AGENTUR DER EUROPÄISCHEN UNION FÜR CYBERSICHERHEIT

EIN VERTRAUENSWÜRDIGES UND CYBERSICHERES EUROPA

Strategie der ENISA

Juni 2020

EIN VERTRAUENSWÜRDIGES UND CYBERSICHERES EUROPA

AGENTUR DER EUROPÄISCHEN UNION FÜR CYBERSICHERHEIT

VORWORT

Gemeinsam mit den Mitgliedstaaten sowie den Organen und Einrichtungen der EU unterstützt die ENISA – die Agentur der Europäischen Union für Cybersicherheit – die EU seit mehr als 15 Jahren nachhaltig in ihrem Anliegen, das Vertrauen in die Digitalisierung und die Sicherheit innerhalb Europas zu stärken. Durch die Zusammenführung von Gemeinschaften trug die ENISA erfolgreich dazu bei, dass Europa besser auf Cybervorfälle vorbereitet ist und entsprechend reagieren kann.

Gleichzeitig schreitet die Digitalisierung unserer Wirtschaft und Gesellschaft dramatisch voran. Dies wurde im Zuge der COVID-19-Krise deutlich, als ein kollektiver und massiver Umstieg auf Remote-IT-Lösungen die Aufrechterhaltung vieler Aktivitäten sicherte. Diese Krise hat gezeigt, wie sehr Cyberangreifer unsere Abhängigkeit von diesen Technologien ausnutzen. Außerdem wurde deutlich, dass die Bedrohungslage nicht mehr auf gezielte Cyberangriffe beschränkt ist, sondern ganz neue Formen annimmt, die Millionen von Unternehmen und Bürgern massiv bedrohen, beispielsweise durch eine steigende Zahl raffinierter Vorfälle im Zusammenhang mit Ransomware. Die rasante Entwicklung digitaler Produkte und Dienste, die von der Cloud über Videokonferenzen bis hin zu 5G und KI reichen, stellt uns zudem vor neue Herausforderungen.

Aufgrund ihres ständigen Mandats und ihrer erweiterten Aufgaben und Funktionen kommt der ENISA mehr denn je eine führende Rolle zu, wenn es darum geht, die EU und ihre Mitgliedstaaten bei der Bewältigung dieser Herausforderungen zu unterstützen und eine neue Ära der Cybersicherheit in Europa einzuläuten.

Hierzu wird die ENISA alles daran setzen, relevante Trends zu antizipieren sowie Sachkenntnis und Wissen, die dem Stand der Technik entsprechen, für alle zu ermitteln und auszutauschen.

Sie wird zusammen mit der Europäischen Kommission und den Mitgliedstaaten öffentliche und private Akteure sowie Bürger dabei unterstützen, Risiken im Zusammenhang mit Cybervorfällen zu verhindern und zu beherrschen. Durch die Einführung des Zertifizierungsrahmens für die Cybersicherheit trägt die ENISA zu einem Paradigmenwechsel bei, indem sie das Sicherheitsniveau digitaler Lösungen in Europa verbessert. Damit schafft sie eine solidere Entscheidungs- und Vertrauensgrundlage. Darüber hinaus wird die Agentur eng mit der operativen Gemeinschaft im Bereich der Cybersicherheit für Europa zusammenarbeiten und auf eine gemeinsame Reaktion beim nächsten massiven Cybervorfall in Europa hinarbeiten.

In ihrer neuen Funktion wird sich die ENISA bei ihrer täglichen Arbeit von Offenheit, Flexibilität und Zuverlässigkeit leiten lassen und die Herangehensweisen noch enger mit den Mitgliedstaaten und der Europäischen Kommission abstimmen. Die ENISA wird außerdem alles daran setzen, angesichts der anhaltenden Klimakrise ihren ökologischen Fußabdruck zu verringern und ein sozial verantwortliches, inklusives Arbeitsumfeld zu schaffen.

Dieses Strategiepapier wurde im Rahmen eines auf Zusammenarbeit und Inklusion ausgerichteten Prozesses unter Beteiligung des gesamten Personals der ENISA, der Mitglieder ihres Verwaltungsrats und der Beratergruppe erstellt. Es legt die klaren Ziele fest, die die ENISA beflügeln werden, die zahlreichen Herausforderungen zu meistern.

Im Namen des Verwaltungsrats

Jean-Baptiste Demaison
Vorsitzender des Verwaltungsrats

Krzysztof Silicki
Stellvertretender Vorsitzender des Verwaltungsrats

VISION

Ein vertrauenswürdiges und cybersicheres Europa

AUFTRAG

Die Agentur der Europäischen Union für Cybersicherheit (ENISA) hat den Auftrag, in Zusammenarbeit mit der weiter gefassten Gemeinschaft ein hohes gemeinsames Niveau der Netz- und Informationssicherheit in der Union zu erreichen. Sie ist ein Fachzentrum für Cybersicherheit und unterstützt die Mitgliedstaaten und die Organe der EU mit unabhängigen, fachkundigen Ratschlägen und Lösungen zur Netz- und Informationssicherheit. Die ENISA beteiligt sich an der Ausarbeitung und Umsetzung der Cybersicherheitsstrategien der EU.

Unser Ziel ist es, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur und die Dienste der Union abwehrfähiger und zuverlässiger zu machen und ein sicheres digitales Umfeld für unsere Gesellschaft und die Bürger zu gewährleisten. Wir streben danach, eine flexible, umweltfreundliche und sozial verantwortliche Organisation zu sein, bei der der Mensch im Mittelpunkt steht.

WERTE

Gemeinschaftsbewusstsein
Die ENISA nutzt die Kompetenzen und Sachkenntnisse der Gemeinschaften und fördert Synergien und Vertrauen, um ihre Aufgabe optimal zu erfüllen.

Exzellenz
Die ENISA arbeitet nach dem neuesten Stand der Technik, erfüllt höchste Qualitätsstandards in allen Arbeitsbereichen und bewertet ihre Leistung mit dem Ziel einer kontinuierlichen Verbesserung – dabei setzt sie auf Innovation und Vorausschau.

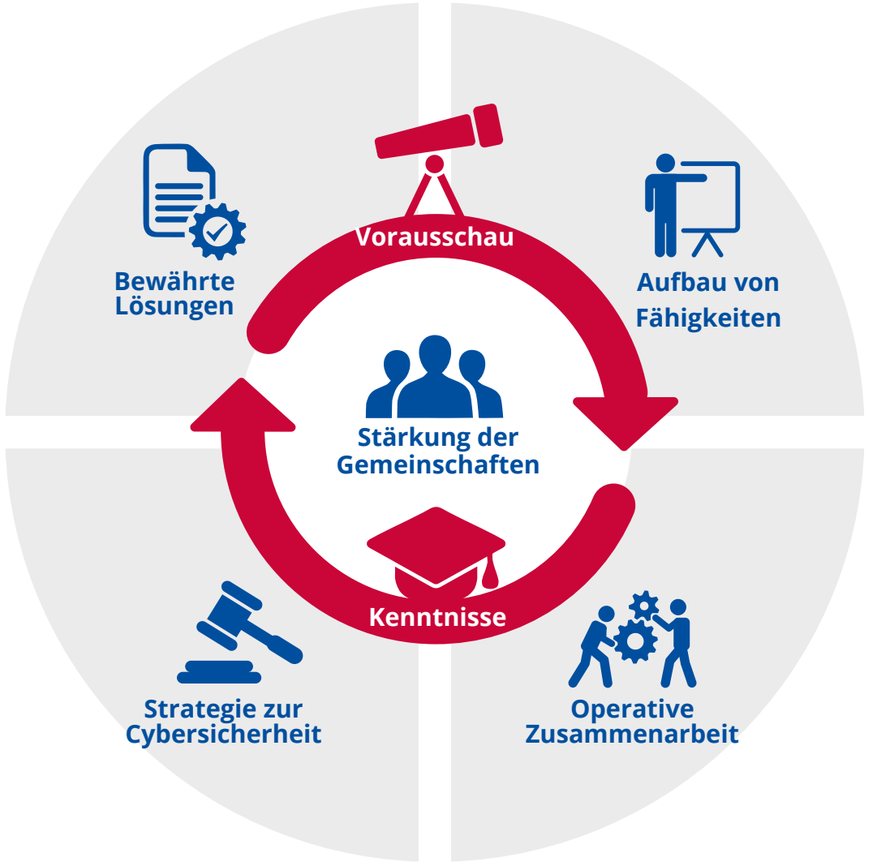
Integrität/Berufsethik
Die ENISA erfüllt ethische Grundsätze und in der EU relevante Regeln und Pflichten bei der Erbringung ihrer Dienste und in ihrem Arbeitsumfeld, um Fairness und Inklusivität sicherzustellen.

Respekt
Die ENISA wendet grundlegende europäische Rechte und Werte auf alle ihre Dienste und Arbeitsbereiche an und respektiert die Erwartungen ihrer Interessenträger.

Verantwortlichkeit
Die ENISA übernimmt Verantwortung und stellt damit sozial und ökologisch nachhaltige Praktiken und Verfahren sicher.

Transparenz
Durch offene, faktische und unabhängige Verfahren, Strukturen und Prozesse beugt die ENISA Voreingenommenheit, Mehrdeutigkeiten, Betrug und Unklarheiten vor.

STRATEGISCHE ZIELE



SZ1

Strategisches Ziel

STARKE UND ENGAGIERTE GEMEINSCHAFTEN IM CYBERSICHERHEITSÖKOSYSTEM

Kontext

Cybersicherheit geht alle an. Europa strebt einen sektorübergreifenden umfassenden Rahmen für die Zusammenarbeit an. Die ENISA spielt eine wichtige Rolle bei der Förderung einer aktiven Zusammenarbeit zwischen den Interessenträgern im Bereich der Cybersicherheit in den Mitgliedstaaten und den Organen und Einrichtungen der EU. Sie setzt sich für die Komplementarität gemeinsamer Anstrengungen ein, indem sie den Interessenträgern Mehrwert bietet, Synergien erforscht sowie begrenzte Sachkenntnis und Ressourcen der Cybersicherheit wirksam nutzt. Die Gemeinschaften sollten in die Lage versetzt werden, das Cybersicherheitsmodell zu erweitern.

Was wir erreichen möchten

- Einen EU-weiten, dem letzten Stand der Forschung entsprechenden Wissensschatz zur Cybersicherheit in Theorie und Praxis, der die Zusammenarbeit der wichtigsten Akteure in diesem Bereich herstellt, Kompetenz und Sachkenntnis in der EU fördert und neue Synergien schafft;
- ein starkes Cybersicherheitsökosystem, dem alle Behörden in den Mitgliedstaaten, die Organe und Einrichtungen der EU, Verbände, Forschungszentren und Hochschulen, die Industrie, private Akteure und Bürger angehören, die alle zu einem cybersicheren Europa beitragen.

SZ2

Strategisches Ziel

CYBERSICHERHEIT ALS WESENTLICHER BESTANDTEIL DER EU-POLITIK

Kontext

Cybersicherheit ist der Eckpfeiler der digitalen Transformation und durchdringt alle Bereiche. Daher muss sie in einer Vielzahl von Politikfeldern und Initiativen berücksichtigt werden. Cybersicherheit darf sich nicht auf eine Fachgemeinschaft technischer Cyberexperten beschränken. Vielmehr muss sie in alle EU-Politikbereiche einfließen. Dabei ist eine Fragmentierung zu vermeiden und ein einheitlicher Ansatz unter Berücksichtigung der Besonderheiten jedes Bereichs zu verfolgen.

Was wir erreichen möchten

- Proaktive Beratung und Unterstützung aller relevanten Akteure auf EU-Ebene sowie Erstellung tragfähiger, gezielter technischer Richtlinien, um sicherzustellen, dass die Cybersicherheit in die Entwicklung politischer Strategien einfließt;
- Einführung von Risikomanagementrahmen zur Cybersicherheit in allen Bereichen und deren Einhaltung während des gesamten Lebenszyklus der Cybersicherheitsstrategie.

SZ3

Strategisches Ziel

WIRKSAME ZUSAMMENARBEIT DER OPERATIVEN AKTEURE INNERHALB DER UNION BEI MASSIVEN CYBERVORFÄLLEN

Kontext

Cybersicherheit ist eine Grundvoraussetzung für den Erfolg der europäischen digitalen Wirtschaft und Gesellschaft. Cyberangriffe kennen keine Grenzen und können alle gesellschaftlichen Schichten betreffen. Daher muss die Union bei massiven (groß angelegten und grenzüberschreitenden) Cyberangriffen und Cyberkrisen sofort reagieren können. Angesichts grenzüberschreitender Verflechtungen bedarf es einer wirksamen Zusammenarbeit zwischen den Mitgliedstaaten und den Organen der EU, damit schneller gehandelt werden kann und die Anstrengungen auf allen Ebenen (strategisch, operativ, technisch und kommunikativ) angemessen koordiniert werden.

Was wir erreichen möchten

- Laufende grenzüberschreitende und gesamtgesellschaftliche Unterstützung der Zusammenarbeit zwischen den Mitgliedstaaten und den Organen der EU; insbesondere bei potenziellen massiven Vorfällen und Krisen Intensivierung der technischen operativen, politischen und strategischen Zusammenarbeit der wichtigsten operativen Akteure, um zeitnah eine Reaktion, einen Informationsaustausch, eine Lageerfassung und eine Krisenkommunikation in der gesamten Union zu ermöglichen;
- umfassendes und schnelles Handeln auf technischer Ebene auf Ersuchen der Mitgliedstaaten, um in Bezug auf das Vorfall- und Krisenmanagement technische und operative Unterstützung zu leisten.

SZ4

Strategisches Ziel

BRANDAKTUELLE KOMPETENZEN UND FÄHIGKEITEN IM BEREICH CYBERSICHERHEIT IN DER EU

Kontext

Cyberangriffe nehmen rasant zu und werden zunehmend raffinierter. Gleichzeitig steigt auch die Nutzung von IKT-Infrastrukturen und -Technologien durch Einzelpersonen, Organisationen und Industrieunternehmen rapide. Die Nachfrage nach Kenntnissen und Kompetenzen in der Cybersicherheit übersteigt das Angebot. Die EU muss in den Aufbau von Kompetenzen und Talenten im Bereich der Cybersicherheit investieren – und zwar auf allen Ebenen, vom Laien bis hin zur hoch qualifizierten Fachkraft. Die Investitionen sollten nicht nur darauf ausgerichtet sein, die Fähigkeiten der Mitgliedstaaten in Bezug auf die Cybersicherheit auszubauen, sondern auch sicherstellen, dass die verschiedenen operativen Gemeinschaften über angemessene Möglichkeiten verfügen, mit der Bedrohungslage umzugehen.

Was wir erreichen möchten

- Abgestimmte Kompetenzen, Berufserfahrung und Bildungsstrukturen im Bereich Cybersicherheit, die der stetig wachsenden Nachfrage in der EU nach Kenntnissen und Kompetenzen in der Cybersicherheit gerecht werden;
- ein hohes Ausgangsniveau, was das Bewusstsein und Wissen über die Cybersicherheit in der EU angeht, und Einbeziehung des Themas in neue Disziplinen;
- erprobte und bewährte Fähigkeiten, die angemessene Möglichkeiten bieten, mit der sich verändernden Bedrohungslage in der EU umzugehen.

SZ5

Strategisches Ziel

HOHES MASS AN VERTRAUEN IN SICHERE DIGITALE LÖSUNGEN

Kontext

Digitale Produkte und Dienste sind mit Chancen und Risiken verbunden, wobei die Risiken identifiziert und gemindert werden müssen. Die Beurteilung der Sicherheit digitaler Lösungen und die Gewährleistung ihrer Vertrauenswürdigkeit sollten unbedingt auf der Grundlage eines gemeinsamen Ansatzes erfolgen und darauf abzielen, die Belange von Gesellschaft, Markt, Wirtschaft und Cybersicherheit im Gleichgewicht zu halten. Eine neutrale Instanz, die transparent handelt, erhöht das Vertrauen der Kunden in digitale Lösungen und das größere digitale Umfeld.

Was wir erreichen möchten

- Ein cybersicheres digitales Umfeld innerhalb der EU, in dem die Bürger den IKT-Produkten, -Diensten und -Prozessen vertrauen können, weil Schlüsseltechnologiebereiche durch Zertifizierungsschemata abgesichert sind.

SZ6

Strategisches Ziel

VORAUSSCHAU AUF SICH ABZEICHNENDE UND KÜNFTIGE HERAUSFORDERUNGEN IN PUNCTO CYBERSICHERHEIT

Kontext

Zahlreiche neue Technologien, die noch in den Kinderschuhen stecken oder kurz vor der Markteinführung stehen, könnten von Vorausschauverfahren profitieren. Ein strukturierter Prozess zur Förderung des Dialogs zwischen Interessenträgern würde es Entscheidungsträgern und politischen Entscheidungsträgern ermöglichen, frühzeitig Abhilfestrategien festzulegen, die die Abwehrfähigkeit der EU gegenüber Cyberbedrohungen verbessern, und Lösungen für neue Herausforderungen zu finden.

Was wir erreichen möchten

- Erkennung neuer Trends und Muster mithilfe von Vorausschau- und Zukunftsszenarien, um die Cyberrisiken der Interessenträger zu mindern;
- frühe Bewertung der Herausforderungen und Risiken im Zusammenhang mit der Einführung und Anpassung neuer künftiger Optionen und Ausarbeitung angemessener Abhilfestrategien gemeinsam mit Interessenträgern.

SZ7

Strategisches Ziel

EFFIZIENTES UND WIRKSAMES INFORMATIONS- UND WISSENSMANAGEMENT ZUR CYBERSICHERHEIT FÜR EUROPA

Kontext

Informationen und Wissen sind die Grundlage für Cybersicherheit. Unser Ziel ist es, in einem Umfeld, das sich aufgrund digitaler Entwicklungen und wechselnder Akteure ständig wandelt, die Herausforderungen unserer Zeit zu meistern. Damit Cyberexperten uns dabei effizient unterstützen können, müssen wir laufend Informationen und Wissen zur Cybersicherheit erfassen, strukturieren, zusammenfassen, analysieren, kommunizieren und verwalten. Diese Phasen sind alle gleichermaßen wichtig, um sicherzustellen, dass Informationen und Wissen im europäischen Cybersicherheitsökosystem ausgetauscht und erweitert werden.

Was wir erreichen möchten

- Gemeinsames Informations- und Wissensmanagement für das europäische Cybersicherheitsökosystem, das leicht zugänglich, maßgeschneidert, zeitnah und sofort anwendbar ist, über angemessene Methoden, Infrastrukturen und Werkzeuge verfügt und mithilfe von Qualitätssicherungsmethoden eine kontinuierliche Verbesserung der Dienste erzielt.

ÜBER DIE ENISA

Die Agentur der Europäischen Union für Cybersicherheit, ENISA, hat die Aufgabe, zu einer hohen Cybersicherheit innerhalb der Union beizutragen. Die Agentur wurde im Jahr 2004 errichtet und durch den Rechtsakt zur Cybersicherheit untermauert. Sie trägt zur Unionspolitik im Bereich der Cybersicherheit bei, erhöht die Vertrauenswürdigkeit von IKT-Produkten, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, kooperiert mit den Mitgliedstaaten und Organen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Aufbau von Fähigkeiten und Sensibilisierung in Bezug auf Cybersicherheit arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und schließlich ein sicheres digitales Umfeld für die Gesellschaft und die Bürger Europas zu gewährleisten. Weitere Informationen über die ENISA und ihre Arbeit finden Sie unter www.enisa.europa.eu.

TP-02-20-759-DE-N

ENISA
Agentur der Europäischen Union für Cybersicherheit

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Griechenland

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Griechenland

enisa.europa.eu