EUROPÄISCHE
KOMMISSION

HOHE VERTRETERIN
DER UNION FÜR
AUSSEN- UND
SICHERHEITSPOLITIK

Brüssel, den 13.9.2017
JOIN(2017) 450 final

GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen

1. EINLEITUNG

Cybersicherheit ist sowohl für unseren Wohlstand als auch für unsere Sicherheit von entscheidender Bedeutung. Da unser tägliches Leben und unsere Wirtschaft in zunehmendem Maße von digitalen Technologien bestimmt werden, sind wir den damit verbundenen Gefahren immer stärker ausgesetzt. Cybersicherheitsvorfälle werden sowohl hinsichtlich ihrer Urheber als auch mit Blick auf die verfolgten Ziele immer vielfältiger. Böswillige Cyberaktivitäten stellen nicht nur eine Bedrohung für unsere Volkswirtschaften und unsere Bemühungen zur Verwirklichung des digitalen Binnenmarktes dar, sondern sie gefährden auch das gesamte Funktionieren unserer Demokratien, unsere Freiheiten und unsere Werte. Unsere künftige Sicherheit hängt davon ab, inwieweit es uns gelingt, die EU vor Cyberbedrohungen zu schützen: Sowohl für unsere zivilen Infrastrukturen als auch für unsere militärischen Kapazitäten benötigen wir sichere Digitalsysteme. Dies wurde vom Europäischen Rat im Juni 2017[1] sowie in der Globalen Strategie für die Außen- und Sicherheitspolitik der Europäischen Union[2] anerkannt.

Die Risiken wachsen exponentiell. Studien ist zu entnehmen, dass sich der durch Cyberkriminalität verursachte wirtschaftliche Schaden zwischen 2013 und 2017 verfünffacht hat und bis 2019 erneut vervierfachen könnte.[3] Besonders stark hat die Verbreitung von Ransomware[4] zugenommen, wobei die jüngsten Angriffe[5] den dramatischen Anstieg der Cyberkriminalität widerspiegeln. Ransomware ist jedoch bei Weitem nicht die einzige Bedrohung.

Cyberbedrohungen gehen sowohl von nichtstaatlichen als auch von staatlichen Akteuren aus: Ihnen liegen oftmals kriminelle Absichten mit finanziellen Interessen zugrunde, sie können aber auch politisch und strategisch motiviert sein. Und weil die Grenze zwischen „traditioneller“ Kriminalität und Cyberkriminalität verschwimmt, wird die kriminelle Bedrohung noch verstärkt, da Straftäter das Internet sowohl als Mittel zur Ausweitung ihrer Aktivitäten als auch für die Suche nach neuen Methoden und Instrumenten für kriminelle Handlungen einsetzen[6]. In der überwiegenden Mehrheit der Fälle gibt es kaum eine Möglichkeit, dem Straftäter auf die Spur zu kommen, und die Aussicht auf eine erfolgreiche Strafverfolgung ist noch geringer.

Gleichzeitig verfolgen staatliche Akteure ihre geopolitischen Ziele in zunehmendem Maße nicht nur anhand herkömmlicher Mittel wie militärischer Gewalt, sondern auch über diskretere Cyberinstrumente, unter anderem mittels Eingriffen in interne demokratische Prozesse. Die Nutzung des Cyberraums für Kriegsführung – sei es allein im Cyberraum oder im Rahmen eines hybriden Ansatzes – wird heutzutage als gegeben angenommen. Da Desinformationskampagnen, gezielte Falschmeldungen und auf kritische Infrastruktur ausgerichtete Cybermaßnahmen immer mehr zunehmen, müssen wir ihnen begegnen. Vor diesem Hintergrund hat die Kommission in ihrem Reflexionspapier über die Zukunft der

---

1 http://www.consilium.europa.eu/de/press/press-releases/2017/06/23-euco-conclusions/

2 http://europa.eu/globalstrategy/

3 Siehe z. B. McAfee & Center for Strategic and International Studies, „Net losses: Estimating the Global Cost of Cybercrime“ 2014.

4 Ransomware ist eine Malware, die Nutzer dabei behindert bzw. daran hindert, auf ihr System zuzugreifen, indem sie entweder den Bildschirm des Geräts oder die Daten des Nutzers blockiert, wobei für den Fall der Zahlung eines Lösegelds die Aufhebung der Blockade in Aussicht gestellt wird.

5 Im Mai 2017 befiel die Ransomware WannaCry mehr als 400 000 Rechner in über 150 Ländern. Einen Monat später waren die Ukraine sowie mehrere Unternehmen weltweit von der Ransomware Petya betroffen.

6 Europol, Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität in der EU 2017.

europäischen Verteidigung[7] die Bedeutung einer Zusammenarbeit im Bereich der Cyberabwehr hervorgehoben.

Wenn es uns nicht gelingt, die Cybersicherheit erheblich zu erhöhen, werden die Gefahren im Zuge des digitalen Wandels stark zunehmen. Bereits im Jahr 2020 könnten zig Milliarden Geräte an das „Internet der Dinge" angeschlossen sein, bei deren Entwicklung jedoch der Cybersicherheit noch immer keine Priorität eingeräumt wird[8]. Wenn wir die Geräte, die unsere Stromnetze, Autos und Verkehrsnetze, Fabriken, Finanzen, Krankenhäuser und Wohnungen steuern, nicht adäquat schützen, kann das verheerende Folgen haben und das Vertrauen der Verbraucher in neue Technologien massiv untergraben. In Anbetracht des Risikos politisch motivierter Angriffe auf zivile Ziele und von Lücken in der militärischen Cyberabwehr ist die Gefahr noch größer einzuschätzen.

Der in dieser Gemeinsamen Mitteilung dargelegte Ansatz soll die EU in die Lage versetzen, diesen Bedrohungen wirksamer zu begegnen. Er soll einen Beitrag zur Erhöhung der Abwehrfähigkeit und der strategischen Autonomie sowie der technologischen Kapazitäten und Kompetenzen leisten und zudem den Aufbau eines soliden Binnenmarktes fördern. Dies setzt voraus, dass unter vollständiger Einbindung aller wichtigen Akteure geeignete Strukturen für ein hohes Maß an Cybersicherheit geschaffen werden, sodass bei Bedarf wirksam reagiert werden kann. Außerdem sieht der Ansatz vor, die Bemühungen zur Aufdeckung und Rückverfolgung von Cyberangriffen und zur Sanktionierung der Urheber zu erhöhen, um für mehr Abschreckung zu sorgen. In Anbetracht der globalen Dimension des Problems soll ferner über eine Plattform für Cybersicherheit unter Führung der EU die internationale Zusammenarbeit auf diesem Gebiet ausgebaut werden. Diese Maßnahmen stützen sich auf die Konzepte für den digitalen Binnenmarkt, die Globale Strategie, die Europäische Sicherheitsagenda[9], den gemeinsamen Rahmen für die Abwehr hybrider Bedrohungen[10] und die Mitteilung über die Einrichtung des Europäischen Verteidigungsfonds[11].[12]

Die EU befasst sich bereits mit vielen dieser Fragen. Nun ist es jedoch an der Zeit, alle Fäden miteinander zu verbinden. Im Jahr 2013 hat die EU eine Cybersicherheitsstrategie dargelegt, in der sie eine Reihe wichtiger Maßnahmen zur Verbesserung der Abwehrfähigkeit gegenüber Cyberangriffen einleitete[13]. Die darin genannten Hauptziele und Grundsätze – insbesondere die Förderung eines zuverlässigen, sicheren und offenen Cyberumfelds – gelten nach wie vor. Doch angesichts der sich ständig weiterentwickelnden und erweiternden Bedrohungslage müssen weitere Maßnahmen ergriffen werden, um Angriffen vorzubeugen bzw. Angriffe abzuwehren.[14]

---

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_de.pdf

8 IDC und TXT Solutions (2014), SMART 2013/0037, Cloud and IoT combination, Studie für die Kommission.

9 COM(2015) 185 final.

10 JOIN(2016) 18 final.

11 COM(2017) 295.

12 Der Ansatz deckt sich zudem mit dem Standpunkt unabhängiger wissenschaftlicher Berater aus der von der Europäischen Kommission eingerichteten Hochrangigen Gruppe wissenschaftlicher Berater im Rahmen des Mechanismus für wissenschaftliche Beratung (siehe Verweis unten).

13 JOIN(2013) 1 final. Eine Bewertung dieser Strategie findet sich in SWD(2017) 295.

14 Sofern keine anderslautenden Angaben gemacht werden, sind die in dieser Mitteilung enthaltenen Vorschläge haushaltsneutral. Jede Initiative mit Auswirkungen auf den Haushalt wird ordnungsgemäß das

In Anbetracht des Anwendungsbereichs ihrer Maßnahmen sowie der ihr zur Verfügung stehenden Instrumente, Strukturen und Kompetenzen ist die Europäische Union gut aufgestellt, das Thema Cybersicherheit anzugehen. Wenngleich die Mitgliedstaaten für ihre nationale Sicherheit verantwortlich bleiben, sprechen der Umfang und der grenzübergreifende Charakter der Bedrohung eindeutig dafür, dass die EU tätig wird und den Mitgliedstaaten Anreize und Unterstützung für die Entwicklung und Aufrechterhaltung umfassenderer und besserer nationaler Cybersicherheitskapazitäten bietet und gleichzeitig entsprechende Kompetenzen auf EU-Ebene aufbaut. Durch diesen Ansatz soll gewährleistet werden, dass alle Akteure – die EU, die Mitgliedstaaten, die Unternehmen und Privatpersonen – der Cybersicherheit unverzüglich die Priorität einräumen, die erforderlich ist, um die Abwehrfähigkeit zu verbessern und auf Ebene der Europäischen Union Cyberangriffen wirksamer begegnen zu können. Es sollen konkrete Maßnahmen getroffen werden, um alle gegen die EU und ihre Mitgliedstaaten gerichteten Cybervorfälle aufzudecken, zu untersuchen und entsprechend darauf zu reagieren, unter anderem durch Verfolgung der Urheber. Außerdem soll der Ansatz dafür sorgen, dass die EU im Rahmen ihres auswärtigen Handelns die Cybersicherheit auf internationaler Bühne wirksam fördern kann. Im Ergebnis wird sich die EU durch die Bekämpfung gegenwärtiger und künftiger Bedrohungen proaktiv für die Sicherung des Wohlstands, der Gesellschaft und der Werte sowie der Grundrechte und -freiheiten in Europa einsetzen, anstatt nur im Nachhinein auf Cybervorfälle zu reagieren.

2. STÄRKUNG DER CYBERABWEHRFÄHIGKEIT DER EU

Für eine wirksame Cyberabwehrfähigkeit bedarf es eines umfassenden gemeinsamen Ansatzes. Das erfordert solidere und wirksamere Strukturen zur Förderung der Cybersicherheit und zum Umgang mit Cyberangriffen, und zwar nicht nur in den Mitgliedstaaten, sondern auch in den Organen, Einrichtungen und sonstigen Stellen der EU. Außerdem braucht es einen umfassenderen, ressortübergreifenden Ansatz zur Verbesserung der Cyberabwehrfähigkeit sowie der strategischen Autonomie, gestützt auf einen starken Binnenmarkt, bedeutende Fortschritte bei den technologischen Kompetenzen der EU und eine weitaus größere Zahl qualifizierter Experten. Dafür muss allgemein anerkannt werden, dass es sich bei der Cybersicherheit um eine gesamtgesellschaftliche Herausforderung handelt, die nur bewältigt werden kann, wenn mehrere Ebenen der Regierung, der Wirtschaft und der Zivilgesellschaft eingebunden werden.

2.1 Stärkung der Agentur der Europäischen Union für Netz- und Informationssicherheit

Die **Agentur der Europäischen Union für Netz- und Informationssicherheit** (ENISA) spielt eine entscheidende Rolle bei der Verbesserung der Cyberabwehrfähigkeit der EU und der Reaktion auf Cybervorfälle, doch ihre Handlungsfähigkeit ist aufgrund ihres derzeitigen Mandats eingeschränkt. Daher legt die Kommission einen ehrgeizigen Reformvorschlag vor, der unter anderem **ein ständiges Mandat für die Agentur**[15] vorsieht. Dadurch soll gewährleistet werden, dass die ENISA die Mitgliedstaaten, die EU-Organe sowie die Unternehmen in Schlüsselbereichen unterstützen kann, beispielsweise bei der Umsetzung der

jährliche Haushaltsverfahren durchlaufen, wobei dem nächsten mehrjährigen Finanzrahmen für die Zeit nach 2020 nicht vorgegriffen wird.

[15] COM(2017) 477.

Richtlinie über die Sicherheit von Netz- und Informationssystemen[16] (im Folgenden „NIS-Richtlinie“) sowie des vorgeschlagenen Rahmens für die Zertifizierung der Cybersicherheit.

Die reformierte ENISA wird bei der Entwicklung und Durchführung der Maßnahmen eine wichtige Beraterrolle einnehmen. So soll sie unter anderem für die Kohärenz zwischen den sektoralen Initiativen und der NIS-Richtlinie sorgen und die Einrichtung von Informationsaustausch- und -analysezentren in wichtigen Bereichen unterstützen. Die ENISA wird die Ansprüche erhöhen und so dafür sorgen, dass Europa besser gerüstet wird, indem sie einmal im Jahr europaweite Übungen zur Cybersicherheit durchführt, bei der die Reaktion auf verschiedenen Ebenen geprüft wird. Außerdem wird sie an der Ausarbeitung einer EU-Strategie für die Zertifizierung der Cybersicherheit im Bereich der Informations- und Kommunikationstechnologien (IKT) mitwirken und zudem bei der Vertiefung der operativen Zusammenarbeit sowie dem Ausbau des Krisenmanagements in der EU eine wichtige Rolle spielen. Die Agentur soll für Cybersicherheitskreise auch als Informations- und Wissenszentrum fungieren.

Um entscheiden zu können, ob die EU gemeinsame Abwehr- oder Gegenmaßnahmen unterstützen sollte, müssen Bedrohungen und Vorfälle rasch gemeinsam untersucht und entschlüsselt werden. In einen solchen Informationsaustausch müssen auf technischer, operativer und strategischer Ebene jeweils alle relevanten Akteure – Einrichtungen und Agenturen der EU sowie die Mitgliedstaaten – eingebunden werden. Ferner wird sich die ENISA in Zusammenarbeit mit den entsprechenden Stellen in den Mitgliedstaaten und auf EU-Ebene – insbesondere das Netzwerk der Computer-Notfallteams (Computer Security Incident Response Teams – CSIRTs)[17], das CERT-EU, Europol und das EU-Zentrum für Informationsgewinnung und -analyse (INTCEN), auch an der Lageeinschätzung auf EU-Ebene beteiligen. Diese Erkenntnisse können im Rahmen der regelmäßigen Überwachung der Bedrohungslage und einer effizienten operativen Zusammenarbeit sowie bei umfangreichen grenzüberschreitenden Vorfällen in die Bedrohungsanalyse und die Entscheidungsfindung einfließen.

2.2 Schaffung eines Binnenmarkts für Cybersicherheit

Das Wachstum des Cybersicherheitsmarktes in der EU – mit Blick auf die Produkte, Dienstleistungen und Verfahren – wird in vielerlei Hinsicht gehemmt. Ein wesentlicher Aspekt ist in diesem Zusammenhang das Fehlen von in der gesamten EU anerkannten Zertifizierungssystemen für die Cybersicherheit, die es ermöglichen würden, Produkte für höhere Abwehrfähigkeits-Standards auszulegen und das Marktvertrauen in der EU zu stärken. Die Kommission schlägt daher vor, einen **EU-Rahmen für die Zertifizierung der Cybersicherheit**[18] einzurichten. In diesem Rahmen würde das Verfahren für die Einführung EU-weiter Systeme für die Zertifizierung der Cybersicherheit von Produkten, Dienstleistungen und/oder Systemen festgelegt, wobei für unterschiedliche Nutzungen (z. B. kritische Infrastruktur oder Geräte für Verbraucher) eine entsprechendes Gewährleistungsstufe vorzusehen wäre[19]. Ein solcher Rahmen wäre für die Unternehmen

[16] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

[17] Siehe Artikel 9 der NIS-Richtlinie.

[18] COM(2017) 477.

[19] Die Gewährleistungsstufe gibt Aufschluss darüber, wie streng die durchlaufenen Sicherheitsprüfungen sind; sie steht in der Regel in einem angemessenen Verhältnis zur Höhe der Risiken, die bei den jeweiligen

insofern eindeutig von Vorteil, weil sie dann beim grenzüberschreitenden Handel nicht mehr mehrere Zertifizierungsverfahren absolvieren müssten, sodass sich der administrative und finanzielle Aufwand für sie verringern würde. Durch die Verwendung der vorgeschlagenen Zertifizierungssysteme würde auch das Vertrauen der Verbraucher gestärkt, da Käufer und Nutzer einer entsprechenden Konformitätsbescheinigung Informationen über die Sicherheitseigenschaften der gekauften bzw. genutzten Produkte oder Dienstleistungen entnehmen könnten. Dadurch würde ein hoher Cybersicherheitsstandard zu einem Wettbewerbsvorteil. Dies würde zu einem Anstieg der Abwehrfähigkeit führen, weil IKT-Produkte und -Dienstleistungen formell anhand festgelegter Cybersicherheitsstandards bewertet würden, die in enger Verbindung mit der breiter angelegten, laufenden Arbeit an IKT-Standards ausgearbeitet werden könnten.[20]

Die in dem Rahmen vorgesehenen Zertifizierungssysteme sollen freiwillig und für die Verkäufer und Dienstleistungserbringer mit keinen unmittelbaren regulatorischen Verpflichtungen verbunden sein. Die Zertifizierungssysteme würden nicht im Widerspruch zu geltenden rechtlichen Anforderungen, wie etwa den EU-Rechtsvorschriften zum Datenschutz, stehen.

Nach Einführung des Rahmens wird die Kommission die Interessenträger auffordern, sich vorrangig mit folgenden drei Bereichen zu befassen:

- Sicherheit bei kritischen oder hochsensiblen Anwendungen[21]: Die Systeme, auf die wir in unserem täglichen Leben angewiesen sind – von unseren Pkw bis hin zu den Maschinen in Fabriken, von den größten Systemen etwa in Flugzeugen oder Kraftwerken bis hin zu den kleinsten, zum Beispiel in Medizinprodukten –, sind in zunehmendem Maße digital und miteinander verbunden. Deshalb müssen die entscheidenden IKT-Komponenten in diesen Produkten und Systemen strengen Sicherheitsprüfungen unterzogen werden.
- Cybersicherheit bei weitverbreiteten digitalen Produkten, Netzen, Systemen und Dienstleistungen, die von privaten und öffentlichen Nutzern gleichermaßen für die Abwehr von Angriffen und die Erfüllung rechtlicher Verpflichtungen[22] in Anspruch genommen werden – wie E-Mail-Verschlüsselung, Firewalls und virtuelle private Netze: Die Ausbreitung solcher Instrumente darf auf keinen Fall neue Risikoquellen oder Schwachstellen mit sich bringen.
- Befolgung des Grundsatzes der „eingebauten Sicherheit“ (security by design) bei kostengünstigen, digitalen, vernetzten Massengebrauchsgeräten, die das Internet der Dinge bilden: Über die geplanten Zertifizierungssysteme könnte die Information bereitgestellt werden, dass ein Produkt unter Verwendung aktueller, sicherer Konzeptionsmethoden hergestellt und geeigneten Sicherheitsprüfungen unterzogen wurde und dass die Verkäufer sich verpflichtet haben, im Falle neu entdeckter Sicherheitslücken oder Bedrohungen die Produktsoftware zu aktualisieren.

Bei diesen Prioritäten sollte ein besonderes Augenmerk auf die Entwicklung der Cybersicherheits-Bedrohungslage und auf die Bedeutung der grundlegenden Dienstleistungen

---

Anwendungsbereichen bzw. Funktionen auftreten (d. h. für IKT-Produkte oder -Dienstleistungen, die für hochsensible Anwendungsbereiche bzw. Funktionen bestimmt sind, gilt eine höhere Gewährleistungsstufe).

[20] COM(2016) 176.

[21] Außer wenn andere Unionsrechtsakte bereits eine obligatorische oder freiwillige Zertifizierung vorsehen.

[22] Beispielsweise die Richtlinie (EU) 2016/1148, die Verordnung (EU) 2016/679, die Richtlinie (EU) 2015/2366 und andere vorgeschlagene Rechtsvorschriften wie der europäische Kodex für die elektronische Kommunikation sehen jeweils vor, dass Organisationen geeignete Sicherheitsmaßnahmen ergreifen müssen, um Risiken im Bereich der Cybersicherheit zu begegnen.

in den Bereichen Verkehr, Energie, Gesundheitswesen, Bankwesen, Finanzmarktinfrastrukturen, Trinkwasser oder digitale Infrastruktur[23] gelegt werden.

Wenngleich bei keinem IKT-Produkt oder -System und keiner IKT-Dienstleistung eine Sicherheit von „100 %“ garantiert werden kann, gibt es mehrere bekannte und gut dokumentierte Mängel bei der Konzeption von IKT-Produkten, die für Angriffe ausgenutzt werden können. Wenn die Hersteller von vernetzten Geräten, IT-Software und Ausrüstung den Grundsatz der „eingebauten Sicherheit“ befolgen, dann ist gewährleistet, dass neue Produkte vor der Markteinführung auf Cybersicherheit ausgelegt werden. Dies könnte Bestandteil eines gemeinsam mit der Industrie weiterzuentwickelnden Grundsatzes der „Sorgfaltspflicht“ sein, durch den Sicherheitslücken bei Produkten bzw. Software anhand unterschiedlicher Methoden verringert werden könnten – von der Konzeption über die Erprobung bis hin zur Überprüfung, gegebenenfalls einschließlich einer formellen Überprüfung, langfristige Wartung und den Einsatz sicherer Prozesse für den Entwicklungslebenszyklus, die Entwicklung von Updates und Patches zur Behebung zuvor unentdeckter Schwachstellen sowie rasche Aktualisierung und Reparatur[24]. Dadurch würde auch das Vertrauen der Verbraucher in digitale Produkte gestärkt.

Außerdem muss die wichtige Rolle gewürdigt werden, die dritten Sicherheitsexperten bei der Aufdeckung von Schwachstellen in bestehenden Produkten und Diensten zukommt; daher sollten die Voraussetzungen für eine mitgliedstaatsübergreifende, koordinierte Offenlegung von Sicherheitslücken[25] auf der Grundlage bewährter Verfahren[26] und der einschlägigen Standards[27] geschaffen werden.

Ferner treten in **bestimmten Wirtschaftszweigen** spezifische Probleme auf, für die sektorspezifische Konzepte entwickelt werden sollten. So könnten die allgemeinen Cybersicherheitsstrategien etwa in den Bereichen Finanzdienstleistungen[28], Energie, Verkehr und Gesundheitswesen[29] durch sektorspezifische Strategien ergänzt werden.

Die Kommission hat bereits die spezifischen Herausforderungen hinsichtlich der **Haftung** dargelegt, die sich im Zusammenhang mit neuen Digitaltechnologien[30] ergeben; nach der gegenwärtig laufenden Analyse der Auswirkungen werden die nächsten Schritte im Juni 2018 folgen. Im Zusammenhang mit der Cybersicherheit stellen sich Fragen bezüglich der Haftung für Schaden, die den Unternehmen und Lieferketten entstehen. Wenn diese Fragen nicht

---

[23] Die Sektoren, auf die die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union Anwendung findet.

[24] Cybersicherheit im europäischen digitalen Binnenmarkt, Hochrangige Gruppe wissenschaftlicher Berater, März 2017.

[25] Bei der koordinierten Offenlegung von Sicherheitslücken handelt es sich um eine Form der Zusammenarbeit, die es Sicherheitsexperten ermöglicht bzw. erleichtert, die Schwachstelle dem Eigentümer oder Verkäufer eines Informationssystems zur Kenntnis zu bringen, sodass der betreffende Eigentümer oder Verkäufer diese rechtzeitig ordnungsgemäß überprüfen und beheben kann, bevor Dritte oder die Öffentlichkeit detaillierte Informationen darüber erlangen.

[26] Siehe beispielsweise „Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations“, ENISA, 2016.

[27] ISO/IEC 29147:2014 Information technology -- Security techniques -- Vulnerability disclosure.

[28] Im Rahmen ihrer künftigen Arbeit in Bezug auf Finanztechnologie wird sich die Kommission auch mit dem Thema Cybersicherheit für den Finanzsektor befassen.

[29] Beispielsweise im Energiesektor für die Kombination von sehr alter mit hochmoderner Informationstechnologie, insbesondere mit Blick auf die echtzeitbezogenen Anforderungen des Stromnetzes.

[30] COM(2017) 228.

geklärt werden, wird die Entwicklung eines starken Binnenmarkts für Cybersicherheitsprodukte und -dienstleistungen beeinträchtigt.

Und schließlich hängt die Entwicklung des EU-Binnenmarktes auch davon ab, wie das Thema Cybersicherheit in die Strategien für die Bereiche Handel und Investitionen eingebunden wird. Die Auswirkungen ausländischer Übernahmen in Bezug auf kritische Technologien – wofür die Cybersicherheit ein wichtiges Beispiel ist – sind ein zentraler Aspekt des Rahmens für **die Prüfung ausländischer Direktinvestitionen in der Europäischen Union**[31], der es ermöglichen soll, Investitionen aus Drittstaaten aus Gründen der Sicherheit und der öffentlichen Ordnung zu prüfen. Analog dazu beeinträchtigen in einer Reihe von Drittstaaten bestehende Cybersicherheitsanforderungen in wichtigen Wirtschaftszweigen bereits den Handel mit Waren und Dienstleistungen aus der EU. Der EU-Rahmen für die Cybersicherheitszertifizierung wird die Position Europas auf internationaler Ebene weiter stärken. Gleichzeitig sollten die Bemühungen zur Entwicklung hochsicherer globaler Standards und zum Abschluss von Vereinbarungen über die gegenseitige Anerkennung fortgesetzt werden.

2.3 Vollständige Umsetzung der Richtlinie über die Sicherheit von Netz- und Informationssystemen

Zwar sind nationale Stellen mittlerweile gut gerüstet, Cybersicherheitsbedrohungen zu bekämpfen, doch ist der EU bewusst, wie wichtig es ist, noch höhere Standards zu setzen. Angesichts der zunehmenden Globalisierung, Digitalisierung und Vernetzung von Schlüsselsektoren, wie beispielsweise des Banken-, Energie- oder Verkehrssektors, treffen massive Cybersicherheitsvorfälle selten nur einen Mitgliedstaat.

Die Richtlinie über die Sicherheit von Netz- und Informationssystemen (im Folgenden die „NIS-Richtlinie“) ist die erste unionsweite Rechtsvorschrift zur Cybersicherheit[32]. Sie dient dem Aufbau von Abwehrfähigkeiten, indem die nationalen Cybersicherheitskapazitäten gestärkt werden, eine bessere Zusammenarbeit zwischen den Mitgliedstaaten gefördert wird und indem Unternehmen in wichtigen Wirtschaftssektoren wirksame Risikomanagementverfahren einzuführen und schwere Sicherheitsvorfälle den nationalen Behörden melden müssen. Diese Verpflichtungen gelten auch die Anbieter der folgenden drei Arten zentraler Internetdienste: Cloud Computing, Suchmaschinen und Online-Marktplätze. Ziel ist ein strafferes und systematischeres Konzept sowie ein besserer Informationsfluss.

Die vollständige Umsetzung der Richtlinie durch alle Mitgliedstaaten bis Mai 2018 ist von entscheidender Bedeutung für die Abwehrfähigkeit der EU bei Cyberangriffen. Die Mitgliedstaaten arbeiten in diesem Prozess gemeinsam daran, bis Herbst 2017 Leitlinien herauszugeben, um die Umsetzung, vor allem in Bezug auf die Betreiber wesentlicher Dienste, stärker zu harmonisieren. Die Kommission veröffentlicht als Teil dieses Cybersicherheitspakets auch eine Mitteilung[33], um diese Bemühungen zu unterstützen, indem sie Verfahren vorstellt, die sich in den Mitgliedstaaten bei der Umsetzung der Richtlinie bewährt haben, und darlegt, wie die Richtlinie in der Praxis funktionieren sollte.

---

[31] COM(2017) 478.

[32] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

[33] COM (2017) 476.

Ein Bereich, in dem die Richtlinie ergänzt werden muss, ist der Informationsfluss. So deckt die Richtlinie nur strategische Schlüsselsektoren ab – doch müssten logischerweise alle Interessenträger, die von einem Cyberangriff betroffen sind, in ähnlicher Weise vorgehen, damit die Schwachstellen und Angriffspunkte für Cyberangriffe systematisch bewertet werden können. Zudem stoßen Zusammenarbeit und Informationsaustausch zwischen dem öffentlichen und dem privaten Sektor auf Hindernisse. Regierungen und Behörden geben cybersicherheitsrelevante Informationen nur ungern weiter, da sie eine Gefährdung der nationalen Sicherheit oder der Wettbewerbsfähigkeit befürchten. Privatunternehmen zögern, Informationen über ihre Cyberschwachstellen und die dadurch erlittenen Verluste weiterzugeben, aus Furcht, dass sensible Geschäftsinformationen in falsche Hände gelangen, ihr Ruf leiden könnte oder sie möglicherweise Datenschutzbestimmungen verletzten[34]. Auch gilt es, das Vertrauen zu stärken, damit öffentlich-private Partnerschaften die Zusammenarbeit und den Informationsaustausch auf eine größere Zahl von Sektoren ausweiten können. Beim Aufbau des für die Informationsweitergabe zwischen dem Privatsektor und dem öffentlichen Sektor nötigen Vertrauens kommt den Zentren für den Austausch und die Analyse von Informationen besondere Bedeutung zu. In einzelnen kritischen Sektoren wurden bereits erste Schritte unternommen, indem beispielsweise für die Luftfahrt das Europäische Zentrum für die Cybersicherheit in der Luftfahrt[35] und für den Energiesektor die Informationsaustausch- und -analysezentren[36] aufgebaut wurden. Die Kommission wird dieses Konzept uneingeschränkt über die ENISA unterstützen, wobei vor allem in den in der NIS-Richtlinie genannten Sektoren, die wesentliche Dienste erbringen, schnellere Fortschritte erzielt werden müssen.

2.4 Abwehrfähigkeit durch eine rasche Reaktion im Notfall

Bei einem Cyberangriff lassen sich die Folgen durch eine schnelle und wirksame Reaktion begrenzen. Dies zeigt auch, dass Behörden gegenüber Cyberangriffen nicht machtlos sind und zum Vertrauensaufbau beitragen können. Was die Reaktion der EU-Organe selbst anbelangt, sollten zunächst die Aspekte der Cybersicherheit durchgehend in die bestehenden Mechanismen der EU für das Krisenmanagement eingebunden werden, d. h, in die integrierte EU-Regelung für die politische Reaktion auf Krisen[37], die vom Ratsvorsitz koordiniert wird, und in die allgemeinen Frühwarnsysteme[38]. Ein besonders schwerer Cybersicherheitsvorfall oder -angriff, auf den ein Mitgliedstaat reagieren muss, könnte für diesen einen hinreichenden Grund bieten, die „Solidaritätsklausel“ der EU[39] geltend zu machen.

---

[34] Cybersicherheit im europäischen digitalen Binnenmarkt, Hochrangige Gruppe wissenschaftlicher Berater, März 2017. Ein besonderes Thema sind die Geschäftsgeheimnisse. Hierzu wurde in der im Juli 2016 verabschiedeten Mitteilung über die Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit festgestellt, dass Cyberdiebstähle von Geschäftsgeheimnissen nur zögerlich gemeldet werden, und dass es darauf ankommt, vertrauenswürdige Kanäle für diese Meldungen zu schaffen, um die Vertraulichkeit zu gewährleisten.

[35] https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

[36] Hierbei handelt es sich um Mitgliederorganisationen ohne Erwerbszweck, die von privaten und öffentlichen Rechtspersonen gegründet wurden, um Informationen über Bedrohungen, Risiken, Vermeidung, Abmilderung und Reaktionen im Bereich der Cybersicherheit auszutauschen. Siehe z. B. die Europäischen Zentren für den Informationsaustausch und Analysen im Energiesektor (http://www.ee-isac.eu).

[37] Dies ermöglicht die Koordinierung der Reaktionen auf massive sektorübergreifende Krisen auf höchstem politischem Niveau.

[38] Diese ermöglichen die interne Informationsweitergabe und Koordinierung über sich abzeichnende sektorübergreifende Krisen oder absehbare oder unmittelbar bevorstehende Bedrohungen, die eine Maßnahme auf EU-Ebene erfordern.

[39] Nach Artikel 222 des Vertrags über die Arbeitsweise der Europäischen Union.

Eine schnelle und wirksame Reaktion erfordert auch einen Mechanismus für den zügigen Informationsaustausch zwischen allen wichtigen Akteuren auf nationaler und EU-Ebene, was wiederum eine klare Zuweisung von Aufgaben und Zuständigkeiten erfordert. Die Kommission hat Einrichtungen und Mitgliedstaaten zu einem Konzeptentwurf konsultiert, wie auf Ebene der Union und der Mitgliedstaaten ein wirksames Verfahren für eine operative Reaktion auf massive Cybersicherheitsvorfälle zur Verfügung gestellt werden kann. In dem im Rahmen dieses Pakets als Empfehlung vorgelegten **Konzeptentwurf**[40] wird erläutert, wie die Cybersicherheit durchgängig in die bestehenden Mechanismen der EU für das Krisenmanagement einbezogen werden kann, und es werden die Ziele und Modalitäten der Zusammenarbeit zwischen den Mitgliedstaaten, aber auch zwischen den Mitgliedstaaten und den einschlägigen Organen, Dienststellen, Agenturen und sonstigen Stellen der EU[41] für den Fall von massiven Cybersicherheitsvorfällen und -krisen festgelegt. Die Empfehlung fordert zudem die Mitgliedstaaten und EU-Organe dazu auf, für die praktische Umsetzung des Konzeptentwurfs einen EU-Rahmen für die Reaktion auf Cybersicherheitskrisen einzurichten. Dieser Konzeptentwurf wird regelmäßig im Rahmen von (Cyber-)Krisenmanagementübungen auf den Prüfstand gestellt[42] und bei Bedarf aktualisiert werden.

Da sich Cybersicherheitsvorfälle erheblich auf das Funktionieren der Volkswirtschaften und den Alltag der Menschen auswirken können, wäre die Einrichtung eines **Cybersicherheits-Notfallfonds** zu prüfen – ähnlich den Krisenmechanismen in anderen Bereichen der EU-Politik. Damit könnten Mitgliedstaaten während oder nach schwerwiegenden Sicherheitsvorfällen EU-Hilfe beantragen, sofern der betreffende Mitgliedstaat bereits vor einem solchen Sicherheitsvorfall ein umsichtiges Cybersicherheitssystem eingerichtet hat, das u. a. eine vollständige Umsetzung der NIS-Richtlinie, ein ausgereiftes Risikomanagementsystem und nationale Aufsichtsregelungen beinhaltet. Mit Hilfe eines solchen Fonds, der die bereits bestehenden Mechanismen für das Krisenmanagement auf EU-Ebene ergänzt, könnten im Interesse der Solidarität Mittel für eine rasche Reaktion freigegeben und bestimmte Notfallmaßnahmen finanziert werden, wie beispielsweise der Austausch der betroffenen Geräte oder der Einsatz von Abhilfe- oder Reaktionsmaßnahmen, wobei über den EU-Katastrophenschutzmechanismus auf nationalen Sachverstand zurückgegriffen werden kann.

2.5 Ein Cybersicherheits-Kompetenznetz mit einem Europäischen Kompetenzzentrum für Cybersicherheitsforschung

Die technischen Werkzeuge für die Cybersicherheit sind nicht nur ein strategisches Gut, sondern stellen auch Schlüsseltechnologien für das künftige Wachstum dar. Es liegt im strategischen Interesse der EU, dass sie die Kapazitäten wahrt und weiterentwickelt, die zur Sicherung ihrer Digitalwirtschaft, Gesellschaft und Demokratie von entscheidender Bedeutung sind, damit kritische Hardware und Software geschützt und zentrale Cybersicherheitsdienste angeboten werden können.

Die 2016 gegründete öffentlich-private Partnerschaft zur Cybersicherheit[43] war ein erster wichtiger Schritt, der bis 2020 bis zu 1,8 Mrd. EUR an Investitionen mobilisieren wird. Der

[40] C(2017) 6100.

[41] Hierunter fallen beispielsweise Europol, die ENISA, das IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) und das EU-Zentrum für Informationsgewinnung und -analyse (INTCEN).

[42] Übungen, die beispielsweise von der ENISA organisiert werden: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

[43] C(2016) 4400 final.

Vergleich mit dem Umfang der Investitionen, die derzeit in anderen Teilen der Welt getätigt werden[44], macht jedoch deutlich, dass die EU auf diesem Gebiet mehr unternehmen und die Fragmentierung der in der EU vorhandenen Kapazitäten überwinden muss.

Angesichts der Komplexität der Cybersicherheitstechnik, der Höhe des erforderlichen Investitionsvolumens und der Notwendigkeit, unionsweit funktionierende Lösungen zu finden, hat die EU einen Mehrwert zu bieten. Aufbauend auf den Arbeiten der Mitgliedstaaten und der öffentlich-privaten Partnerschaft könnte als nächster Schritt die Cybersicherheitskapazität der EU über ein **Netz von Cybersicherheitskompetenzzentren**[45] unter dem Dach des **Europäischen Kompetenzzentrums für Cybersicherheitsforschung** gestärkt werden. Dieses Netz und sein Zentrum dürften die Entwicklung und Verbreitung von Cybersicherheitstechnik fördern und die Bemühungen um den Aufbau von Kapazitäten in diesem Bereich auf EU-Ebene und auf nationaler Ebene ergänzen. Die Kommission wird eine Folgenabschätzung durchführen, um zu untersuchen, welche Optionen – wie beispielsweise die Einrichtung eines gemeinsamen Unternehmens – zur Verfügung stehen, um diese Struktur im Jahr 2018 aufbauen zu können.

In einem ersten Schritt und als Grundlage für künftige Überlegungen wird die Kommission vorschlagen, im Rahmen von Horizont 2020 eine Pilotphase durchzuführen, damit sich die nationalen Zentren zu einem Netz zusammenschließen und so eine neue Dynamik bei der Entwicklung von Kompetenz und Technik im Bereich der Cybersicherheit entfalten können. Sie schlägt hierfür eine kurzfristige Finanzspritze von 50 Mio. EUR vor. Diese Maßnahme ergänzt die laufende Realisierung der öffentlich-privaten Partnerschaft zur Cybersicherheit.

Zunächst wird die Bündelung und Gestaltung der Forschungsanstrengungen das Hauptaugenmerk des Netzes und des Zentrums bilden. Zur Unterstützung des Ausbaus der industriellen Fähigkeiten könnte das Zentrum bei internationalen Projekten als Leiter das Management dieser Fähigkeiten übernehmen. Hiervon könnten zusätzliche Anreize ausgehen, die der Innovation und globalen Wettbewerbsfähigkeit der EU-Unternehmen bei der Entwicklung der Digitaltechnik der nächsten Generation zugute kommen – beispielsweise in Bereichen wie der künstlichen Intelligenz, Quanteninformatik, Blockchain und sichere digitale Identitäten – und sicherstellen, dass EU-Unternehmen Zugang zu Massendaten erhalten. All diese Aspekte sind von zentraler Bedeutung für die Cybersicherheit in der Zukunft. Das Zentrum könnte auch auf die Arbeiten der EU zur Ausweitung der Infrastruktur für Hochleistungsrechner zurückgreifen, die für die Auswertung großer Datenmengen, eine rasche Ver- und Entschlüsselung von Daten, die Überprüfung von Identitäten, die Simulierung von Cyberangriffen und die Auswertung von Videomaterial unerlässlich ist[46].

Das Netz der Kompetenzzentren könnte auch über Fähigkeiten verfügen, die Industrie mit Tests und Simulationen für die in Abschnitt 2.2. erläuterte Cybersicherheitszertifizierung zu unterstützen. Seine Einbeziehung in sämtliche Aktivitäten der EU im Bereich der Cybersicherheit würde sicherstellen, dass seine Ausrichtung sich ständig am aktuellen Bedarf orientiert. Das Ziel des Zentrums würde darin bestehen, nicht nur in der Technik und bei den Cybersicherheitssystemen auf hohe Cybersicherheitsstandards hinzuwirken, sondern auch

---

[44] Die USA werden allein auf das Jahr 2017 gerechnet 19 Mrd. USD und damit 35 % mehr als im Jahr 2016 in die Cybersicherheit investieren. Das Weiße Haus, Pressestelle: 'Fact Sheet: Cybersecurity National Action Plan', vom 9. Februar 2016.

[45] Das Netz würde bereits in den Mitgliedstaaten bestehende Cybersicherheitszentren erfassen und in Zukunft erweitert werden können, wobei es sich bei den Mitgliedern dieses Netzes in der Regel um öffentliche Forschungsorganisationen und Labors handeln wird.

[46] COM(2012) 45 final und COM(2016) 178 final.

beim Aufbau von Spitzenkompetenzen von Fachkräften, indem die nationalen Bemühungen zur Vermittlung digitaler Kompetenzen mit Lösungen und Mustern unterstützt werden. Hierzu könnte es auch die Cybersicherheitsfähigkeiten auf EU-Ebene stärken, indem Synergien vor allem mit der ENISA, CERT-EU, Europol, dem möglichen künftigen Cybersicherheits-Notfallfonds und den nationalen CSIRTs genutzt werden.

Besondere Aufmerksamkeit muss das Kompetenznetz der Tatsache widmen, dass es in Europa an Kapazitäten zur Bewertung der **Verschlüsselung** von Produkten und Diensten mangelt, die von Bürgern, Unternehmen und Regierungen im Binnenmarkt genutzt werden. Eine leistungsstarke Verschlüsselung ist die Grundlage sicherer digitaler Identifizierungssysteme, die für eine wirksame Cybersicherheit von zentraler Bedeutung sind[47]. Sie sorgt zudem dafür, dass das geistige Eigentum sowie die Grundrechte, wie die Meinungsfreiheit und der Schutz personenbezogener Daten, gewahrt werden und die Sicherheit des elektronischen Geschäftsverkehrs gewährleistet ist[48].

Da die zivilen und verteidigungsbezogenen Segmente des EU-Cybersicherheitsmarktes mit den gleichen Herausforderungen konfrontiert sind[49] und Technologien mit doppeltem Verwendungszweck einsetzen, ist eine enge Zusammenarbeit in kritischen Bereichen geboten, weshalb in einer zweiten Phase das Netz und sein Zentrum unter vollständiger Wahrung der Bestimmungen des EU-Vertrags über die Gemeinsame Sicherheits- und Verteidigungspolitik um eine Cyberabwehrdimension ergänzt werden könnten. Genauso wie die technologische Ausrichtung des Netzes könnte seine Verteidigungsdimension die Zusammenarbeit der Mitgliedstaaten im Bereich der Cyberabwehr beschleunigen – etwa durch Informationsaustausch, eine abgestimmte Lageerfassung, den Aufbau von Fachwissen und koordinierte Reaktionen – und die Mitgliedstaaten bei der Entwicklung gemeinsamer Fähigkeiten unterstützen. Es könnte den Mitgliedstaaten auch als Plattform dafür dienen, Schwerpunkte der EU-Cyberabwehr festzulegen, gemeinsame Lösungen zu untersuchen, zur Entwicklung gemeinsamer Strategien beizutragen und gemeinsame Ausbildungsmaßnahmen, Übungen und Tests zur Cyberabwehr auf europäischer Ebene zu erleichtern sowie die Arbeiten zu Taxonomien und Normen der Cyberabwehr zu unterstützen, wobei dem Zentrum eine unterstützende und beratende Rolle zukommt. Hierzu müsste das Zentrum eng und in vollständiger Komplementarität mit der Europäischen Verteidigungsagentur bei der Cyberabwehr und mit der ENISA im Bereich der Cyberabwehrfähigkeit zusammenarbeiten. Diese Verteidigungsdimension würde den Prozess berücksichtigen, der mit dem Reflexionspapier zur Zukunft der europäischen Verteidigung in Gang gesetzt wurde.

Die für die Cyberabwehr benötigte hohe Abwehrfähigkeit erfordert eine besondere Ausrichtung der Forschungs- und Technologieanstrengungen. Die von Unternehmen entwickelten Projekte und Technologien zur Cyberabwehr könnten sowohl für die Forschungs- als auch die Entwicklungsphase Mittel aus dem Europäischen Verteidigungsfonds erhalten. [50]Von besonderer Relevanz in diesem Zusammenhang könnten einzelne Bereiche sein, wie auf Quanteninformatik gestützte Verschlüsselungssysteme, die

---

[47] Die Kommission wird im Rahmen von Horizont 2020 einen neuen Horizont-Preis für die besten innovativen Lösungen für eine nahtlose Online-Authentifizierung ausloben, der mit 4 Mio. EUR dotiert sein wird.

[48] Cybersicherheit im europäischen digitalen Binnenmarkt, Hochrangige Gruppe wissenschaftlicher Berater, März 2017.

[49] „Study on synergies between the civilian and the defence cybersecurity markets“ (Optimity; SMART 2014-0059).

[50] Bereits jetzt räumt das Europäische Entwicklungsprogramm für die Verteidigungsindustrie Projekten der Cyberabwehr Priorität ein, die auch eines der Themen einer 2018 zu veröffentlichenden Aufforderung zur Einreichung von Vorschlägen sein wird.

Erfassung von Cybersicherheitslagen, biometrische Zugangskontrollsysteme, fortgeschrittene Erkennung anhaltender Bedrohungen oder Daten-Mining. Der Hohe Vertreter, die Europäische Verteidigungsagentur und die Kommission werden die Mitgliedstaaten bei der Ermittlung der Bereiche unterstützen, in denen gemeinsame Cybersicherheitsprojekte für eine Finanzierung durch den Europäischen Verteidigungsfonds in Frage kommen.

2.6 Aufbau einer starken EU-Basis für Cyberfähigkeiten

Eine wichtige Dimension der Cybersicherheit ist die Bildung. Eine Cybersicherheit, die ihren Namen verdient, hängt in starkem Maße von den Fähigkeiten der betreffenden Personen ab. In Europa werden im Privatsektor bis zum Jahr 2022 jedoch voraussichtlich 350 000 Fachkräfte mit entsprechenden Cybersicherheitsfähigkeiten fehlen[51]. Die Ausbildung im Bereich der Cybersicherheit sollte auf allen Ebenen weiterentwickelt werden – angefangen bei der regelmäßigen Schulung von im Bereich der Cybersicherheit tätigen Arbeitnehmern, einer zusätzlichen Cybersicherheits-Weiterbildung aller IKT-Fachkräfte bis hin zu neuen Lehrplänen zur Cybersicherheit. Eingerichtet werden sollten leistungsstarke akademische Zentren, die die Nachfrage nach einer forcierten Aus- und Weiterbildung decken und die sich am Europäischen Kompetenzzentrum für Cybersicherheitsforschung und an der ENISA orientieren könnten. Es sollte eine Selbstverständlichkeit werden, dass Sicherheitsgrundsätze bereits bei der Konzeption von IKT-Produkten und -Systemen berücksichtigt werden. Die Ausbildung im Bereich der Cybersicherheit sollte sich nicht auf IT-Fachkräfte beschränken, sondern auch durchgängig in die Lehrpläne anderer Bereiche aufgenommen werden, etwa in die Lehrpläne für Ingenieure, des Business Management oder für Juristen, aber auch für sektorspezifische Ausbildungswege. Schließlich sollten Lehrer und Schüler der Primar- und Sekundarschulen beim Erwerb digitaler Kompetenzen für die Cyberkriminalität und die Cybersicherheit sensibilisiert werden.

Die EU sollte zusammen mit den Mitgliedstaaten diese Aufgaben unterstützen, indem aufbauend auf den Arbeiten der Koalition für digitale Kompetenzen und Arbeitsplätze[52] beispielsweise in die Ausbildung von Lehrlingen in KMU die Cybersicherheit als Ausbildungsinhalt aufgenommen wird.

2.7 Förderung der Cyber-Hygiene und Sensibilisierung

Da 95 % der Sicherheitsvorfälle wohl auf „eine Form menschlichen Versagens – beabsichtigt oder nicht“[53] zurückzuführen sind, spielt der Faktor Mensch eine wichtige Rolle. Damit trägt jeder Verantwortung für die Cybersicherheit. Dies bedeutet auch, dass sich jeder Einzelne, Unternehmen und öffentliche Verwaltungen in ihrem Verhalten ändern müssen, damit sichergestellt ist, dass jeder die Bedrohung kennt und mit den notwendigen Werkzeugen und Fähigkeiten ausgestattet ist, um Angriffe schnell erkennen und sich aktiv dagegen schützen zu können. Die Menschen müssen sich die Cyber-Hygiene zur Gewohnheit werden lassen und Unternehmen und Organisationen müssen geeignete risikobasierte Cybersicherheitsprogramme festlegen und regelmäßig aktualisieren, um mit der sich weiterentwickelnden Risikolandschaft Schritt zu halten.

Nach der NIS-Richtlinie sind die Mitgliedstaaten nicht nur dafür zuständig, Informationen über Cyberangriffe auf EU-Ebene auszutauschen, sondern auch für die Einführung ausgereifter nationaler Cybersicherheitsstrategien und -grundlagen für die Sicherheit von

---

[51] „Global Information Security Workforce Study“ 2017. Weltweit fehlen 1,8 Mio. Fachkräfte.

[52] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

[53] IBM „The Cybersecurity Intelligence Index“ 2014, zitiert im „Securitymagazine.com“, 19. Juni 2014.

Netz- und Informationssystemen. Öffentliche Verwaltungen auf EU- und nationaler Ebene sollten zudem eine wichtige Rolle dabei spielen, diese Bemühungen voranzutreiben.

Zunächst sollten die Mitgliedstaaten eine maximale Verfügbarkeit der Cybersicherheitswerkzeuge für Unternehmen und Privatpersonen gewährleisten. Insbesondere sollte mehr für die Prävention von Cyberkriminalität und die Abmilderung ihrer Folgen für die Endnutzer getan werden. So gibt es bereits bei Europol die „NoMoreRansom"-Kampagne[54], die aus der engen Zusammenarbeit zwischen Vollzugsbehörden und Unternehmen der Cybersicherheitsbranche entstanden ist, um Nutzer darin zu unterstützen, den Befall ihrer Computer mit Ransomeware zu vermeiden und Daten zu entschlüsseln, wenn sie Opfer eines Angriffs geworden sind. Solche Systeme sollten auch für andere Arten von Schadsoftware in anderen Bereichen eingeführt werden. Die EU sollte ein Portal entwickeln, das als **einzige Anlaufstelle all diese Werkzeuge zusammenbringt**, die Nutzer in Fragen der Vermeidung und Erkennung von Schadsoftware berät und mit Meldemechanismen verlinkt.

Zweitens sollten die Mitgliedstaaten bei der **Entwicklung elektronischer Behördendienste schneller und verstärkt auf Werkzeuge setzen, die die Cybersicherheit erhöhen** und hierbei auch das Kompetenznetz in vollem Umfang nutzen. Aufbauend auf dem EU-Rahmen über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt[55], der seit 2016 in Kraft ist und für ein berechenbares Rechtsumfeld für sichere und nahtlose elektronische Transaktionen zwischen Unternehmen, Privatpersonen und Behörden sorgt, sollte die Festlegung sicherer Identifizierungsmittel gefördert werden. Darüber hinaus sollten öffentliche Einrichtungen, vor allem solche, die wesentliche Dienste anbieten, sicherstellen, dass ihr Personal in allen für die Cybersicherheit relevanten Bereichen geschult ist.

Drittens sollten die Mitgliedstaaten dafür sorgen, dass bei **Sensibilisierungskampagnen**, die sich beispielsweise an Schulen, Hochschulen, Unternehmen und Forschungseinrichtungen richten, die Cybersicherheit einen Schwerpunkt bildet. Die gemeinsamen Kommunikationsbemühungen auf EU- und nationaler Ebene während des Monats der Cybersicherheit, der jedes Jahr im Oktober unter Federführung der ENISA stattfindet, werden verstärkt, um eine größere Reichweite zu erlangen. Wichtig ist auch die Schärfung des Bewusstseins für über soziale Medien verbreitete **Desinformationskampagnen und Falschmeldungen**, die auf eine Unterminierung demokratischer Prozesse und europäischer Werte abzielen. Zwar liegt die Verantwortung weiterhin bei den Mitgliedstaaten – auch für die Wahlen zum Europäischen Parlament – doch die Bündelung von Fachwissen und der Erfahrungsaustausch auf europäischer Ebene haben bereits dazu beigetragen, gezielt Maßnahmen einzuleiten[56].

Auch die Wirtschaft im Allgemeinen ist gefordert, hier allerdings vor allem die Anbieter und Hersteller digitaler Dienste. Sie muss die Nutzer (Privatpersonen, Unternehmen und öffentliche Verwaltungen) mit Werkzeugen unterstützen, die es ihnen ermöglichen, die

---

54 https://www.nomoreransom.org/.

55 Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, verabschiedet am 23. Juli 2014. Auch die Europäische Kommission bietet über die Fazilität „Connecting Europe" Bausteine und Werkzeuge für die Interoperabilität von eID und elektronischer Signatur (z. B. Listen vertrauenswürdiger Browser).

56 So wurde 2015 von den Mitgliedstaaten und dem Hohen Vertreter die East StratCom Task Force eingesetzt, um sich mit Russlands laufender Desinformationskampagne zu befassen. Das Team entwickelt Kommunikationsprodukte und Kampagnen, die darauf ausgerichtet sind, in den Regionen der Östlichen Partnerschaft die EU-Politik zu erläutern.

Verantwortung für ihr Online-Handeln zu übernehmen, und deutlich machen, dass die Pflege der Cyber-Hygiene ein unerlässlicher Teil des Verbraucherangebots ist[57]. Um Schwachstellen erkennen und beheben zu können, sollten sich die Unternehmen um interne Prozesse bemühen, mit denen sich Schwachstellen, unabhängig davon, ob deren Ursache in dem betreffenden Unternehmen selbst oder außerhalb dieses Unternehmens liegt, untersucht, eingeordnet und behoben werden können.

Hauptmaßnahmen

- Vollständige Umsetzung der Richtlinie über die Sicherheit von Netz- und Informationssystemen;
- rasche Annahme der Verordnung über das neue Mandat der ENISA und einen europäischen Zertifizierungsrahmen durch das Europäische Parlament und den Rat[58];
- eine gemeinsame Initiative von Kommission und Wirtschaft zur Festlegung des Grundsatzes der „Sorgfaltspflicht" im Hinblick auf die Reduzierung von Produkt- oder Softwareschwachstellen und die Förderung der „konstruktiven Sicherheit";
- zügige Umsetzung des Konzeptentwurfs für eine grenzübergreifende Reaktion auf schwerwiegende Sicherheitsvorfälle;
- Einleitung einer Folgenabschätzung zur Untersuchung der Möglichkeit für einen von der Kommission 2018 vorzulegenden Vorschlag für den Aufbau eines Netzes von Cybersicherheitskompetenzzentren und eines Europäischen Kompetenzzentrums für Cybersicherheitsforschung;
- Unterstützung der Mitgliedstaaten bei der Ermittlung der Bereiche, in denen gemeinsame Cybersicherheitsprojekte für eine Förderung durch den Europäischen Verteidigungsfonds in Frage kommen;
- Einrichtung einer unionsweiten zentralen Anlaufstelle für Opfer von Cyberangriffen, die Informationen über die neuesten Bedrohungen zur Verfügung stellt sowie praktische Beratung und Werkzeuge für die Cybersicherheit anbietet;
- Maßnahmen der Mitgliedstaaten, die Cybersicherheit durchgängig in Bildungsprogramme, in elektronische Behördendienste und in Sensibilisierungskampagnen aufzunehmen;
- Maßnahmen der Wirtschaft, ihr Personal in Fragen der Cybersicherheit fortzubilden und das Konzept der „konstruktiven Sicherheit" auf ihre Produkte, Dienste und Prozesse anzuwenden.

3. SCHAFFUNG EINES EU-RAHMENS ZUR WIRKSAMEN ABSCHRECKUNG

Eine wirkungsvolle Abschreckung setzt einen Rahmen voraus, dessen Maßnahmen glaubwürdig sind und potenzielle Cyberkriminelle und Angreifer abschrecken. Solange die Urheber von Cyberangriffen – ob es sich dabei um Staaten oder andere Angreifer handelt – nicht mehr zu befürchten haben, als dass ihr Vorhaben misslingt, werden sie kaum davon ablassen. Eine wirksamere Strafverfolgung mit Schwerpunkt auf Enttarnung, Rückverfolgbarkeit und Verfolgung von Cyberkriminellen ist für eine wirksame Abschreckung von grundlegender Bedeutung. Zusätzlich dazu muss die EU ihre Mitgliedstaaten beim Aufbau von Cybersicherheitskapazitäten mit doppeltem Verwendungszweck unterstützen. Um bei den Cyberangriffen eine Trendwende einzuleiten, muss die Gefahr, gefasst und strafrechtlich sanktioniert zu werden, zunehmen. Cyberangriffe

[57] Einige Hersteller sind bereits mit diesem Konzept der „konstruktiven Sicherheit" vertraut, das sich in einigen europäischen Produktvorschriften findet (wie z. B. in der Maschinenrichtlinie 2006/42/EG).

[58] COM (2017) 477.

sollten umgehend strafrechtliche Ermittlungen nach sich ziehen. Die Urheber sollten vor Gericht gestellt werden oder es sollten angemessene politische bzw. diplomatische Reaktionen folgen. Bei einer größeren Krise mit bedeutenden internationalen und verteidigungspolitischen Implikationen könnte die Hohe Vertreterin dem Rat Handlungsoptionen vorlegen.

Ein Schritt zur Verbesserung der strafrechtlichen Verfolgung von Cyberangriffen wurde bereits 2013 mit dem Erlass der Richtlinie über Angriffe auf Informationssysteme[59] unternommen. Darin wurden Mindestvorschriften für die Festlegung von Straftaten und Strafen bei Angriffen auf Informationssysteme festgelegt und operative Maßnahmen zur Verbesserung der behördlichen Zusammenarbeit bereitgestellt. Die Richtlinie hat bei der Angleichung der Einstufung von Cyberangriffen als Straftaten in den Mitgliedstaaten erhebliche Fortschritte bewirkt, was die grenzüberschreitende Zusammenarbeit der Strafverfolgungsbehörden, die diese Art von Straftaten untersuchen, erleichtert. Es besteht allerdings noch Spielraum, um das Potenzial der Richtlinie durch vollständige Umsetzung aller Bestimmungen durch die Mitgliedstaaten voll auszuschöpfen[60]. Die Kommission wird die Mitgliedstaaten auch weiterhin bei der Umsetzung der Richtlinie unterstützen, sieht bei der Richtlinie derzeit aber keinen Änderungsbedarf.

3.1 Identifizierung böswilliger Akteure

Um unsere Chance, die Verantwortlichen vor Gericht zu stellen, zu erhöhen, müssen wir unsere Fähigkeit zur Identifizierung der Urheber von Cyberangriffen dringend verbessern. Das Auffinden von Informationen, die bei Ermittlungen gegen Cyberkriminalität helfen – meistens in Form digitaler Spuren – stellt für die Strafverfolgungsbehörden eine große Herausforderung dar. Aus diesem Grund müssen wir unsere technologischen Kompetenzen für wirkungsvolle Ermittlungen erhöhen und zu diesem Zweck unter anderem das Europäische Zentrum zur Bekämpfung der Cyberkriminalität bei Europol mit weiteren Experten aufstocken. Europol ist bei der Unterstützung der Mitgliedstaaten bei Mehr-Länder-Ermittlungen zu einem zentralen Akteur geworden. Es sollte zu einem Kompetenzzentrum ausgebaut werden, auf das die Strafverfolgungsbehörden der Mitgliedstaaten bei Ermittlungen im Internet und Cyber-Forensik zurückgreifen können.

Die weitverbreitete Praxis, zahlreiche – mitunter Tausende – Nutzer einer IP-Adresse zuzuordnen, macht Ermittlungen gegen böswilliges Verhalten im Internet technisch außerordentlich schwierig. Dadurch muss auch bei schweren Straftaten, wie sexuellem Missbrauch von Kindern, zur Ermittlung eines einzigen Straftäters mitunter eine große Anzahl von Nutzern durchleuchtet werden. Die EU wird sich deshalb für die Einführung des neuen Protokolls (IPv6) einsetzen, das die Zuordnung einer einzigen IP-Adresse pro Nutzer ermöglicht, was für die Strafverfolgung und Ermittlungen im Bereich der Cybersicherheit mit klaren Vorteilen verbunden ist. Als ersten Schritt in diese Richtung wird die Kommission in all ihren Politikbereichen die Umstellung auf IPv6 vorschreiben, worunter auch Anforderungen im öffentlichen Auftragswesen und in der Projekt- und Forschungsfinanzierung fallen, und die notwendigen Schulungsmaterialien fördern. Zusätzlich dazu sollten es die Mitgliedstaaten in Betracht ziehen, mit Internetdienstanbietern freiwillige Vereinbarungen zur Beschleunigung der Einführung von IPv6 zu schließen.

[59] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme.

[60] COM(2017) 474.

Belgien nimmt bei der Einführung des IPv6 die weltweite Spitzenposition ein[61]*, was nicht zuletzt auf die Zusammenarbeit zwischen öffentlichen und privaten Stellen zurückzuführen ist: so haben sich die maßgeblichen Akteure im Rahmen einer Selbstregulierungsmaßnahme darauf verständigt, IP-Adressen auf maximal 16 Nutzer zu begrenzen, was die Umstellung auf IPv6 gefördert hat.*[62]

Ganz allgemein sollte die Rechenschaftslegung im Internet weiter gefördert werden. Das heißt, es sollten Maßnahmen gefördert werden, die dem Missbrauch von Domänennamen für die Verbreitung nicht angeforderter Mitteilungen oder für Phishing-Angriffe vorbeugen. Zu diesem Zweck wird die Kommission im Einklang mit den Bemühungen der Zentralstelle für die Vergabe von Internet-Namen und -Adressen[63] auf die Verbesserung von Funktionsweise und Verfügbarkeit sowie Genauigkeit der im Domänennamen und in den IP WHOIS[64]-Systemen enthaltenen Angaben hinarbeiten.

3.2 Beschleunigung der Strafverfolgungsmaßnahmen

Wirksame **Ermittlungen** und eine wirksame **Verfolgung** der durch den Cyberraum ermöglichten Kriminalität stellen einen wesentlichen Abschreckungsfaktor dar. Doch muss der heute bestehende Verfahrensrahmen besser an das Internetzeitalter angepasst werden[65]. Die Geschwindigkeit von Cyber-Angriffen kann unsere Verfahren überfordern und insbesondere eine zügige grenzüberschreitende Zusammenarbeit erfordern. Zu diesem Zweck wird die Kommission wie in der Europäischen Sicherheitsagenda angekündigt Anfang 2018 Vorschläge zur **Erleichterung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln** vorlegen. Parallel dazu führt die Kommission derzeit praktische Maßnahmen durch, die bei strafrechtlichen Ermittlungen den Zugang zu elektronischen Beweismitteln verbessern sollen und die auch die Finanzierung von Schulungen für die grenzüberschreitende Zusammenarbeit, die Entwicklung einer elektronischen Plattform für den Informationsaustausch innerhalb der EU und die Standardisierung der von den Mitgliedstaaten bei der justiziellen Zusammenarbeit verwendeten Formulare einschließen.
Ein weiteres Hindernis für eine wirksame Verfolgung stellen die unterschiedlichen forensischen Verfahren dar, nach denen in den Mitgliedstaaten bei Ermittlungen gegen Cyberkriminalität elektronische Beweismittel gesammelt werden. Dem könnte durch Bemühungen um Festlegung gemeinsamer forensischer Standards entgegengewirkt werden. Doch müssen nicht nur Rückverfolgbarkeit und Zuweisung gefördert, sondern zusätzlich dazu auch die forensischen Kapazitäten verstärkt werden. Ein Schritt in diese Richtung bestünde darin, die forensischen Kapazitäten bei Europol weiter auszubauen und zu diesem Zweck die vorhandenen Budget- und Humanressourcen des bei Europol angesiedelten Europäischen Zentrums zur Bekämpfung der Cyberkriminalität dem wachsenden Bedarf an operativer Unterstützung bei grenzübergreifenden Ermittlungen gegen Cyberkriminalität anzupassen. Zum anderen könnte dem oben dargelegten technischen Fokus im Bereich der

---

61 https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

62 http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

63 Die Zentralstelle für die Vergabe von Internet-Namen und -Adressen (Internet Corporation for Assigned Names and Numbers, ICANN) ist eine Einrichtung ohne Erwerbszweck, die die Pflege mehrerer Datenbanken zu den Namensräumen im Internet und deren Verfahren koordiniert.

64 Ein Frage- und Antwortprotokoll, das in großem Umfang bei der Abfrage von Datenbanken, in denen die registrierten Nutzer einer Internetressource oder deren Rechtsnachfolger gespeichert sind, eingesetzt wird.

65 So wechselte der (virtuelle) zentrale Avalanche-Botnetz-Command-und-Control-Server alle fünf Minuten seine physischen Server und Domänen, um nur ein Beispiel zu nennen.

Verschlüsselung durch Untersuchung der Frage Rechnung getragen werden, wie deren Missbrauch durch Straftäter bei der Bekämpfung schwerer Straftaten wie Terrorismus und Cyberkriminalität zu erheblichen Herausforderungen führt. Die Ergebnisse der derzeitigen Überlegungen zur **Rolle der Verschlüsselung bei strafrechtlichen Ermittlungen**[66] wird die Kommission bis Oktober 2017 vorlegen[67].

Im Kontext des Grenzen ignorierenden Internets bietet der durch das **Budapester Übereinkommen über Computerkriminalität**[68] des Europarates geschaffene Rahmen für die internationale Zusammenarbeit einer Gruppe sehr unterschiedlicher Länder die Möglichkeit, bei ihren nationalen Rechtsvorschriften zur Bekämpfung der Cyberkriminalität einen optimalen rechtlichen Standard zu nutzen. Zurzeit wird über ein mögliches Zusatzprotokoll nachgedacht[69], das auch die nützliche Gelegenheit bieten könnte, die Frage des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln in einem internationalen Kontext anzuschneiden. Die EU ruft alle Länder auf, kein neues internationales Rechtsinstrument für den Bereich Cyberkriminalität zu schaffen, sondern stattdessen angemessene nationale Vorschriften zu erarbeiten und die Zusammenarbeit innerhalb des bestehenden internationalen Rahmens fortzusetzen.

Die hohe Verfügbarkeit von Anonymisierungsprogrammen erleichtert es Straftätern, sich zu verstecken. Das „**Darknet**“[70] hat Straftätern neue Zugriffsmöglichkeiten auf kinderpornografisches Material, Drogen oder Feuerwaffen eröffnet – oftmals nur mit geringem Risiko, gefasst zu werden[71]. Auch stellt es heute eine wichtige Quelle für die Beschaffung der bei Cyberkriminalität verwendeten Werkzeuge, wie Schadsoftware und Hackerinstrumente dar. Gemeinsam mit den maßgeblichen Akteuren wird die Kommission die nationalen Vorgehensweisen analysieren, um neue Lösungen zu finden. Europol sollte Ermittlungen zum Darknet erleichtern und unterstützen, drohende Gefahren beurteilen, das jeweils zuständige Land bestimmen helfen und eine Rangliste der Hochrisikofälle erstellen, während die EU bei der Koordinierung der internationalen Maßnahmen eine führende Rolle spielen kann[72].
Ein Bereich, in dem die Cyberkriminalität zunimmt, ist die betrügerische Nutzung von Kreditkartendaten oder anderer elektronischer Zahlungsmittel. Die durch Cyberangriffe auf Online-Händler oder andere rechtmäßige Unternehmungen erlangten Zahlungsdaten werden

---

66 Vorsitz des Rates, Ergebnis der Tagung des Rates Justiz und Inneres vom 8. und 9. Dezember 2016, Nr. 15391/16.

67 Achter Fortschrittsbericht „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion“, COM(2017) 354 final vom 29. Juni 2017.

68 Das Übereinkommen ist der erste internationale Vertrag über Straftaten, die über das Internet und sonstige Computernetze begangen werden; Gegenstand sind insbesondere Urheberrechtsverletzungen, computerbezogener Betrug, Kinderpornografie und Verletzungen der Netzwerksicherheit. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 2017 hatten 55 Länder das Übereinkommen des Europarats über Computerkriminalität ratifiziert oder waren diesem beigetreten.

69 Aufgabenbeschreibung für die Erstellung eines Entwurfs eines zweiten Zusatzprotokolls zum Budapester Übereinkommen über Computerkriminalität, T-CY (2017)3.

70 Das Darknet besteht aus Inhalten in Overlay-Netzen, die zwar das Internet nutzen, auf die aber nur mit einer bestimmten Software, Konfigurierung oder Autorisierung zugegriffen werden kann. Das Darknet ist ein kleiner Teil des Deep Web, dem Teil des Internets, der nicht von Suchmaschinen indexiert ist.

71 Eine bemerkenswerte Ausnahme stellt hier die unlängst erfolgte Entfernung von zwei der größten kriminellen Dark Web Märkte, AlphaBay und Hansa, dar: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

72 Europol spielt in diesem Bereich bereits eine wichtige Rolle. Für ein Beispiel aus jüngerer Zeit siehe: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

dann im Internet gehandelt und können von Straftätern für Zahlungsbetrug genutzt werden[73]. Die Kommission schlägt gerade vor, die Abschreckung durch eine **Richtlinie zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit bargeldlosen Zahlungsmitteln**[74] zu erhöhen. Hierdurch sollen die bestehenden Vorschriften in diesem Bereich aktualisiert und die Fähigkeit der Strafverfolgungsbehörden, diese Form der Kriminalität in Angriff zu nehmen, gestärkt werden.
Auch die Ermittlungskompetenzen der Strafverfolgungsbehörden der Mitgliedstaaten im Bereich der Cyberkriminalität müssen verbessert werden; Gleiches gilt für das Verständnis der durch den Cyberraum ermöglichten Kriminalität und die Ermittlungsoptionen von Staatsanwälten und Richtern. Eurojust und Europol tragen in enger Zusammenarbeit mit spezialisierten Beratergruppen innerhalb des bei Europol angesiedelten Zentrums zur Bekämpfung der Cyberkriminalität und mit den Netzen aus Leitern der Referate für Computerkriminalität und den auf Cyberkriminalität spezialisierten Staatsanwälten zur Erreichung dieses Ziels und zu einer verbesserten Koordinierung bei. Die Kommission wird für die Bekämpfung der Cyberkriminalität 10,5 Mio. EUR bereitstellen, die hauptsächlich aus ihrem **Fonds für die innere Sicherheit: Polizei** kommen werden. Da auch Schulungen ein wichtiges Element sind, hat die Europäische Gruppe für Schulung und Ausbildung in Bezug auf Cyberkriminalität eine Reihe nützlicher Materialien erstellt. Diese sollten nun mit Unterstützung der Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (EPA) in großem Maßstab unter den an der Strafverfolgung beteiligten Berufsgruppen verbreitet werden.

3.3 Zusammenarbeit zwischen öffentlichen und privaten Stellen bei der Bekämpfung der Cyberkriminalität

Die Wirksamkeit der traditionellen Strafverfolgungsmethoden wird durch die digitale Welt, die größtenteils durch privat betriebene Infrastruktur und eine Vielzahl unterschiedlicher Akteure in verschiedenen Ländern gekennzeichnet ist, infrage gestellt. Die Zusammenarbeit mit dem privaten Sektor, auch mit der IT-Branche und der Zivilgesellschaft, ist für die öffentlichen Behörden bei der effektiven Bekämpfung der Cyberkriminalität daher von elementarer Bedeutung. Auch der Finanzsektor spielt in diesem Kontext eine wichtige Rolle und die Zusammenarbeit mit ihm sollte verstärkt werden. So sollte in Sachen Cyberkriminalität beispielsweise die Rolle der Zentralstellen für Verdachtsanzeigen[75] gestärkt werden.

[73] Betrugserlöse stellen für die organisierte Kriminalität eine wichtige Einkommensquelle und damit die Voraussetzung für andere Straftaten, wie Terrorismus, Drogenschmuggel und Menschenhandel dar.

[74] COM(2017) 489.

[75] Die nationalen Zentralstellen für Geldwäsche-Verdachtsanzeigen nehmen Meldungen verdächtiger Transaktionen sowie sonstige Informationen zu Geldwäsche, damit zusammenhängenden Vortaten und Terrorismusfinanzierung entgegen, analysieren diese und verbreiten die Ergebnisse ihrer Analyse.

Einige Mitgliedstaaten haben bereits wichtige Schritte unternommen. In den Niederlanden arbeiten Finanzinstitute und Strafverfolgungsbehörden Hand in Hand, um im Rahmen der Task Force „Internetkriminalität" Betrug im Internet und Cyberkriminalität zu bekämpfen. In Deutschland bildet das „German Competence Centre against Cyber Crime" eine operative Schaltstelle für ihre Mitglieder, über die diese in enger Zusammenarbeit mit dem Bundeskriminalamt Informationen austauschen und Maßnahmen zum Schutz gegen Cyberkriminalität erarbeiten. 16 Mitgliedstaaten[76] haben Exzellenzzentren für die Bekämpfung der Cyberkriminalität geschaffen, um die Zusammenarbeit zwischen Strafverfolgungsbehörden, Hochschulen und privaten Partnern bei Entwicklung und Austausch empfehlenswerter Praktiken und bei Schulungen und Kapazitätsaufbau zu erleichtern.
Die Kommission unterstützt die Bildung von öffentlich-privaten Partnerschaften und Mechanismen der Zusammenarbeit durch spezifische Projekte wie das „Online Fraud Cyber Centre and Experts Network"[77], das ein Modell und einen Standard für den Informationsaustausch umsetzt, um die Risiken von Internet-Straftaten und Internet-Betrugsfälle zu analysieren und einzudämmen.

Bei Fällen von Cyberkriminalität müssen Privatunternehmen Informationen über konkrete Sicherheitsvorfälle, zu denen auch personenbezogene Daten zählen, unter vollständiger Einhaltung der Datenschutzvorschriften an die Strafverfolgungsbehörden weitergeben können. Die Reform der EU-Datenschutzvorschriften, die im Mai 2018 wirksam wird, geht mit einer Reihe gemeinsamer Vorschriften einher, in denen festgelegt ist, unter welchen Bedingungen Strafverfolgungsbehörden und private Stellen zusammenarbeiten können. Die Europäische Kommission wird gemeinsam mit dem Europäischen Datenschutzausschuss und den maßgeblichen Akteuren die empfehlenswertesten Praktiken in diesem Bereich ermitteln und gegebenenfalls Leitlinien ausgeben.

3.4 Intensivierung der Maßnahmen auf politischer Ebene

In dem unlängst beschlossenen **Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten**[78] (dem Instrumentarium für die Cyberdiplomatie („Cyber Diplomacy Toolbox")) werden die der Gemeinsamen Außen- und Sicherheitspolitik zuzurechnenden – auch restriktiven – Maßnahmen dargelegt, die zur Verstärkung der Reaktion der EU auf Aktivitäten, die ihren politischen, sicherheitsbezogenen und wirtschaftlichen Interessen schaden, eingesetzt werden können. Dieser Rahmen stellt einen wichtigen Schritt beim Kapazitätsaufbau auf EU- und mitgliedstaatlicher Ebene dar, und wird es künftig ermöglichen, derartige Aktivitäten zu signalisieren und Gegenmaßnahmen einzuleiten. Er wird unsere Fähigkeit zur Zuordnung böswilliger Cyberaktivitäten erhöhen und soll dadurch das Verhalten potenzieller Aggressoren beeinflussen, gleichzeitig aber auch der Notwendigkeit einer verhältnismäßigen Reaktion Rechnung tragen. Die Zuordnung zu einem Staat oder einem anderen Urheber bleibt politische Entscheidung eines souveränen Staates und muss sich auf alle verfügbaren nachrichtendienstlichen Quellen stützen. Mit den Mitgliedstaaten wird derzeit an der Umsetzung dieses Rahmens gearbeitet und diese Arbeiten

[76] Belgien, Bulgarien, Deutschland, Estland, Frankreich, Griechenland, Irland, Litauen, Österreich, Polen, Rumänien, Slowenien, Spanien, Tschechische Republik, Vereinigtes Königreich und Zypern.

[77] Die EU-Initiative OF2CEN soll den systematischen EU-weiten Austausch von Informationen über Internetbetrug zwischen Banken und Starfverfolgungsstellen ermöglichen, um Auszahlungen an Betrüger und Geldkuriere zu verhindern und Ermittlungen gegen die Urheber sowie deren Verfolgung zu erleichtern. Sie wird von der EU (Fonds für die innere Sicherheit: Polizei) kofinanziert.

[78] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

sollten auch in enger Abstimmung mit dem Konzeptentwurf zur koordinierten Reaktion auf grenzüberschreitende Cybersicherheitsvorfälle und -krisen großen Ausmaßes[79] fortgesetzt werden. Die für den Einsatz von Maßnahmen dieses Rahmens notwendige Einschätzung der Lage sollte in enger Zusammenarbeit mit den Mitgliedstaaten und den EU-Organen von INTCEN[80] mit anderen Informationen zusammengeführt, analysiert und weitergegeben werden.

3.5 Abschreckung durch die Cyberabwehrkompetenzen der Mitgliedstaaten zwecks Erhöhung der Cybersicherheit

Die Mitgliedstaaten entwickeln bereits Kompetenzen im Bereich der Cyberabwehr. Da die Grenzen zwischen Cyberabwehr und Cybersicherheit verwischen, Cyberinstrumente und -technologien einen doppelten Verwendungszweck aufweisen und sich die Ansätze der Mitgliedstaaten stark unterscheiden, ist die EU gut aufgestellt, um zur Erschließung von Synergien zwischen den militärischen und den zivilen Bemühungen beizutragen[81].

Diejenigen Mitgliedstaaten, die über fortschrittlichere Kompetenzen im Bereich der Cybersicherheit verfügen und diese zusammenführen wollen, können in Betracht ziehen, die Cyberabwehr mit Unterstützung durch die Hohe Vertreterin, die Kommission und die Europäische Verteidigungsagentur in den Rahmen der „Ständigen Strukturierten Zusammenarbeit“ (SSZ) aufzunehmen. Dieses Ansinnen könnte durch die oben beschriebenen Bemühungen zur Förderung der Kompetenzen der Unternehmen in der EU sowie der strategischen Autonomie unterstützt werden. Die EU kann ferner die Interoperabilität fördern, indem sie unter anderem die Entwicklung von Kompetenzen, die Koordination von Aus- und Weiterbildung sowie Bemühungen zur Standardisierung im Bereich der Güter mit doppeltem Verwendungszweck unterstützt.

Außerdem sollte der gemeinsame Rahmen uneingeschränkt genutzt werden, um hybriden Bedrohungen zu begegnen, die oftmals Cyberangriffe einschließen. Dies sollte insbesondere über die EU-Analyseeinheit für hybride Bedrohungen und das kürzlich in Helsinki eingerichtete Europäische Zentrum für die Abwehr hybrider Bedrohungen erfolgen, deren Aufgabe darin besteht, den strategischen Dialog zu fördern sowie Forschung und Analysen durchzuführen.

Ferner wird die EU, gestützt auf den 2014 eingeführten EU-Rahmen für die Cyberabwehrstrategie[82], erneut auf eine stärkere Einbeziehung der Cybersicherheit und Cyberabwehr in die Gemeinsame Sicherheits- und Verteidigungspolitik (GSVP) hinwirken. Die Cyberabwehrfähigkeit bei konkreten GSVP-Missionen und -Operationen ist von entscheidender Bedeutung: Es müssen standardisierte Verfahren und technische Fähigkeiten entwickelt werden, die sowohl bei der Durchführung ziviler und militärischer Missionen und Operationen als auch für ihren jeweiligen Planungs- und Durchführungsstab sowie für IT-Anbieter des EAD von Nutzen sein können. Um die Zusammenarbeit der Mitgliedstaaten und die Koordination der Bemühungen der EU in diesem Bereich zu verbessern, werden die Europäische Verteidigungsagentur und der EAD, in Zusammenarbeit mit den Kommissionsdienststellen, die strategische Abstimmung zwischen den Entscheidungsträgern

---

79 C(2017) 6100.

80 JOIN(2016) 018 final.

81 Die EU betrachtet den Cyberraum als gesondertes Operationsgebiet – wie Land, Luft und See. Die Cyberabwehr umfasst auch den Schutz und die Abwehrfähigkeit von Weltraumeinrichtungen und damit verbundener Bodeninfrastruktur.

82 www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515

der Mitgliedstaaten im Bereich der Cyberabwehr vorantreiben. Zudem wird die EU im Rahmen ihrer Bemühungen für eine technologische und industrielle Basis der europäischen Verteidigung die Entwicklung europäischer Cybersicherheitslösungen unterstützen. Dies schließt auch die Förderung regionaler Exzellenzcluster für den Bereich der Cybersicherheit und Cyberabwehr ein.

Die Kommissionsdienststellen werden in enger Zusammenarbeit mit dem EAD, den Mitgliedstaaten und einschlägigen EU-Einrichtungen bis 2018 eine **Plattform zur Aus- und Weiterbildung im Bereich der Cyberabwehr** einrichten, um dem derzeitigen Kompetenzdefizit auf dem Gebiet der Cyberabwehr zu begegnen. Dies geschieht in Ergänzung der Arbeit der Europäischen Verteidigungsagentur in diesem Bereich und trägt dazu bei, die Kompetenzlücken bei der Cybersicherheit und Cyberabwehr zu schließen.

Hauptmaßnahmen

- Initiative der Kommission für den grenzübergreifenden Zugang zu elektronischen Beweismitteln (Anfang 2018);
- rasche Annahme der vorgeschlagenen Richtlinie zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln durch das Europäische Parlament und den Rat;
- Einführung von Anforderungen in Bezug auf IPv6 bei der EU-Beschaffung, -Forschung und -Projektfinanzierung; freiwillige Vereinbarungen zwischen den Mitgliedstaaten und Internetdienstanbietern zur Förderung der Einführung von IPv6;
- neuer/erweiterter Schwerpunkt bei Europol auf Cyberforensik und Überwachung des Darknets;
- Umsetzung des Rahmens für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten;
- Erhöhung der finanziellen Unterstützung für nationale und transnationale Projekte, die zur Verbesserung der Strafverfolgung im Cyberraum beitragen;
- Einrichtung einer Bildungsplattform für den Bereich der Cybersicherheit im Jahr 2018, um dem derzeitigen Kompetenzdefizit bei Cybersicherheit und Cyberabwehr zu begegnen.

4. DIE INTERNATIONALE ZUSAMMENARBEIT IN DER CYBERSICHERHEIT STÄRKEN

In der internationalen Politik der EU in Sachen Cybersicherheit, die sich von den Grundwerten und -rechten der Union, wie der Freiheit der Meinungsäußerung, dem Recht auf Privatsphäre, dem Schutz personenbezogener Daten und der Wahrung eines offenen, freien und sicheren Cyberraums, leiten lässt, nimmt sich die EU der stetig neuen Herausforderung an, einen globalen stabilen Cyberraum voranzubringen und dabei zu Europas strategischer Autonomie im Cyberraum beizutragen.

4.1 Cybersicherheit in den Außenbeziehungen

Alles spricht dafür, dass Cyberangriffe aus anderen Ländern überall auf der Welt als eine der größten Bedrohungen der nationalen Sicherheit angesehen werden.[83] Da diese Bedrohung ihrem Wesen nach global ist, können Cyberangriffe – von deren Abwehr die internationale

[83] *Spring 2017 Global Attitudes Survey*, Pew Research Centre.

Stabilität und Sicherheit immer mehr abhängt – nur verhindert und deren Urheber abgeschreckt werden, indem wir starke Bündnisse mit Drittländern aufbauen und pflegen. Die Union wird in ihrem bilateralen, regionalen und multilateralen Engagement und ihren Multi-Stakeholder-Kontakten der Einrichtung eines strategischen Rahmens zu Konfliktprävention und Stabilität im Cyberraum Priorität einräumen.

Die EU setzt sich entschlossen dafür ein, dass das Völkerrecht, und insbesondere die Charta der Vereinten Nationen, auch im Cyberraum gilt. Sie unterstützt ferner die von der VN-Gruppe von Regierungssachverständigen eingebrachten freiwilligen, nicht bindenden Rechtsnormen, Regeln und Grundsätze des verantwortungsvollen Staatshandelns[84], die das verbindliche Völkerrecht ergänzen sollen. Die EU fördert außerdem die Entwicklung und Umsetzung regionaler vertrauensbildender Maßnahmen, sowohl in der Organisation für Sicherheit und Zusammenarbeit in Europa als auch in anderen Regionen.

Auf bilateraler Ebene werden die Cyber-Dialoge[85] weiter ausgebaut und durch Anstrengungen ergänzt, die einer besseren Zusammenarbeit mit Drittländern zur Stärkung der Grundsätze der Sorgfaltspflicht und Staatsverantwortung im Cyberraum dienen sollen. Die EU wird Fragen der internationalen Sicherheit im Cyberraum in ihrem internationalen Engagement vorrangig behandeln und zugleich dafür sorgen, dass die Cybersicherheit nicht als Vorwand für Protektionismus und die Einschränkung von Grundrechten und -freiheiten wie der Freiheit der Meinungsäußerung und der Informationsfreiheit, missbraucht wird. Ein umfassendes Cybersicherheitskonzept kommt nicht ohne die Wahrung der Menschenrechte aus. Die EU wird deshalb wie bisher auf globaler Ebene an ihren Grundwerten festhalten und sich dabei auf die EU-Menschenrechtsleitlinien zum Thema Online-Freiheit[86] stützen. Für die EU ist hierbei die Beteiligung aller Interessenträger an der Internet-Governance von großer Bedeutung.

Die Kommission hat außerdem einen Vorschlag[87] zur Modernisierung des EU-Ausfuhrkontrollsystems, einschließlich der Einführung von Kontrollen von Ausfuhren kritischer Technologien für digitale Überwachung, vorgelegt, die für Menschenrechtsverletzungen oder die Bedrohung der eigenen Sicherheit der EU missbraucht werden könnten; sie wird ferner den Dialog mit Drittländern aufnehmen, um globale Konvergenz und verantwortliches Handeln auf diesem Gebiet zu fördern.

4.2 Kapazitätsaufbau in der Cybersicherheit

Globale Stabilität im Cyberraum hängt von der lokalen und nationalen Fähigkeit aller Länder ab, Cybervorfälle zu verhindern bzw. auf sie zu reagieren und Cyberdelikte aufzuklären und zu ahnden. Unterstützende Bemühungen, die Abwehrfähigkeit von Drittländern auf nationaler Ebene aufzubauen, werden das Cybersicherheitsniveau weltweit verbessern, was sich positiv auf die EU auswirken wird. Um der immer neuen Cyberbedrohungen Herr zu werden zu können, sind Anstrengungen in der Ausbildung, der Entwicklung von politischen und juristischen Konzepten sowie effizient funktionierende IT-Notfallteams und Cybercrime-Einheiten in allen Ländern der Welt erforderlich.

---

84 A/68/98 und A/70/174.

85 Im September 2017 führte die EU mit den USA, China, Japan, der Republik Korea und Indien Gespräche über das Thema Cybersicherheit.

86 *EU Human Rights Guidelines on Freedom of Expression Online and Offline* (EU-Menschenrechtsleitlinien für die Meinungsfreiheit online und offline).

87 COM(2016) 616.

Seit 2013 hat die EU eine führende Rolle beim internationalen Kapazitätsaufbau im Cyberbereich und verbindet diese Anstrengungen systematisch mit ihrer Entwicklungszusammenarbeit. Die EU wird weiterhin und im Einklang mit dem Digital4Development-Konzept[88] ein auf Rechtsnormen basierendes Modell für den Kapazitätsaufbau vorantreiben. Die Prioritäten beim Kapazitätsaufbau werden bei den Nachbarstaaten der Union und den Entwicklungsländern liegen, in denen sich sowohl die Internetanbindung wie auch die Bedrohungen rasch entwickeln. Die Anstrengungen der Union werden die Entwicklungsagenda der EU vor dem Hintergrund der Agenda 2030 für nachhaltige Entwicklung und die allgemeinen Bemühungen um den Kapazitätsaufbau ergänzen.

Damit die Union künftig ihre kollektive Sachkenntnis zur Unterstützung dieses Kapazitätsaufbaus besser mobilisieren kann, sollte ein entsprechend ausgelegtes EU-Netzwerk für den Kapazitätsaufbau im Cyberraum eingerichtet werden, an dem sich der EAD, die für Cyberangelegenheiten zuständigen Stellen der Mitgliedstaaten, EU-Agenturen, Kommissionsdienststellen, die Wissenschaft und die Zivilgesellschaft beteiligen. Es werden Leitlinien der EU für den Kapazitätsaufbau im Cyberraum aufgestellt werden, um eine bessere politische Orientierung zu bieten und die EU-Maßnahmen im Rahmen der Hilfe für Drittländer besser zu priorisieren.

Die Union wir auch mit anderen Gebern in diesem Bereich zusammenarbeiten, um Doppelarbeit zu vermeiden und einen gezielteren Kapazitätsaufbau in verschiedenen Regionen zu ermöglichen.

4.3 Zusammenarbeit zwischen der EU und der NATO

Auf der Grundlage der bereits erzielten beträchtlichen Fortschritte wird die Union, wie in der Gemeinsamen Erklärung vom 8. Juli 2016[89] vorgesehen, die Zusammenarbeit zwischen der EU und der NATO in den Bereichen Cybersicherheit, hybride Bedrohungen und Cyberabwehr vertiefen. Die Prioritäten umfassen u. a. die Förderung der Interoperabilität durch kohärente Anforderungen und Standards für die Cyberabwehr, die Intensivierung der Zusammenarbeit bei Ausbildung und Übungen und die Harmonisierung der Ausbildungsanforderungen.

Die EU und die NATO werden außerdem die Forschung zum Thema Cyberabwehr sowie die Innovationszusammenarbeit fördern, und sich auf die geltende technische Vereinbarung zwischen ihren Cybersicherheitseinrichtungen über den Informationsaustausch in Sachen Cybersicherheit[90] stützen. Die jüngsten gemeinsamen Anstrengungen zur Bekämpfung hybrider Bedrohungen, insbesondere die Zusammenarbeit zwischen der EU-Analyseeinheit für hybride Bedrohungen und der Schwestereinheit der NATO, sollten weiterverfolgt werden, um die Abwehr- und Reaktionsfähigkeit im Falle von Cyberkrisen zu verbessern. Eine weitergehende Zusammenarbeit zwischen der EU und der NATO wird im Rahmen von Cyberabwehrübungen unter Beteiligung des EAD, anderer EU-Einrichtungen sowie der entsprechenden NATO-Einrichtungen, u. a. des NATO Cooperative Cyber Defence Centre of Excellence in Tallin, gefördert. Die NATO und die EU werden zum ersten Mal parallele und koordinierte Übungen zur Reaktion auf ein hybrides Szenario abhalten, wobei die NATO 2017 und die EU im darauffolgenden Jahr die Leitung übernimmt. Der nächste Bericht über

[88] SWD(2017) 157 final.
[89] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[90] CERT-EU and NATO Computer Incident Response Capability (NCIRC).

die Zusammenarbeit zwischen der EU und der NATO, der den beiden Räten im Dezember 2017 vorzulegen ist, wird Gelegenheit bieten, die Möglichkeiten einer noch engeren Zusammenarbeit auszuloten, insbesondere durch Gewährleistung gemeinsamer, sicherer und robuster Mittel für die Kommunikation zwischen allen mitwirkenden Organen und Einrichtungen, einschließlich der ENISA.

Hauptmaßnahmen

- Weiterentwicklung des strategischen Rahmens für Konfliktprävention und Stabilität im Cyberraum
- Aufbau eines neuen Netzwerks für den Kapazitätsaufbau, um Drittländer in ihrer Fähigkeit, Cyberbedrohungen entgegenzutreten, zu unterstützen, und Ausarbeitung von EU-Leitlinien für den Kapazitätsaufbau im Bereich Cybersicherheit, um die EU-Maßnahmen besser priorisieren zu können
- Ausweitung der Zusammenarbeit zwischen der EU und der NATO, u. a. Beteiligung an parallelen und koordinierten Übungen und bessere Interoperabilität bei den Cybersicherheitsstandards

5. FAZIT

Vorsorgende Maßnahmen der EU in der Cybersicherheit sind sowohl für den digitalen Binnenmarkt als auch für unsere Sicherheits- und Verteidigungsunion von zentraler Bedeutung. Die europäische Cybersicherheit zu verbessern und die Bedrohung ziviler und militärischer Ziele abzuwenden, ist ein Muss.

Der vom estnischen Ratsvorsitz organisierte Digital-Gipfel am 29. September 2017 bietet Gelegenheit, die gemeinsame Entschlossenheit zu bekräftigen, die Cybersicherheit in den Mittelpunkt der EU als digitaler Gesellschaft zu stellen. Als Teil dieser gemeinsamen Verpflichtung fordert die Kommission die Mitgliedstaaten auf, verbindlich darzulegen, wie sie in Bereichen vorgehen wollen, in denen die Zuständigkeit in erster Linie bei ihnen liegt. Dies sollte die Erhöhung der Cybersicherheit durch folgende Maßnahmen umfassen:

- Gewährleistung einer vollständigen und wirksamen Umsetzung der NIS-Richtlinie bis zum 9. Mai 2018 und Zusicherung der Ressourcen, die die für Cybersicherheit zuständigen Behörden benötigen, um ihre Aufgaben wirksam erfüllen zu können;
- Anwendung der gleichen Regeln auf öffentliche Verwaltungen, ganz entsprechend ihrer sozialen und wirtschaftlichen Rolle insgesamt;
- Schaffung von Ausbildungsmöglichkeiten im Bereich Cybersicherheit in der öffentlichen Verwaltung;
- Vorrangige Einbeziehung der Thematik Cyberbedrohungen in Informationskampagnen und Aufnahme des Themas Cybersicherheit in die Lehrpläne von Hochschulen und Berufsausbildungseinrichtungen;
- Nutzung der Initiativen im Rahmen der ständigen strukturierten Zusammenarbeit (PESCO) und des Europäischen Verteidigungsfonds, um die Entwicklung von Cyberabwehrprojekten voranzubringen.

In dieser gemeinsamen Mitteilung haben wir die Tragweite der Bedrohung wie auch die Bandbreite der Maßnahmen aufgezeigt, die die Union ergreifen kann. Wir brauchen ein abwehrfähiges Europa, das seine Menschen wirksam schützen kann, indem es möglichen

Cybersicherheitsvorfällen zuvorkommt, zuverlässige Schutzmechanismen in seine Struktur und sein Handeln integriert, sich schnell von Cyberangriffen erholt und deren Urheber abschreckt. In dieser Mitteilung werden gezielte Maßnahmen vorgestellt, die die Cybersicherheitsstrukturen und -kapazitäten der EU weiter in koordinierter Weise mit der uneingeschränkten Mitarbeit der Mitgliedstaaten und beteiligten EU-Strukturen und unter Wahrung ihrer Zuständigkeiten und Verpflichtungen festigen werden. Die Durchführung wird deutlich zeigen, dass die Union und ihre Mitgliedstaaten zusammenstehen werden, um einen Cybersicherheitsstandard zu schaffen, der den ständig wachsenden Herausforderungen, vor denen Europa steht, gerecht wird.