Europäisches Parlament

Hin zu einer unabhängigen und vertrauenswürdigen IKT-Branche in der EU

Die wirksame Bekämpfung der Cyberkriminalität und die Gewährleistung des Schutzes der Privatsphäre sind ausschlaggebend für das Vertrauen von Einzelpersonen in ein digitales Umfeld, in dem Zahl und Komplexität der Cyberbedrohungen zunehmen. Eine Reihe von Herausforderungen trennt die Europäische Union (EU) von ihrem Ziel eines vertrauenswürdigen und gegenüber Cyberangriffen standhaften digitalen Binnenmarkts: (1) unzureichende Mittel für den Ausbau europäischer Cybersicherheitsunternehmen, (2) Fragmentierung der europäischen Cybersicherheitsbranche, (3) starke Abhängigkeit von Anbietern außerhalb der EU, (4) Missverhältnis zwischen den FuE-Programmen der öffentlichen Hand und den Erfordernissen des Marktes, (5) regulatorische Fragmentierung und (6) uneinheitliche Anforderungen für die Standardisierung und die Vergabe öffentlicher Aufträge in den Mitgliedstaaten.

Der Regelungsrahmen der EU für den Schutz der Privatsphäre und den Datenschutz ist zwar einer der fortschrittlichsten der Welt; damit die personenbezogenen Daten der europäischen Bürger umfassend geschützt werden, müssen jedoch nach wie vor Herausforderungen überwunden werden. Im globalen Internet geben nicht in der EU niedergelassene Marktführer im Bereich Digitales personenbezogene Daten an Drittländer weiter, in denen deutlich weniger strenge Datenschutzbestimmungen gelten.

Mit der Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie), dem vor Kurzem angenommenen Cybersicherheitspaket und dem aktualisierten Regelungsrahmen für den Datenschutz sollen diese Probleme gelöst werden. Dennoch gibt es nach wie vor enorme Herausforderungen.

Für den Aufbau einer vertrauenswürdigen digitalen Wirtschaft und Gesellschaft ist es in diesem Zusammenhang unerlässlich, politische Maßnahmen für eine bessere Widerstandsfähigkeit der EU gegenüber Cyberangriffen einzuführen. Mit den vorgeschlagenen politischen Optionen soll ein institutioneller Rahmen geschaffen werden, in dem öffentliche Stellen auf europäischer und einzelstaatlicher Ebene die Zusammenarbeit und die Koordinierung bei der Abwehr von Cyberbedrohungen verbessern können. Zudem sollen sie dazu beitragen, eine gesunde und wettbewerbsfähige Cybersicherheitsbranche in Europa zu fördern, um die zu starke Abhängigkeit von Cybersicherheitsanbietern außerhalb der EU zu verringern. Die politischen Optionen sind darüber hinaus auf die Endnutzer digitaler Dienste ausgerichtet, die ein wichtiges Glied in der Sicherheitskette bilden.

Die politischen Maßnahmen gliedern sich in vier Blöcke: institutionelle Maßnahmen, marktpolitische Maßnahmen, industriepolitische Maßnahmen und Maßnahmen auf der Nachfrageseite. Ziel der institutionellen Maßnahmen ist es, regulatorische Abhilfemaßnahmen zur Bekämpfung der Cyberkriminalität voranzutreiben und die Koordinierung zwischen einzelnen öffentlichen Verwaltungen zu verbessern. Mit marktpolitischen Maßnahmen sollen gleiche Wettbewerbsbedingungen in den Mitgliedstaaten geschaffen und der grenzüberschreitende Handel mit Produkten und Dienstleistungen im Bereich Cybersicherheit erleichtert werden. Industriepolitische Maßnahmen sind darauf ausgerichtet, günstige Bedingungen dafür zu schaffen, dass sich die europäische Cybersicherheitsbranche im Wettbewerb mit Anbietern aus Drittländern durchsetzt. Maßnahmen auf der Nachfrageseite wiederum sollen zu einem stärkeren Einsatz und einem größeren Wissen der Endnutzer (Einzelpersonen und Unternehmen, vor allem KMU) im Bereich Cybersicherheit beitragen.

Institutionelle Maßnahmen

1. **Stärkung der Rolle der EU und der Stellen, die in den Mitgliedstaaten für Fragen der Cybersicherheit zuständig sind**

   Cyberbedrohungen sind ihrem Wesen nach grenzüberschreitend. Dies macht es schwer, sich ihrer auf einzelstaatlicher Ebene anzunehmen. Die Cybersicherheit fällt jedoch nach wie vor in die Zuständigkeit der Mitgliedstaaten, während sich die Rolle der EU-Gremien (allen voran der ENISA) darauf beschränkt, den Mitgliedstaaten beratend zur Seite zu stehen und die Bürger zu sensibilisieren. Mit der NIS-Richtlinie und der vorgeschlagenen Verordnung über die Agentur (COM(2017)0477) werden der ENISA neue Aufgaben übertragen. Dennoch beschränkt sich ihr Aufgabenbereich nach wie vor doch sehr auf die Bereiche Beratung und Unterstützung. Wie in dem Vorschlag für eine neue Verordnung über die Agentur empfohlen, wäre es ratsam, die Rolle der ENISA als einer unabhängigen und ständigen Agentur, die nicht Spielball einzelstaatlicher Interessen ist, zu stärken.

2. **Vereinheitlichung der Rechtsvorschriften zur Bekämpfung der Cyberkriminalität**

   Cyberkriminalität wird in der EU nicht strafrechtlich einheitlich verfolgt. Dies ermöglicht es Cyberkriminellen, aus lascheren Vorschriften Nutzen zu ziehen. Zudem werden strafrechtliche Ermittlungen und die Strafverfolgung dadurch behindert, dass Cyberangriffe keine Grenzen kennen und das dem Völkerrecht zugrunde liegende Territorialitätsprinzip zum Tragen kommt. Beides trägt dazu bei, dass Cyberkriminelle straffrei davonkommen.

   Ende 2016 wurde das Europäische Justizielle Netz gegen Cyberkriminalität ins Leben gerufen, um den Austausch von Fachwissen und über bewährte Verfahren zwischen den Justizbehörden der EU-Mitgliedstaaten zu verstärken. Doch dies geht nicht weit genug. Für eine bessere Bekämpfung von Cyberkriminellen wäre es sicherlich hilfreich, wenn die Definition des Begriffs „Cyberkriminalität" vereinheitlicht würde und die Verfahren für die Beschaffung elektronischer Beweismittel in Strafverfahren sowie die Strafen für die Schuldigen in den Mitgliedstaaten erläutert würden.

Marktpolitische Maßnahmen

3. **Vereinheitlichung der Anforderungen für die Vergabe öffentlicher Aufträge im Hinblick auf Cybersicherheitslösungen**

   Bei der Förderung der Cybersicherheitsbranche spielt die Vergabe öffentlicher Aufträge eine Schlüsselrolle. Allerdings wird die Entwicklung europaweiter Cybersicherheitsunternehmen dadurch behindert, dass die Anforderungen für die Vergabe öffentlicher Aufträge im Hinblick auf Cybersicherheitslösungen, vor allem die Regelungen und Standards für die Zertifizierung, zwischen den EU-Mitgliedstaaten und in diesen von Behörde zu Behörde unterschiedlich sind. Dadurch wird zum einen die Marktfragmentierung in Europa gefördert und zum anderen der Ausbau europäischer Unternehmen begrenzt.

   Durch eine Vereinheitlichung der Anforderungen der Einrichtungen der EU und der Mitgliedstaaten würde die Entwicklung europäischer Cybersicherheitslösungen vorangetrieben. Durch die Einführung eines Vertrauenssiegels für europäische Cybersicherheitsprodukte wird die Wirksamkeit der Maßnahme weiter erhöht, indem dieses Siegel zu einer einheitlichen Anforderung wird, die den europäischen Anbietern zugutekommen könnte.

4. **Einführung von Vertrauenssiegeln für europäische Cybersicherheitsprodukte**

   Die Einführung europäischer Vertrauenssiegel für Cybersicherheitsprodukte könnte dem gesamten Ökosystem zugutekommen. Verbraucher könnten vertrauenswürdige Anbieter beim Erwerb von Cybersicherheitslösungen leicht erkennen, und Cybersicherheitsprodukte mit diesem Vertrauenssiegel könnten ohne weitere Anpassungen an die jeweiligen einzelstaatlichen Anforderungen in der gesamten EU vertrieben werden. Vertrauenssiegel können darüber hinaus von zusätzlichem Nutzen für das Marketing sein, da sie äußerst hilfreich dafür sind, die Qualität und Zuverlässigkeit europäischer Cybersicherheitsprodukte erkennen zu lassen.

Der Erfolg der Vertrauenssiegel hängt von Folgendem ab: (1) der Entwicklung transparenter Zertifizierungsverfahren, (2) einem nicht zu hohen Verwaltungsaufwand und (3) der Zugänglichkeit für alle Unternehmen, unabhängig von ihrer Größe und ihrem Standort.

5. Vereinheitlichung der Standardisierung und Zertifizierung von Cybersicherheitsprodukten

Die Standardisierungsverfahren für Cybersicherheitsprodukte erleben zurzeit einen wahren Aufschwung, da eine Reihe von Organisationen versucht, die Sicherheitsanforderungen für mehrere neue IKT-Technologien festzulegen. Die EU sollte bei der Vereinheitlichung der zahlreichen bereits festgelegten Standards im Bereich der Cybersicherheit eine Vorreiterrolle übernehmen und einen kohärenten Rahmen für die Zertifizierung auf europäischer Ebene festlegen.

Mit der gemeinsamen Mitteilung der Kommission über die wirksame Erhöhung der Cybersicherheit in der EU kann ein Schritt in die richtige Richtung getan werden, indem der ENISA die Zuständigkeit für die Schaffung eines EU-weiten Rahmens für die Zertifizierung der Cybersicherheit übertragen wird, mit dem die Verfahren für die Einführung von Regelungen für die Zertifizierung der Cybersicherheit festgelegt werden. Diese Zertifizierungsregelungen werden zwar freiwillig sein, doch sie sind ein wichtiger erster Schritt.

Industriepolitische Maßnahmen

6. Förderung der Entwicklung quelloffener Cybersicherheitsprodukte

Cybersicherheitsprodukte können als proprietäre Software oder durch Open-Source-Technologien entwickelt werden. Im ersten Fall werden in der Regel „Black Box"-Lösungen geboten: Dabei ist es den Verbrauchern nicht möglich, zu überprüfen, wie diese tatsächlich funktionieren. Open-Source-Software hingegen ermöglicht es Forschern, Fehlercodes und Schwachstellen zu überprüfen und die Zuverlässigkeit und Vertrauenswürdigkeit von Cybersicherheitsprodukten beständig zu verbessern. Dennoch können Cyberangriffe dadurch nicht gänzlich ausgeschlossen werden, und unter Umständen ist Open-Source-Software für Fälle, in denen ein gewisser Grad an Geheimhaltung erforderlich ist (Erkennung und Verhinderung von Angriffen, Informationen über Bedrohungen usw.), nicht geeignet. Dass der Code von jedem analysiert und geändert werden kann, könnten Cyberkriminelle auch dafür nutzen, neue Schwachstellen zu entwickeln.

EU-Gremien können Anreize für die Entwicklung quelloffener Cybersicherheitsprodukte setzen, indem sie (1) die Vergabe öffentlicher Aufträge im Hinblick auf Cybersicherheits- und IT-Lösungen auch an „Open-Source"-Anforderungen knüpfen, (2) bei Projekten im Bereich Open-Source-Software zusammenarbeiten, um gemeinsam innovative offene Lösungen zu erarbeiten, (3) rechtliche Fragen des geistigen Eigentums klären und (4) Forschung auf der Grundlage von Open-Source-Technologien fördern.

Open-Source ist zwar eine überaus interessante Option, sollte jedoch in den Bereichen der Technik, in denen ein direkter Wettbewerb vermieden wird und von der EU starke proprietäre Lösungen eingesetzt werden, mit Bedacht ausgewählt werden. Open-Source-Lösungen können zwar die Widerstandsfähigkeit von Produkten und Dienstleistungen im Bereich IKT gegenüber Cyberangriffen verbessern, doch sie bieten Anbietern in der EU mitunter keinen Wettbewerbsvorteil.

7. Entwicklung einer Industriepolitik im Bereich Cybersicherheit

Mit den derzeitigen industriepolitischen Maßnahmen der EU wird nicht angemessen auf Fragen der Cybersicherheit eingegangen. Weder in der Mitteilung mit dem Titel „Eine Industriepolitik für die Sicherheitsbranche" noch in der Mitteilung mit dem Titel „Für ein Wiedererstarken der europäischen Industrie" wird Cybersicherheit als einer der strategischen Bereiche genannt, die es zu fördern gilt.

Es wäre notwendig, sämtliche Maßnahmen zur Stärkung der europäischen Cybersicherheitsbranche in einem umfassenden Aktionsplan mit eindeutigen Zielen und einem genauen Fahrplan zu gliedern. Der Schwerpunkt sollte auf den Bereichen liegen, in denen gute Voraussetzungen dafür herrschen, dass die EU eine Führungsrolle übernimmt (industrielle Sicherheit und Cybersicherheit in der Luftfahrt, im Eisenbahnverkehr und in der Automobilindustrie), ebenso wie auf den Bereichen, die es erfordern, dass die EU unabhängig ist (Verteidigung, Kryptografie).

Die Industriepolitik sollte darauf abstellen, Kompetenzzentren in ganz Europa aufzubauen, in denen Theorie und Innovation zusammengeführt und Standpunkte und Ideen ausgetauscht und gemeinsam

weiterentwickelt werden können, so dass ein kommerzieller Erfolg erzielt wird. Das in der jüngsten Cybersicherheitsstrategie der Kommission vorgesehene Netz von Kompetenzzentren für Cybersicherheit kann, sofern es gut ausgebaut wird, ein Schritt in die richtige Richtung sein. Darüber hinaus sollte vorgesehen werden, dass die EU dazu beiträgt, Ausfuhren europäischer Lösungen und Dienstleistungen im Bereich Cybersicherheit in Drittländer, allen voran in die Vereinigten Staaten, Asien und in den ENOA-Raum[1], zu fördern.

8. Förderung der Schaffung von Investitionsinstrumenten für die Cybersicherheitsbranche

Die Förderung für europäische Cybersicherheitsunternehmen konzentriert sich auf die frühen Phasen (Startkapital), während die Fördermittel für die Konsolidierungs- und die Expansionsphase äußerst überschaubar sind. Durch diese unzureichende Förderung werden zwei wesentliche Geschäftsprozesse beeinträchtigt: (1) die Marketingtätigkeiten zur Erhöhung des Bekanntheitsgrads der Unternehmen und (2) die für den Eintritt in neue Märkte erforderliche Anpassung der Produkte und Dienstleistungen der Unternehmen. Daher ist es notwendig, Finanzierungsinstrumente zu gestalten und zu fördern, die alle Phasen des Geschäftslebens abdecken, vor allem da es sich um eine Branche handelt, der herkömmliche Finanzierungspartner (Banken) bisweilen mit Widerwillen begegnen.

Die EU hat mehrere Finanzierungsinstrumente, die für die Cybersicherheitsbranche infrage kämen. Beispielsweise könnten Mittel aus dem Europäischen Fonds für strategische Investitionen (EFSI), einer gemeinsamen Initiative der EIB[2]-Gruppe und der Kommission, nicht nur für die allgemeine „digitale" Branche, sondern auch für die Cybersicherheitsbranche verwendet werden. Dazu könnte eine Plattform für Investitionen in die Cybersicherheit aufgebaut werden, mit der anschließend Cybersicherheitsprojekte in der EU gefördert würden. Diese Plattform würde nicht nur dazu dienen, die ihr zugewiesenen Mittel aus dem EFSI zu verwalten, sondern sie würde sich auch aus Mitteln aus anderen Quellen (z. B. öffentliche Mittel einzelstaatlicher Behörden und Mittel aus der Privatwirtschaft) speisen, die wiederum durch sie verwaltet würden, um entsprechend dem Bedarf der Cybersicherheitsunternehmen mehrere Finanzierungsinstrumente einzurichten.

Private Mittel sollten ebenfalls zum Wirtschaftswachstum beitragen; Voraussetzung dafür ist jedoch ein stabiles und vorhersehbares Umfeld, in das investiert werden soll. Europäische Einrichtungen könnten private Investitionen in der Branche indirekt fördern, indem sie Kernthemen wie die Standardisierung oder die Kennzeichnung harmonisieren und vereinheitlichen sowie indem sie gemeinsam in Maßnahmen der gemischten Finanzierung investieren und die Investitionskapazitäten von Institutionen wie der EIB ausnutzen.

9. Förderung marktgesteuerter Forschungstätigkeiten

Es ist bewiesen, dass zwischen den Erfordernissen des Marktes und der Erforschung von Fragen der Cybersicherheit in der EU ein Missverhältnis besteht. Die lange Laufzeit von EU-Programmen – drei bis fünf Jahre von der Entwicklung bis zum Abschluss eines Projekts – ist Teil dieses Problems. In der europäischen Cybersicherheitsbranche wird tendenziell von Schritt zu Schritt gedacht: Der Fokus liegt weniger auf langfristiger strategischer Planung als vielmehr auf dem Aufbau operativer Kapazitäten. Gegenwärtig wird Forschung ausgehend von den Impulsen der Wissenschaft anstatt im Sinne der Nachfrage des Marktes betrieben, was zur Folge hat, dass die wissenschaftlichen Ergebnisse der EU letzten Endes von Unternehmen in Drittländern erzielt werden. Ebenso deutet vieles darauf hin, dass die Höhe der in Europa verfügbaren Fördermittel für FuE-Tätigkeiten kaum dafür ausreicht, die Branche maßgeblich zu beeinflussen.

Um der wachsenden Zahl von Cyberbedrohungen beizukommen, müssen sich die für die Festlegung von Forschungsthemen zuständigen öffentlichen Stellen und die Anbieter im Bereich Cybersicherheit, die die Herausforderungen, denen ihre Kunden gegenüberstehen, aus erster Hand kennen, besser abstimmen. Zudem empfehlen sich eine Erhöhung der Mittel für FuE-Tätigkeiten und eine sorgfältige Überwachung der Beiträge privater Partner, wie sie in der neuen vertraglichen Vereinbarung über öffentlich-private Partnerschaften im Rahmen des Programms Horizont 2020 dargelegt wird.

[1] Europa, der Nahe Osten und Afrika.
[2] Europäische Investitionsbank

10. Bessere Verfügbarkeit von Arbeitnehmern im Bereich Cybersicherheit

Die Cybersicherheitsbranche in Europa leidet unter Fachkräftemangel. Dabei handelt es sich um ein in vielen Bereichen der digitalen Wirtschaft weit verbreitetes Problem, das jedoch in den innovativeren und wachsenden Bereichen wie der Cybersicherheit noch akuter ist.

Um das Problem zu lösen, könnte(n) (1) die gegenwärtigen Erfordernisse der formalen und nicht formalen Bildung im Bereich der Cybersicherheit gemeinsam mit Forschungseinrichtungen und der Branche analysiert werden, (2) innerhalb der Branche und in Fortbildungseinrichtungen Programme des lebenslangen Lernens gefördert werden, die sich an vorhandene Fachkräfte richten und diese dabei unterstützen, eine berufliche Laufbahn einzuschlagen, (3) Studierende für die Karrierechancen in der Cybersicherheitsbranche sensibilisiert und Cybersicherheit als Wahlfach in Schulen gefördert werden, (4) Cybersicherheit als Studiengang an Hochschulen und in der Berufsbildung gefördert werden, (5) unter Beteiligung aller Interessenträger (der Branche, der Regierungen, des Militärs) ein umfassendes EU-weites Curriculum und eine Reihe einheitlicher technischer Bereiche festgelegt werden, (6) die Zusammenarbeit zwischen Bildungseinrichtungen, Nachrichtenagenturen und Militär zwecks des Austausches wichtiger fachlicher und sozialer Kompetenzen verstärkt werden und (7) geeigneten Bewerbern in der EU Mittel für Masterstudiengänge und Doktorate an Hochschulen in Europa oder andernorts zur Verfügung gestellt werden.

Maßnahmen auf der Nachfrageseite

11. Sensibilisierung von Endnutzern (Einzelpersonen, KMU) für Cyberbedrohungen

Cybersicherheit betrifft nicht nur die Technologie, sondern auch die Menschen. Ob bzw. inwieweit jemand Opfer eines Cyberangriffs wird, hängt davon ab, wie er digitale Dienste nutzt. Ungeschulte Nutzer und diejenigen mit einem weniger ausgeprägten Bewusstsein für Cyberbedrohungen werden zu einem schwachen Glied in der Sicherheitskette.

Für sichere Online-Interaktionen für alle Bürger unabhängig von deren allgemeiner oder beruflicher Bildung wäre es hilfreich, Schüler und Studierende zu schulen, Kampagnen zur Sensibilisierung für Cybersicherheitsfragen ins Leben zu rufen und maßgeschneiderte Cybersicherheitsübungen für unterschiedliche Zielgruppen (Minderjährige, Jugendliche, Eltern, Ausbilder, Fachkräfte, Forscher, hochrangige Führungskräfte usw.) einzuleiten.

Dieser Punkt betrifft vor allem Einzelpersonen und Angestellte von KMU, denen es nicht nur an einem ausgeprägten Bewusstsein für Fragen der Cybersicherheit, sondern grundsätzlich an ausreichenden Informationen über diese Fragen fehlt. Erschwerend kommt hinzu, dass je nach den soziodemografischen Merkmalen der Einzelpersonen und der Branche und Größe der Unternehmen große Unterschiede zu beobachten sind. Es wird daher angeraten, mit Bedachtnahme auf diese Faktoren unterschiedliche Maßnahmen festzulegen. Im Hinblick auf die Umsetzung dieser Maßnahmen könnte die Kommission die erforderlichen Mittel und die grundlegende Strategie bereitstellen, während die nationalen und regionalen Regierungen und Branchenverbände für die Anpassung der Maßnahmen an die jeweiligen Bedingungen in der Bevölkerung und unter den Angestellten zuständig sein könnten. Diese Anpassung könnte mit einer konsequenten Weiterverfolgung durch andere europäische Einrichtungen einhergehen. Darüber hinaus könnte die EU eine Vorreiterrolle dabei übernehmen, ein einheitliches Portal zur Zusammenführung aller europäischen Cybersicherheits-Tools in einer einzigen Anlaufstelle aufzubauen, auf dem die Nutzer zudem darüber beraten werden könnten, wie sie ihre Systeme, Netzen und Daten sichern können. Andere Sensibilisierungsmaßnahmen wie der europäische Monat der Cybersicherheit könnten z. B. dadurch gestärkt werden, dass ihre Werbemittel erhöht werden, wodurch wiederum mehr EU-Bürger erreicht würden.

Dieses Dokument beruht auf einer STOA-Studie zum Thema „Hin zu einer unabhängigen und vertrauenswürdigen IKT-Branche in der EU“ (PE 614.531), die im Dezember 2017 veröffentlicht wurde. Die Studie wurde von Iclaves SL (Spanien) im Auftrag der Lenkungsgruppe für die Bewertung wissenschaftlicher und technologischer Optionen und unter Leitung des Referats Wissenschaftliche Vorausschau (STOA) der Generaldirektion Wissenschaftlicher Dienst (GD EPRS) des Europäischen Parlaments durchgeführt.

Autoren: Rafael Rivera, Juan Pablo Villar, Carlota Tarín, Arturo Ribagorda, Juan Manuel Estévez, José María De Fuentes und Lorena González. Zuständiger STOA-Verwaltungsrat: Zsolt G. Pataki. Die Studie ist verfügbar unter: http://www.europarl.europa.eu/stoa/.