agenten: https://www.cybergym.io/

- Mozilla Erfahrung mit Mythos: https://hacks.mozilla.org/2026/05/behind-the-scenes-hardening-firefox/
- CURL Erfahrung mit Mythos: https://daniel.haxx.se/blog/2026/05/11/mythos-finds-a-curl-vulnerability/

Umfrage

Wie wird sich Ihrer Einschätzung nach die Cyber-Bedrohungslage durch KI im nächsten Jahr entwickeln?



menti.com
8954 1387

130 of 135 responded

Aktuelle Informationen & Ausblick

AKTUELLE DORA-INFORMATIONEN & AUSBLICK

DORA-Vorfälle:

- ESA-Bericht in anonymisierter und aggregierter Form über schwerwiegende IKT-bezogene Vorfälle (Art 22 Abs 2 DORA): Veröffentlichung in Kürze erwartet
- Anweisungen zur Befüllung der Meldevorlagen in Erstellung

Meldung Informationsregister 2027:

- Gs. soll der Prozessdurchlauf von 2026 beibehalten werden, dh
  - Stichtag, auf den sich die Meldung bezieht ist der 31.12.2026
  - Meldung an FMA bis zum 31.3.2027

Stichprobe zur Strategie für das IKT-Drittparteienrisiko & Ausstiegsplan:

- Frist zur Einmeldung der Dokumente 29.5.2026 ⇨ Analysebeginn
- Feedback im Herbst / Winter dJ

DORA & NIS2:

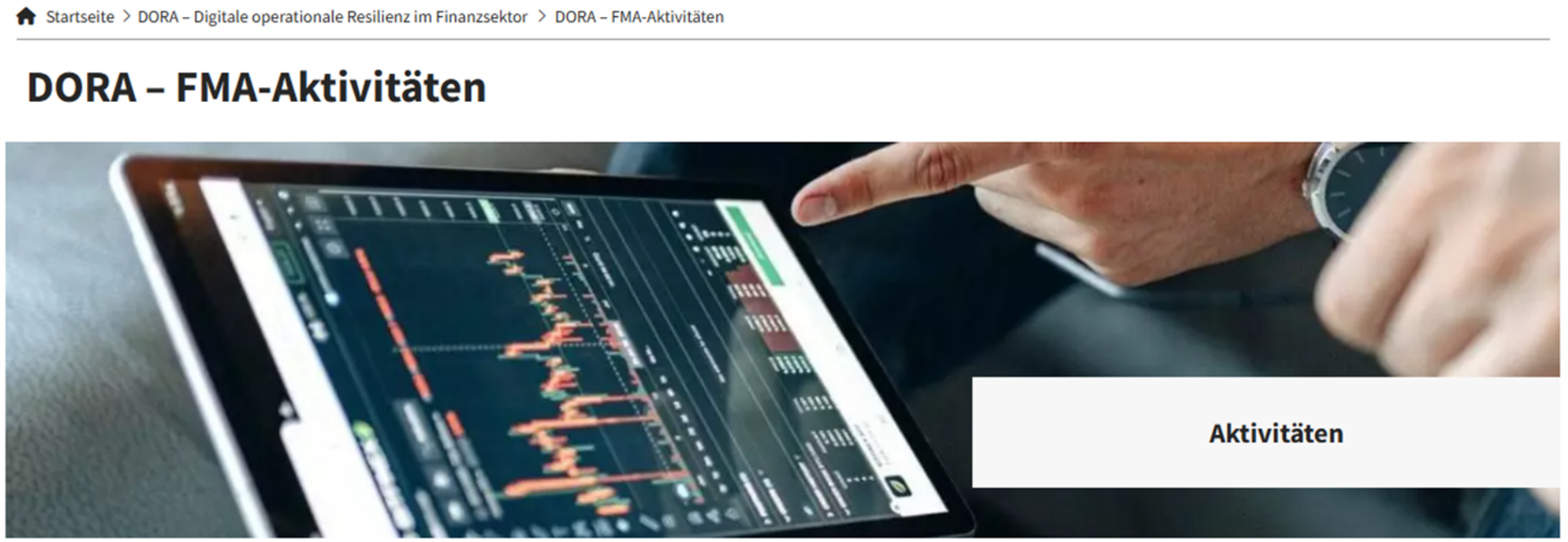
- Informationen zum Verhältnis zwischen DORA und NIS2/NISG 2026 für Finanzunternehmen https://www.fma.gv.at/querschnittsthemen/dora/fma-aktivitaeten-zu-dora/

FMA/OeNB-DORA-Dialog

- Plan des nächsten Dialogs für Anfang September 2026
  Fokus: Überwachungsrahmen für kritische IKT-Drittdienstleister

DIALOGUNTERLAGEN

https://www.fma.gv.at/querschnittsthemen/dora/fma-aktivitaeten-zu-dora/



Veröffentlichung der Dialogunterlagen auf der FMA-DORA-Website

FINANZMARKTAUFSICHT ÖSTERREICH

Kompetenz Kontrolle Konsequenz

OESTERREICHISCHE NATIONALBANK

EUROSYSTEM