



Kommission legt EU-Aktionsplan für Cybersicherheit und künstliche Intelligenz vor

Strasbourg, 7. Juli 2026

Die Europäische Kommission hat einen Aktionsplan für eine strukturierte Reaktion vorgelegt, um den Risiken zu begegnen und die Chancen fortgeschrittener Modelle der künstlichen Intelligenz (KI) für die Cybersicherheit zu nutzen.

Mithilfe neuer fortgeschrittener KI-Modelle wird die Cybersicherheit neu definiert. KI kann missbraucht werden, um Schwachstellen zu finden, Angriffe zu automatisieren und das Ausmaß und das Tempo von Cybersicherheitsvorfällen in beispielloser Geschwindigkeit zu steigern.

Aufbauend auf dem einzigartigen EU-Rechtsrahmen für KI und Cybersicherheit wird der Aktionsplan die Mitgliedstaaten, die Industrie und Organisationen auf EU-Ebene an einen Tisch bringen, um die Cybersicherheit unserer digitalen Landschaft angesichts der Schwachstellen, die infolge fortgeschrittener KI sichtbar werden, zu stärken.

Bewertung von KI-Modellen

Eine wirksame Sicherheit erfordert ein gründliches Verständnis dessen, wie neue Technologien eingesetzt, missbraucht und ausgenutzt werden können. Nach der [KI-Verordnung](#) müssen fortgeschrittene KI-Modelle bewertet und Risikominderungsmaßnahmen sorgfältig geprüft werden, bevor die Modelle in der EU in Verkehr gebracht werden dürfen.

Um heimische Sachkenntnis zu fördern, wird die Kommission eine gezielte Aufforderung zur Einreichung von Vorschlägen zur Einrichtung einer EU-Evaluierungskapazität für Cybersicherheit veröffentlichen, die voraussichtlich 2027 einsatzbereit sein wird. Diese neue Kapazität wird zur Regulierungsfunktion des KI-Büros beitragen und die Bewertung der KI-Fähigkeiten und -Risiken durch Dritte weltweit stärken.

Zugang zu fortgeschrittenen KI-Modellen

Europa braucht außerdem klare und transparente Bedingungen für den Zugang zu den fortgeschrittensten KI-Systemen.

Die Kommission wird mit der Agentur der Europäischen Union für Cybersicherheit ([ENISA](#)) zusammenarbeiten, um einen europäischen Konzeptentwurf für den strukturierten Zugang zu fortgeschrittenen KI-Fähigkeiten für die Cybersicherheit festzulegen. Diese Anleitung wird einschlägigen europäischen öffentlichen und privaten Organisationen dabei helfen, Zugang zu fortgeschrittenen KI-Modellen zu erhalten.

Testen von KI für Cybersicherheit

Die ENISA und die [Gemeinsame Forschungsstelle](#) der Kommission werden eine sichere Plattform für das Testen von KI für die Cybersicherheit aufbauen, auch mit simulierten Umgebungen. Dadurch werden die Akteure in kritischen Sektoren wie Finanzwesen, Energie, Gesundheit, Verkehr und öffentliche Verwaltung wichtige Kenntnisse über die sichere Nutzung von KI erlangen.

Stärkung der Cybersicherheit der EU und Beseitigung von Schwachstellen

Die EU muss ihre kritischen Infrastrukturen vor den Schwachstellen schützen, die sich aus dem potenziellen Missbrauch dieser Technologien ergeben.

Wie in den Cybersicherheitsvorschriften der EU vorgesehen, sollten alle Organisationen ihre Cyberhygienepraktiken, ihre Risikomanagementmaßnahmen und die Grundsätze der Sicherheit durch Technikgestaltung verstärkt anwenden.

Organisationen sollten damit beginnen, bereits vorhandene KI-Fähigkeiten, auch in Form quelloffener Modelle, zu nutzen, um Schwachstellen schneller zu erkennen und zu beheben sowie Cyberangriffe zu verhindern und darauf zu reagieren.

Zur Unterstützung der Organisationen bei diesem Übergang wird die ENISA Partnerschaften zwischen Behörden, Unternehmen und Open-Source-Gemeinschaften im Cyberökosystem fördern und erleichtern. Dazu gehören Anleitungen, Empfehlungen und bewährte Verfahren sowie eine Kampagne zur Beschaffung kritischer quelloffener Software.

Ausbau der europäischen KI-Fähigkeiten im Cyberbereich

Um das Wachstum des europäischen Marktes zu fördern, wird die Kommission die Große Herausforderung der EU für „KI für Cybersicherheit“ auf den Weg bringen. Diese Ausschreibung wird Unternehmen, Forschende und Organisationen zusammenbringen, damit sie KI-Lösungen für die Cybersicherheit entwickeln.

Zudem muss die EU weiterhin in die Entwicklung ihrer eigenen souveränen fortgeschrittenen KI-Fähigkeiten investieren und kann sich dabei auf die von den [KI-Fabriken und künftigen Gigafabriken](#) bereitgestellte Infrastruktur stützen. In diesem Zusammenhang könnte die im [Paket zur technologischen Souveränität](#) angekündigte künftige europäische Technologie-Eigenkapitalkapazität private Investitionen mobilisieren, um heimische KI-Kapazitäten auszubauen.

Hintergrund

Die EU verfügt über einen geeigneten Rechtsrahmen, mit dem sie Fragen der Cybersicherheit im Zeitalter neu entstehender Technologien wie KI gut angehen kann. Nach der KI-Verordnung müssen die von KI-Modellen ausgehenden Risiken bewertet und gemindert werden. Diese Anforderungen werden im [Praxisleitfaden für KI mit allgemeinem Verwendungszweck](#) weiter präzisiert, um den Anbietern fortgeschrittener Modelle die Einhaltung der Vorschriften zu erleichtern. Diese Bestimmungen werden ab dem 2. August 2026 durchgesetzt.

Die [Cyberresilienzverordnung](#), die Ende 2027 in Kraft treten soll, schreibt die Sicherheit durch Technikgestaltung für alle Hardware- und Softwareprodukte vor. Zusammen mit der [Verordnung über die digitale operationale Resilienz für den Finanzsektor](#) (DORA) zielt die [Richtlinie über die Sicherheit von Netz- und Informationssystemen](#) (NIS-2-Richtlinie) darauf ab, die Sicherheit kritischer Sektoren wie Verkehr und Energie zu erhöhen. Mit der [Cybersolidaritätsverordnung](#) werden die Kapazitäten in der EU zur Erkennung von, Vorsorge für und Bewältigung von schwerwiegenden Cybersicherheitsbedrohungen und -angriffen sowie solchen großen Ausmaßes gestärkt.

Weitere Informationen

[EU-Aktionsplan für Cybersicherheit und künstliche Intelligenz](#)

[Factsheet](#)

IP/26/1544

Zitate:

"KI ändert von Grund auf, was Cybersicherheit bedeutet. Da müssen wir Schritt halten. Die EU verfügt über ein solides Fundament, um auf Schwachstellen, die neue Technologien mit sich bringen, angemessen zu reagieren. Wir müssen bestehende Fähigkeiten, Netze und den Rechtsrahmen nutzen und ausrichten, um die Cybersicherheit zum Schutz unserer digitalen Landschaft zu stärken."
Henna Virkkunen, Exekutiv-Vizepräsidentin für technologische Souveränität, Sicherheit und Demokratie - 07/07/2026

Kontakt für die Medien:

[Thomas REGNIER](#) (+32 2 29 91099)
[Patricia POROPAT](#) (+32 2 29 80485)

Kontakt für die Öffentlichkeit: [Europe Direct](#) – telefonisch unter [00 800 67 89 10 11](#) oder per [E-Mail](#)

Medien zum Thema



[Press conference of Henna Virkkunen, Executive Vice-President of the European Commission, on the Action Plan on cybersecurity and AI](#)