Europäische Kommission

LAGE DER UNION 2018

Die Cybersicherheit in Europa wirksam erhöhen

#SOTEU

12. September 2018

„Cyberangriffe kennen keine Grenzen, aber bei unserer Reaktionsfähigkeit gibt es von Land zu Land große Unterschiede. Dadurch entstehen Schlupflöcher, und Verwundbarkeiten ziehen immer neue Angriffe an. Die EU braucht solidere und wirksamere Strukturen, um eine stärkere Abwehrfähigkeit gegen Cyberangriffe zu gewährleisten und auf Cyberangriffe zu reagieren. Wir wollen bei dieser weltweiten Bedrohung nicht zu den schwächsten Gliedern gehören.“

Jean-Claude Juncker, Digital-Gipfel in Tallinn, 29. September 2017

Die Europäische Kommission und die Hohe Vertreterin schlugen 2017 ein breit angelegtes Maßnahmenpaket zur wirksamen Erhöhung der Cybersicherheit in der EU vor. Damit sollen in Europa die richtigen Instrumente zur Verfügung stehen, um die sich ständig verändernde Bedrohung durch Cyberkriminalität zu bewältigen. Jetzt werden diese Anstrengungen durch einen Vorschlag ergänzt, der dazu beiträgt, Ressourcen und Fachwissen in Forschung und Innovation zu bündeln, und der die EU dabei unterstützt, eine Führungsrolle in der Cybersicherheit der nächsten Generation und bei digitalen Technologien zu übernehmen.

Aktuelle Bedrohungen durch Cyberkriminalität

> 4000 Ransomware-Angriffe pro Tag im Jahr 2016

In 80 % der europäischen Unternehmen kam es im vergangenen Jahr zu mindestens einem Cybersicherheitsvorfall

In der gesamten Wirtschaft nahm die Zahl der Sicherheitsvorfälle um 38 % zu – das ist der stärkste Zuwachs in den letzten zwölf Jahren

In einigen Mitgliedstaaten fallen **50 % aller Straftaten** in den Bereich Cyberkriminalität

> 150 Länder und > 230 000 Systeme waren beim Angriff mit der Schadsoftware Wannycry im Mai 2017 sektor- und länderübergreifend betroffen – mit beträchtlichen Auswirkungen auf wesentliche, mit dem Internet verbundene Dienste, darunter Krankenhäuser und Ambulanzdienste

Die Abwehrfähigkeit gegenüber Cyberangriffen stärken

Die Kommission unterstützt bereits jetzt die Verbesserung der Abschreckung, Abwehrfähigkeit und Reaktion der EU bei Cyberangriffen, unter anderem durch Folgendes:

Unterstützung der wirksamen Umsetzung der ersten EU-Rechtsvorschrift im Bereich Cybersicherheit (Richtlinie zur Netz- und Informationssicherheit):

AUSBAU DER KAPAZITÄTEN

Die Mitgliedstaaten müssen ihre Cybersicherheitskapazitäten ausbauen

ZUSAMMENARBEIT

Verstärkte Zusammenarbeit auf EU-Ebene

RISIKOVERHÜTUNG

Akteure in zentralen Sektoren (z. B. Energie, Verkehr, Gesundheitswesen) müssen Maßnahmen für die Risikoverhütung und den Umgang mit Cybervorfällen ergreifen

Zusammenarbeit mit den Mitgliedstaaten:

EU-AGENTUR FÜR CYBERSICHERHEIT

Stärkung der Agentur der Europäischen Union für Cybersicherheit, um die Mitgliedstaaten besser zu unterstützen

EU-ZERTIFIZIERUNGSRAHMEN

ein unionsweiter Zertifizierungsrahmen, mit dem die Cybersicherheit von Produkten und Dienstleistungen gewährleistet werden soll

KOORDINIERTE REAKTION

Sicherstellung einer schnellen und koordinierten Reaktion auf großangelegte Cyberangriffe

Die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) unterstützt die einschlägigen Behörden der Mitgliedstaaten bei einer besseren Sicherung der EU gegen Cyberangriffes.

Bündelung von Ressourcen und Fachkenntnissen in der Cybersicherheits-technologie

Über die bereits bestehenden EU-Initiativen zur Cybersicherheit hinaus schlägt die Kommission heute vor, diese Bemühungen zu ergänzen und ein Netz von Kompetenzzentren sowie ein Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung zu schaffen. Dadurch sollen die Entwicklung und Einführung der Instrumente und Technologien unterstützt werden, die erforderlich sind, um einer sich ständig wandelnden Bedrohung begegnen zu können.

Aufgabe dieses europäischen Zentrums wird es sein, zusammen mit den Mitgliedstaaten die für Cybersicherheit im nächsten langfristigen EU-Haushalt vorgesehenen Mittel möglichst gezielt zu koordinieren. Dies wird zum Aufbau neuer europäischer Kapazitäten im Cyberbereich beitragen.

Avec plus de **660 centres de compétences en matière de cybersécurité** répartis dans l'ensemble de l'UE, celle-ci dispose déjà d'une expertise considérable en la matière. Afin d'exploiter et d'utiliser efficacement cette expertise, la Commission propose de créer un mécanisme pour:

vorhandenes Fachwissen bündeln, teilen und den Zugang gewährleisten

Unterstützung bei der Einführung von EU-Cybersicherheitsprodukten und -lösungen

Sicherstellung einer langfristigen strategischen Zusammenarbeit zwischen Wirtschaft, Forschungsgemeinschaften und Regierungen

Koinvestitionen und gemeinsame Nutzung kostenintensiver Infrastruktur

Europäisches Kompetenzzentrum:

es wird die Verwendung der für Cybersicherheit bestimmten Mittel des nächsten langfristigen EU-Haushalts für die Jahre 2021-2027 aus den Programmen „Digitales Europa“ und „Horizont Europa“ koordinieren. Das Zentrum wird das Netz nationaler Koordinierungszentren und die Kompetenzgemeinschaft unterstützen und Forschung und Innovation im Bereich **Cybersicherheit** vorantreiben. Ferner wird es **gemeinsame Investitionen** der EU, der Mitgliedstaaten und der Industrie organisieren. Beispielsweise werden im Rahmen des Programms „Digitales Europa“ **2 Mrd. EUR** investiert, um die Sicherheit der digitalen Wirtschaft, der Gesellschaft und der Demokratien in der EU zu gewährleisten. Dies umfasst die Stärkung der Cybersicherheitsbranche der EU und die Finanzierung von modernster Cybersicherheitsausrüstung und infrastruktur.

Netz nationaler Koordinierungszentren:

Jeder Mitgliedstaat wird ein nationales Koordinierungszentrum benennen, das an der Spitze des Netzes steht und sich für die Entwicklung neuer Cybersicherheitskapazitäten und weiteren Kompetenzausbau einsetzen wird. Das Netz wird zur Ermittlung und Unterstützung der relevantesten Cybersicherheitsprojekte in den Mitgliedstaaten beitragen.

Kompetenzgemeinschaft:

eine große, offene und vielseitige Gruppe von Interessenträgern im Bereich Cybersicherheit aus der Wissenschaft sowie dem privaten und dem öffentlichen Sektor, einschließlich Zivil- und Militärbehörden.

Was wird sich verbessern?

- bessere Koordinierung der Arbeit;
- Zugang zu Fachwissen;
- Zugang zu Erprobungs- und Versuchseinrichtungen;
- Bewertung der Cybersicherheit von Produkten;
- Zugang zu innovativen Cybersicherheitsprodukten und lösungen;
- Unterstützung der Marktentwicklung von Produkten und Dienstleistungen;
- verbesserte Sichtbarkeit bei potenziellen Investoren und Geschäftspartnern;
- Kosteneinsparungen durch Koinvestitionen mit anderen Mitgliedstaaten;
- Fähigkeit der EU zur autonomen Sicherung ihrer Wirtschaft und Demokratie;
- EU übernimmt eine weltweite Führungsrolle bei der Cybersicherheit.

Wer sind die Nutznießer?