**EWSA unterbreitet Vorschläge für Verwirklichung von Cybersicherheit**

**Die EU sollte u. a. das Mandat der ENISA als EU-Cybersicherheitsagentur stärken, einen europäischen Zertifizierungsrahmen festlegen und ihr Augenmerk auf die Kompetenzen und den Schutz der Internetnutzer richten.**

Auf seiner Plenartagung am 14. Februar 2018 verabschiedete der EWSA eine einschlägige [Stellungnahme](http://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/cybersecurity-act), die von **Alberto Mazzola** und **Antonio Longo** aus der Fachgruppe Verkehr, Energie, Infrastrukturen, Informationsgesellschaft (TEN) erarbeitet wurde. Er unterstützt darin den Rechtsakt zur Cybersicherheit, den die Europäische Kommission dem Rat im September 2017 im Rahmen des [Cybersicherheitspakets](https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_de) vorgelegt hatte.

Cybersicherheit ist ein weltweites Anliegen, gar eine globale Herausforderung geworden, denn Angriffe können an jedem beliebigen Ort stattfinden. Laut einer Spezial-Eurobarometer-Umfrage zum Cybersicherheitsbewusstsein der Europäer sorgen sich 73 % der Internetnutzer um die Sicherheit online übertragener personenbezogener Daten bei der Nutzung von Websites, während 65 % befürchten, dass diese Daten von Behörden nicht sicher aufbewahrt werden. Die meisten Befragten haben die Sorge, Opfer der diversen Formen von Cyberkriminalität zu werden, vor allem von Malware (69 %), Identitätsdiebstahl (69 %) und Bankkarten- sowie Online-Banking-Betrug (66 %).

Im Hinblick auf den Ausbau des europäischen Cybersicherheitsrahmens schlägt der EWSA eine Reihe praktischer Maßnahmen vor.

* **Stärkung der ENISA als EU-Cybersicherheitsagentur**

Die **Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA)** ist ein Kompetenzzentrum für Cybersicherheit in Europa mit Sitz in Griechenland. Der EWSA stimmt der Europäischen Kommission darin zu, dass die ENISA ein ständiges Mandat erhalten sollte. Er ist jedoch der Ansicht, dass die ENISA mehr finanzielle Ressourcen benötigt und ihre Tätigkeiten insbesondere auf elektronische Behördendienste, insbesondere die globale und EU-weite digitale Identität für Personen und Organisationen, die Verhütung und Bekämpfung von Identitätsdiebstahl und Online-Betrug sowie die Bekämpfung des Diebstahls von geistigem Eigentum ausrichten sollte.

Entscheidend ist auch die Verbesserung der Zusammenarbeit zwischen den Interessenträgern. Hierzu könnte eine intensivere Zusammenarbeit mit den Mitgliedstaaten und die Schaffung eines formalen Netzes der Agenturen für Cybersicherheit beitragen. Die ENISA könnte dann die nationalen Aufsichtsbehörden prüfen und so das Vertrauen stärken. „Alle Mitgliedsstaaten sollten eine nationale Cybersicherheitsagentur einrichten“, mahnte **Herr Mazzola.** „Über die Hälfte von ihnen haben noch kein Pendant zur ENISA. Die Europäische Kommission sollte dafür sorgen, dass bewährte Verfahren und wirksame Maßnahmen der Mitgliedstaaten ermittelt und ausgetauscht werden.“

In Anbetracht der knappen Mittelausstattung der ENISA empfiehlt der EWSA, die sektorspezifischen EU-Agenturen, insbesondere die Europäische Bankenaufsichtsbehörde (EBA), die Europäische Agentur für Flugsicherheit (EASA), die Europäische Arzneimittel-Agentur (EMA) und die Eisenbahnagentur der Europäischen Union (ERA), einzubeziehen und mit ihnen zusammenzuarbeiten, um ihre einschlägigen Kompetenzen zu nutzen.

* **Mehr strategische Investitionen**

Laut EWSA sollte die EU Investitionen verstärkt auf strategische Cybersicherheitsziele im Wege einer engen öffentlich-privaten Zusammenarbeit ausrichten. Die erforderlichen Mittel könnten über verschiedene europäische und nationale Fonds, privatwirtschaftliche Investitionen und einen speziell geschaffenen **EU-Cybersicherheitsfonds** bereitgestellt werden.

Im Einzelnen schlägt der EWSA vor, die aktuelle vertragliche öffentlich-private Partnerschaft (cPPP) zu einem dreigliedrigen gemeinsamen Unternehmen (aus Europäischer Kommission, Mitgliedstaaten und Unternehmen) weiterzuentwickeln, um über mehr Ressourcen zu verfügen und das Vertrauen unter den Interessenträgern zu festigen. Zudem sollte Europa ein neues Finanzierungsfenster in der aktuellen und künftigen Fazilität „Connecting Europe“ sowie im nächsten EFSI 3.0 öffnen.

* **Ein EU-Cybersicherheits-Kompetenznetz**

Die EU benötigt digitale Souveränität, um weltweit wettbewerbsfähig zu sein und ein solides technologisches Fundament aufzubauen. Diesbezüglich unterstützt der EWSA den Vorschlag der Europäischen Kommission, ein **EU-Kompetenznetz für Cybersicherheit** aufzubauen, das sich auf einen kohärenten, langfristigen, alle Stufen der Cybersicherheitswertschöpfungskette umfassenden Rahmen stützt.

Dieses Netz würde technisches Fachwissen und Schulungen in Cyber-Hygiene bereitstellen und durch die Verringerung der Abhängigkeit von Know-how aus Drittländern für spitzentechnologische Fähigkeiten den Aufbau einer wettbewerbsfähigen europäischen industriellen Basis fördern.

Dem Netz würde auf europäischer Ebene ein **Forschungs- und Kompetenzzentrum für Cybersicherheit** zur Seite stehen, das die nationalen Kompetenzzentren in der gesamten EU miteinander verknüpft. Es würde Forschungsprojekte koordinieren und den Aufbau eines innovationsfreundlichen europäischen Ökosystems für Cybersicherheit ermöglichen.

* **Eine europäische Cybersicherheitszertifizierung**

Der EWSA befürwortet die Schaffung eines **EU-Cybersicherheitszertifizierungsrahmens**, der den Erfordernissen der verschiedenen Sektoren gerecht wird. Zertifizierungssysteme dienen der Verbesserung der Sicherheit im Einklang mit dem aktuellen Bedarf und Bedrohungswissen und sollten auf international anerkannten europäischen Normen für Cybersicherheit und IKT gründen.

In einem Zertifizierungsrahmen könnten gemeinsame Anforderungen festgelegt werden, um die derzeitige Fragmentierung zu überwinden. Eine einheitliche Auslegung der Regeln wie auch die gegenseitige Anerkennung zwischen den Mitgliedstaaten nach gemeinsamen Rahmenvorgaben würde den Schutz des digitalen Binnenmarktes erleichtern.

* **Ein anerkanntes EU-Kennzeichnungssystem**

Die Zertifizierung sollte ein geeignetes **System zur Kennzeichnung** von Hardware und Software umfassen, das auch auf aus Drittländern importierte Produkte anzuwenden ist. Die Kennzeichnung hätte mehrere Vorteile: Verringerung der Kosten für die Unternehmen, Überwindung der Marktfragmentierung aufgrund der unterschiedlichen nationalen Zertifizierungssysteme und verständlichere Information der Verbraucher über die Merkmale der gekauften Waren.

Nach Meinung des EWSA wäre die Schaffung eines **Gütezeichens** nach dem Vorbild des in der Adressleiste von Websites angezeigten Sperrschlosses zweckmäßig, um das Vertrauen der Verbraucher zu stärken, die dadurch unmittelbar über die Zuverlässigkeit von Produkten bzw. die Vertrauenswürdigkeit von Websites aufgeklärt würden.

* **Der Faktor Mensch: Verbrauchererziehung und -schutz**

Die Menschen sind als Nutznießer des Internets wesentliche Interessenträger der Digitaltechnik, laufen jedoch gleichzeitig Gefahr, Opfer von Cyberkriminalität zu werden. Nach Ansicht des EWSA sollte der Vorschlag der Europäischen Kommission die **Verbesserung der Cyberfähigkeiten** der Bürger und Unternehmen deutlicher ins Visier nehmen.

Zur Verbesserung der Cyber-Hygiene und der Sensibilisierung empfiehlt der EWSA drei Aktionsbereiche auf der Grundlage von lebenslangem Lernen und Schulungsprogrammen, Sensibilisierungskampagnen und der Aufstellung EU‑zertifizierter Lehrpläne für Sekundarschulen und die Ausbildung von Fachkräften.

„Der Faktor Mensch ist maßgebend für die Verwirklichung von Cybersicherheit. Menschen sind Nutzer und Verbraucher. Wir müssen in Bildungs- und Schulungsprogramme investieren, um eine starke Ausgangsbasis an Cyberfähigkeiten aufzubauen, das Wissen um „sicheres“ Cyberverhalten zu fördern und gleichzeitig das Vertrauen der Nutzer ins Internet zu festigen. Voraussetzung dafür ist die Bereitschaft zur Zusammenarbeit sämtlicher nationalen und regionalen Behörden sowie Unternehmen einschl. KMU,“ erläuterte **Herr Longo**.

* **Das Internet der Dinge (Internet of Things, IoT)**

Dem Faktor Mensch kommt auch im Kontext der „normalen“ IoP-Geräte (IoP = Internet of People) in unserem Alltag, bspw. der digitalen Komponenten unserer Autos und Häuser, eine wesentliche Bedeutung zu. Wir verlassen uns auf eine immer weiter steigende Zahl vernetzte Geräte, die häufig nicht so gut geschützt sind wie herkömmliche Geräte und Cyberkriminellen eine größere Angriffsfläche bieten. Eine EU-Zertifizierung könnte deshalb das Sicherheitsniveau des **Internets der Dinge (IoT)** verbessern.