kaspersky

# Hohes Schutzniveau und Resilienz gegen Cyberangriffe, effektiver Kampf gegen Cyberkriminalität, Stärkung von Cybersecurity-Awareness und Know-how.

***Impulse von Kaspersky für die Cybersicherheitspolitik in den kommenden vier Jahren***

*Trotz gestärkter Resilienz beschreibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Lage der IT-Sicherheit in Deutschland in seinem Bericht vom November 2024 als angespannt – vor allem mit Blick auf Ransomware-Angriffe, Cyberkriminalität, Cybersabotage und Cyberspionage. Kaspersky-Daten bestätigen die verschärfte Bedrohungslage in der Bundesrepublik: So zeigt eine Kaspersky-Studie vom Oktober 2024, dass über die Hälfte der Unternehmen in Deutschland (60 Prozent) mit mehr Cyberangriffen in den vergangenen 12 Monaten zu kämpfen hatte.*

*Kaspersky ist der Auffassung, dass die Stärkung von Cybersicherheit und Resilienz eine gemeinschaftliche Aufgabe und Verantwortung von Politik, Verwaltung, Wirtschaft, Wissenschaft und Zivilgesellschaft ist. Deswegen sollte ein kooperativer Ansatz bei der Planung und Umsetzung der Cybersicherheitspolitik verfolgt werden. Gleichzeitig gilt es, die Steigerung von Cybersicherheit und Resilienz in den kommenden Jahren zu einem politischen Schwerpunkt zu machen.*

## 1. Der Mensch steht im Mittelpunkt: Cybersecurity-Awareness und Know-how nachhaltig steigern

Wenn es um die Steigerung der Resilienz geht, sollte ein besonderes Augenmerk auf den Menschen gelegt werden. Eine Kaspersky-Studie hat gezeigt, dass 61 Prozent aller Cybersicherheitsvorfälle zwischen 2021 und 2023 in Unternehmen in Deutschland durch menschliches Fehlverhalten verursacht wurden. Entsprechend sollten das Bewusstsein für Cyberbedrohungen umfassend geschärft und Wissen sowie Fähigkeiten in der Cybersicherheit zielgerichtet entwickelt werden.

Zugleich bedarf es einer verbesserten Kooperation zwischen Bildungseinrichtungen, der Industrie und dem öffentlichen Sektor, ergänzt durch die gezielte Förderung von Cybersicherheits-Schulungsmaßnahmen und insbesondere im Hinblick auf die Bedürfnisse von KMU. Frauen sollten ermutigt werden, Rollen und Verantwortung in der Cybersicherheit – einem bislang besonders männerdominierten Berufsfeld – zu übernehmen.

Angesichts zunehmend komplexer Cyberbedrohungen stehen viele Unternehmen vor der Herausforderung, leistungsfähige und gut organisierte Cybersicherheitsteams aufzubauen. Für die qualitative und bedarfsorientierte Verbesserung der notwendigen Kompetenzen sind koordinierte und langfristige Maßnahmen erforderlich. Zum einen erscheinen bildungspolitische Reformen sinnvoll. So sollten Informatik als Pflichtfach in die Lehrpläne der Schulen integriert werden und die Zahl der Informatik- und Cybersicherheitslehrstühle an Universitäten ausgebaut werden. Der Zugang von Quereinsteigern zum Berufsfeld – auch im öffentlichen Dienst – muss erleichtert werden.

## 2. EU-Cybersicherheitsregularien kooperativ und europaweit koordiniert umsetzen

Um im gesamten EU-Binnenmarkt ein einheitlich hohes Maß an Cybersicherheit zu erreichen und die Resilienz gegen Cyberkriminalität signifikant zu erhöhen, bedarf es über alle Mitgliedstaaten hinweg einer abgestimmten und möglichst einheitlichen Umsetzung der EU-Digitalgesetzgebung, wie beispielsweise der NIS2-Richtlinie. Hierfür sollte sich Deutschland einsetzen.

Die Bundesrepublik muss zudem zeitnah einen klaren regulatorischen Rahmen schaffen. Unsicherheiten mit Blick auf die Betroffenheit, insbesondere bei international agierenden Unternehmen mit breitem Produktportfolio, müssen im Umsetzungsgesetz geklärt werden. Das BSI sollte einen kooperativen Austausch mit allen betroffenen Unternehmen führen, um die Cybersicherheit übergreifend zu fördern, das Cyber-Lagebild nachhaltig zu verbessern und Synergien zu erzielen.

### 3. Transparenz und Vertrauenswürdigkeit von Cybersicherheitslösungen und Anbietern stärken

Insbesondere der Cyber Resilience Act der EU beinhaltet zahlreiche Transparenzbestimmungen für Produkte, Dienstleistungen und Unternehmen. Für ein Höchstmaß an Sicherheit sollten Politik und Verwaltung an Anbieter von Cybersicherheitslösungen umfangreichere Transparenzanforderungen stellen, die die Vertrauenswürdigkeit des Anbieters belegen. Hierzu zählen externe Prüfungen, z. B. von Quellcodes oder der Sicherheit der Software-/Hardware-Entwicklungsprozesse, ein koordiniertes Schwachstellenmanagement sowie Audits und Zertifizierungen nach internationalen Standards. Kaspersky hat mit der Globalen Transparenzinitiative zahlreiche Maßnahmen entwickelt und umgesetzt und teilt die gemachten Erfahrungen gern mit interessierten Stakeholdern.

### 4. Zusammenarbeit im Cybersicherheits-Ökosystem stärken und fördern

Fundierte Informationen und verlässliche Angriffs- und Erkennungsdaten sind in der Cybersicherheit von essenzieller Bedeutung. Denn wirkungsvolle Schutzmaßnahmen lassen sich nur auf Basis der genauen Kenntnis der Cyberlandschaft ergreifen. Vor diesem Hintergrund ist der Informationsaustausch zwischen allen Akteuren, die Beiträge zur Stärkung von Cybersicherheit und Resilienz leisten können, besonders wichtig und sollte politisch unterstützt werden. Die koordinierte und vertrauensvolle Offenlegung von Schwachstellen muss weiter gefördert werden, auch über die bestehenden europäischen Cybersicherheitsregularien hinaus. Nationale Initiativen sollten, wenn möglich, internationalisiert und auf europäischer Ebene konsolidiert werden, um Synergien nutzbar zu machen. Öffentlich-private Partnerschaften (PPP) sollten gefördert werden, um konkrete Maßnahmen zum Schutz vor Cyberbedrohungen sowie zur Steigerung von Awareness zu entwickeln.

Die sorgfältige Analyse neuer Technologien und ihrer potenziellen Auswirkungen auf die Cybersicherheit ist von entscheidender Bedeutung für die Wirksamkeit künftiger politischer und regulatorischer Maßnahmen. Mit Blick auf eine adäquate Risikoanalyse und die Entwicklung von Schutzstrategien sollte die Politik in Zusammenarbeit mit Wirtschaft und Wissenschaft neue Kooperationsformen schaffen und internationale Initiativen stärken.

### 5. Cybersicherheits-, Wettbewerbs- und Beschaffungspolitik faktenbasiert weiterentwickeln

Deutschland und Europa sollten leistungsfähige Cybersicherheits-Ökosysteme aufbauen, die alle Kompetenzträger einbeziehen, die an der Steigerung der Cybersicherheit werteorientiert mitarbeiten. In der Politikgestaltung empfiehlt Kaspersky einen ausgewogenen Mix, bestehend aus (i) einer faktenbasierten technischen Regulierung der IKT-Lieferkette im Sinne von Supply-Chain-Security, (ii) der Schaffung eines attraktiven Investitionsrahmens und (iii) einer Fokussierung auf Supply-Chain-Security sowie Security by Design. Das BSI sollte seine Aufgaben nicht nur gegenüber den Bundesministerien auf der Grundlage von wissenschaftlich-technischen Erkenntnissen durchführen, sondern gegenüber allen betroffenen Einrichtungen. Damit würde die wertvolle Arbeit des BSI zur Steigerung von Cybersicherheit und Resilienz als technisch-wissenschaftliche Bundesbehörde weiter gefördert und eine nachhaltige Basis für eine vertrauensvolle Zusammenarbeit mit Wissenschaft, Wirtschaft und Zivilgesellschaft gelegt.

### 6. Standards und ethische Prinzipien für den Einsatz von KI in der Cybersicherheit fördern

Gemäß einer im Herbst 2024 veröffentlichten Kaspersky-Studie hatten in den letzten 12 Monaten 60 Prozent der Unternehmen in Deutschland mit einer Zunahme an Cyberangriffen zu kämpfen. 37 Prozent vermuten, dass die Mehrheit dieser Angriffe durch Künstliche Intelligenz unterstützt wurde. In der Bekämpfung von Cyberkriminalität sowie der Steigerung von Cybersicherheit und Resilienz müssen Künstliche Intelligenz und Machine Learning zielgerichtet genutzt werden. So führte der Einsatz neuer Machine-Learning-Modelle im ersten Halbjahr 2024 dazu, dass Kaspersky die Erkennungsrate für Advanced Persistant Threats (APT) um 25 Prozent steigern konnte. Dabei ist eine verantwortungsvolle Nutzung dieser Technologie wichtig. Zu diesem Zweck hat Kaspersky ethische Grundsätze definiert, die beim Internet Government Forum der Vereinten Nationen Ende 2023 erstmals vorgestellt wurden. Hierzu zählen eine umfassende Transparenz, die Priorisierung von Resilienz und Sicherheit im Rahmen der KI-Entwicklung, menschliche Kontrolle sowie Datenschutz. KI darf in der Cybersicherheit zudem nur für defensive Zwecke genutzt werden. Der Dialog zu ethischen Prinzipien für den Einsatz von KI in der Cybersicherheit sollte von Politik und Verwaltung gefördert werden.

### 7. Verantwortungsvolle Cybersicherheitsforschung fördern

Trotz größtmöglicher Sorgfalt in der Entwicklung und Freigabe sind IT-Produkte selten frei von Sicherheitslücken, die von Cyberkriminellen ausgenutzt werden können. Deswegen setzt Kaspersky auch für seine eigenen Produkte auf die Zusammenarbeit mit Cybersicherheitsforschern und hat ein Bug-Bounty-Programm entwickelt. Schwachstellen müssen frühestmöglich gefunden und behoben werden können. Für die IT-Sicherheitsforschung müssen Rechtssicherheit und klare Standards geschaffen werden. Dabei sollte das Computerstrafrecht in Deutschland so ausgestaltet werden, dass verantwortungsvolle IT-Sicherheitsforschung gefördert wird. Forschende, die Beiträge zur Steigerung der Cybersicherheit leisten, indem sie Cybersicherheitslücken dem Hersteller oder dem BSI melden, dürfen nicht dem Risiko strafrechtlicher Verfolgung oder zivilrechtlichen Unterlassungs- und Schadensersatzansprüchen ausgesetzt sein.

**Über Kaspersky**

*Kaspersky ist ein internationales Unternehmen für Cybersicherheit und digitale Privatsphäre, das im Jahr 1997 gegründet wurde. Der Cybersicherheitsanbieter schützt über eine Milliarde Geräte vor Cyberbedrohungen und zielgerichteten Angriffen. Die tiefgreifende Threat Intelligence sowie Sicherheitsexpertise von Kaspersky dient als Grundlage für innovative Sicherheitslösungen und -dienste, um Unternehmen, kritische Infrastrukturen, Regierungen und Privatanwender weltweit zu schützen. Das umfassende Sicherheitsportfolio des Unternehmens beinhaltet führenden Endpoint-Schutz sowie eine Reihe spezialisierter Sicherheitslösungen und -Services sowie cyberimmune Lösungen zur Verteidigung gegen komplexe und sich weiter entwickelnde Cyberbedrohungen. Über 200.000 Unternehmenskunden werden von den Technologien von Kaspersky geschützt. Weitere Informationen zu Kaspersky unter https://www.kaspersky.de/*

**Kontakt**

Jochen Michels, Director Public Affairs Europe, jochen.michels@kaspersky.com