



Kommission stärkt Resilienz und Kapazitäten der EU im Bereich der Cybersicherheit

Strasbourg, 20. Januar 2026

Europa ist täglich Cyberangriffen und hybriden Angriffen auf wesentliche Dienste und demokratische Institutionen ausgesetzt, die von erfahrenen staatlichen und kriminellen Gruppen verübt werden. Angesichts dieser wachsenden Bedrohungen hat die Europäische Kommission heute ein **neues Cybersicherheitspaket** vorgeschlagen, um die Resilienz und die Kapazitäten der EU im Bereich der Cybersicherheit weiter zu stärken.

Das Paket umfasst einen Vorschlag für eine **überarbeitete Cybersicherheitsverordnung**, mit der die Sicherheit der EU-Lieferketten im Bereich der Informations- und Kommunikationstechnik (IKT) verbessert wird. So soll durch ein einfacheres Zertifizierungsverfahren sichergestellt werden, dass Produkte, die die EU-Bürgerinnen und -Bürger erreichen, von vornherein cybersicher sind. Der Vorschlag erleichtert auch die Einhaltung der bestehenden EU-Cybersicherheitsvorschriften und stärkt die Rolle der Agentur der Europäischen Union für Cybersicherheit (ENISA) im Hinblick auf die Unterstützung der Mitgliedstaaten und der EU beim Umgang mit Cybersicherheitsbedrohungen.

Stärkung der Sicherheit der IKT-Lieferketten in der EU

Die neue Cybersicherheitsverordnung soll die Risiken in der IKT-Lieferkette der EU verringern, die von Lieferanten aus Drittländern ausgehen, bei denen Bedenken hinsichtlich der Cybersicherheit bestehen. Damit wird ein vertrauenswürdiger Rahmen für die Sicherheit der IKT-Lieferkette festgelegt, der auf einem harmonisierten, verhältnismäßigen und risikobasierten Ansatz beruht. Dies wird es der EU und den Mitgliedstaaten ermöglichen, Risiken in den 18 kritischen Sektoren der EU gemeinsam zu ermitteln und zu mindern, wobei auch die wirtschaftlichen Auswirkungen und das Marktangebot berücksichtigt werden.

Die jüngsten Cybersicherheitsvorfälle haben die großen Risiken deutlich gemacht, die von Schwachstellen in den für das Funktionieren kritischer Dienste und Infrastrukturen unerlässlichen IKT-Lieferketten ausgehen. In der heutigen geopolitischen Landschaft geht es bei der Sicherheit der Lieferketten nicht mehr nur um die Sicherheit technischer Produkte oder Dienste, sondern auch um Risiken im Zusammenhang mit Lieferanten, insbesondere um Abhängigkeiten und Einflussnahme aus dem Ausland.

Die neue Cybersicherheitsverordnung wird die obligatorische Minderung der von Hochrisikoanbietern aus Drittländern ausgehenden Risiken für die europäischen Mobilfunknetze ermöglichen und auf den Arbeiten aufbauen, die bereits im Rahmen des [Instrumentariums für die 5G-Sicherheit](#) durchgeführt wurden.

Vereinfachung und Erweiterung des europäischen Rahmens für die Cybersicherheitszertifizierung

Mit der überarbeiteten Cybersicherheitsverordnung wird sichergestellt, dass Produkte und Dienste, die die Verbraucherinnen und Verbraucher in der EU erreichen, effizienter auf ihre Sicherheit geprüft werden. Dies wird durch einen erneuerten europäischen Rahmen für die Cybersicherheitszertifizierung (ECCF) erfolgen. Der ECCF wird für mehr Klarheit und einfachere Verfahren sorgen, sodass Zertifizierungssysteme standardmäßig innerhalb von 12 Monaten entwickelt werden können. Außerdem wird eine flexiblere und transparentere Governance eingeführt, um die Interessenträger durch Information und Konsultation der Öffentlichkeit besser einzubeziehen.

Zertifizierungssysteme, die von der ENISA verwaltet werden, werden zu einem praktischen, freiwilligen Instrument für Unternehmen, mit dessen Hilfe sie die Einhaltung der EU-Rechtsvorschriften nachweisen und so den Aufwand und die Kosten verringern können. Neben IKT-

Produkten, -Diensten und -Prozessen sowie verwalteten Sicherheitsdiensten werden Unternehmen und Organisationen in der Lage sein, ihre Cyberabwehr zertifizieren zu lassen, um dem Marktbedarf gerecht zu werden. Letztlich wird der erneuerte ECCF einen Wettbewerbsvorteil für EU-Unternehmen darstellen. Für Bürgerinnen und Bürger, Unternehmen und Behörden in der EU wird er ein hohes Maß an Sicherheit und Vertrauen in komplexe IKT-Lieferketten gewährleisten.

Einfachere Einhaltung der Cybersicherheitsvorschriften

Das Paket enthält Maßnahmen zur Vereinfachung der Einhaltung der EU-Cybersicherheitsvorschriften und Risikomanagementanforderungen für in der EU tätige Unternehmen, die die in der Digital-Omnibus-Verordnung vorgeschlagene [zentrale Anlaufstelle zur Meldung von Vorfällen](#) ergänzen. Mit gezielten Änderungen der NIS-2-Richtlinie soll die Rechtsklarheit erhöht werden. Dies wird 28 700 Unternehmen, darunter 6 200 Kleinst- und Kleinunternehmen, die Einhaltung der Vorschriften erleichtern. Außerdem wird eine neue Kategorie kleiner Midcap-Unternehmen eingeführt, um die Befolgungskosten für 22 500 Unternehmen zu senken. Die Änderungen werden die Zuständigkeiten vereinfachen, die Erhebung von Daten über Ransomware-Angriffe straffen und die Beaufsichtigung grenzüberschreitend tätiger Einrichtungen dank der verstärkten Koordinierungsrolle der ENISA erleichtern.

Ermächtigung der ENISA zur Stärkung der Resilienz Europas im Bereich der Cybersicherheit

Seit der Annahme des ersten Rechtsakts zur Cybersicherheit im Jahr 2019 ist die ENISA zu einem Eckpfeiler des Cybersicherheitsökosystems der EU geworden. Gestützt auf die heute vorgelegte überarbeitete Cybersicherheitsverordnung kann die ENISA der EU und ihren Mitgliedstaaten künftig besser dabei helfen, die gemeinsamen Bedrohungen zu erfassen. Sie ermöglicht es ihnen auch, sich auf Cyberverfälle vorzubereiten und darauf zu reagieren.

Die Agentur wird Unternehmen und Interessenträger, die in der EU tätig sind, weiter unterstützen, indem sie frühzeitig vor Cyberbedrohungen und -vorfällen warnt. In Zusammenarbeit mit Europol und den [Computer-Notfallteams](#) wird sie Unternehmen helfen, auf Ransomware-Angriffe zu reagieren und sich von ihnen zu erholen. Darüber hinaus wird die ENISA ein Unionskonzept entwickeln, um den Interessenträgern bessere Dienste für das Schwachstellenmanagement zur Verfügung zu stellen. Sie wird die zentrale Anlaufstelle zur Meldung von Sicherheitsvorfällen betreiben, die mit der [Digital-Omnibus-Verordnung](#) vorgeschlagen wird.

Die ENISA wird nach wie vor eine Schlüsselrolle beim weiteren Aufbau einer qualifizierten Arbeitskräftebasis im Bereich der Cybersicherheit in Europa spielen. Dazu wird sie die Akademie für Cybersicherheitskompetenzen als Pilotinitiative fortführen und EU-weite Systeme zur Bescheinigung von Cybersicherheitskompetenzen einrichten.

Nächste Schritte

Die neue Cybersicherheitsverordnung wird unmittelbar nach der Annahme durch das Europäische Parlament und den Rat der EU in Kraft treten. Die begleitenden Änderungen der NIS-2-Richtlinie werden ebenfalls zur Annahme vorgelegt. Nach deren Annahme haben die Mitgliedstaaten ein Jahr Zeit, um die Richtlinie in nationales Recht umzusetzen und der Kommission ihre Umsetzungsvorschriften zu übermitteln.

Weitere Informationen

[Fragen und Antworten](#)

[Factsheet](#)

[Überarbeitete Cybersicherheitsverordnung](#)

[Gezielte Änderungen der NIS-2-Richtlinie](#)

"Cybersicherheitsbedrohungen sind nicht nur technische Herausforderungen. Sie stellen strategische Risiken für unsere Demokratie, Wirtschaft und Lebensweise dar. Dank des neuen Cybersicherheitspakets werden wir über die Mittel verfügen, um unsere kritischen IKT-Lieferketten besser zu schützen und um Cyberangriffen entschlossen zu begegnen. Dies ist ein wichtiger Schritt zur Sicherung der technologischen Souveränität Europas und zur Gewährleistung einer größeren Sicherheit für alle."
Henna Virkkunen, Exekutiv-Vizepräsidentin für technologische Souveränität, Sicherheit und Demokratie - 20/01/2026

Kontakt für die Medien:

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

[Nika BLAZEVIC](#) (+32 2 29 92717)

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

Medien zum Thema



[College read-out / press conference by Henna Virkkunen, Executive Vice-President of the European Commission, on the Cybersecurity Act](#)