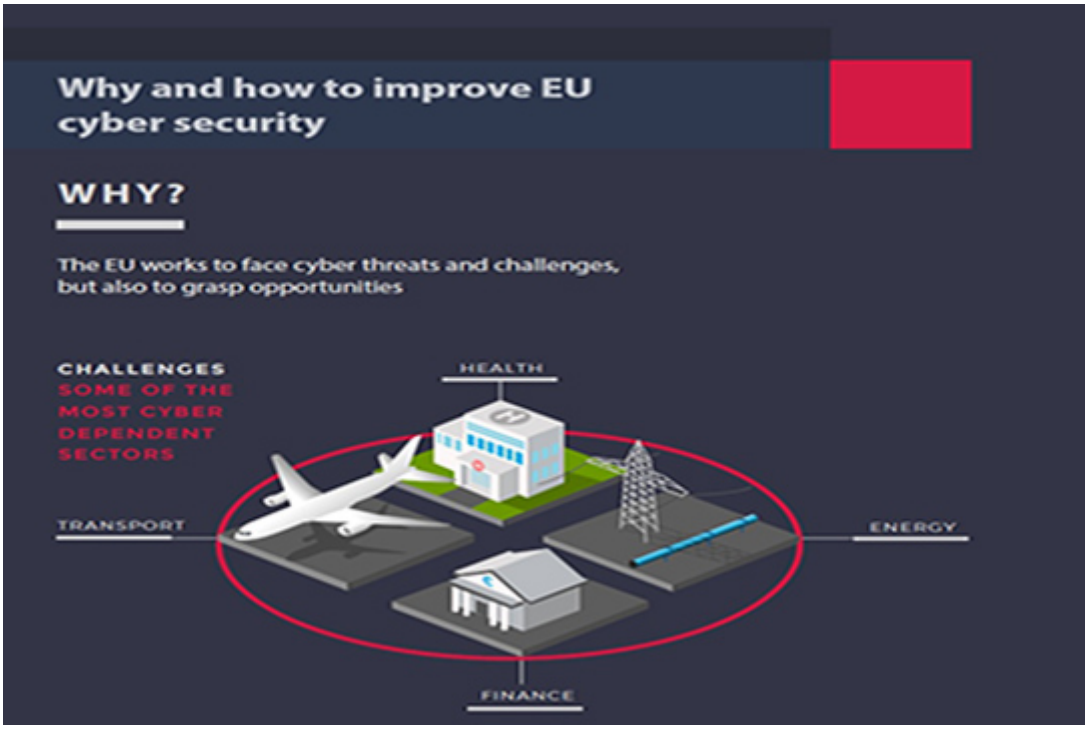
Europäischer Rat
Rat der Europäischen Union

Reform der Cybersicherheit in Europa

Infografik – EU-Cybersicherheit



Vollständige Infografik

Die Europäische Union will ihre Vorschriften zur Cybersicherheit stärken, um der wachsenden Bedrohung durch Cyberangriffe zu begegnen und die Chancen des neuen digitalen Zeitalters zu nutzen.

Auf seiner Tagung vom 19./20. Oktober 2017 hat der Europäische Rat nach dem Vorschlag eines **Reformpakets** der Europäischen Kommission im September zur Annahme eines **gemeinsamen Konzepts für die Cybersicherheit in der EU** aufgerufen.

Diese Reform stützt sich auf die Maßnahmen, die im Rahmen der EU-Strategie für die Cybersicherheit eingeleitet wurden, insbesondere deren Hauptpfeiler, die Richtlinie zur Netz- und Informationssicherheit – der **NIS-Richtlinie**.

Zu den neuen Initiativen, die in dem Vorschlag vorgesehen sind, gehören:

- die Einrichtung einer **schlagkräftigeren EU-Agentur für Cyber-Sicherheit**
- die Einführung eines **EU-weiten Zertifizierungssystems für Cybersicherheit**
- die rasche Umsetzung der NIS-Richtlinie.

Die Staats- und Regierungschefs der EU sehen die Reform im Bereich der Cybersicherheit als einen der wichtigsten aktuellen Punkte auf dem Weg zur Vollendung des **digitalen Binnenmarkts** der EU.

› Schlussfolgerungen des Europäischen Rates, 19./20.10.2017

› Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in Europa wirksam erhöhen (Europäische Kommission)

› Der digitale Binnenmarkt für Europa

Warum ist dies nötig?

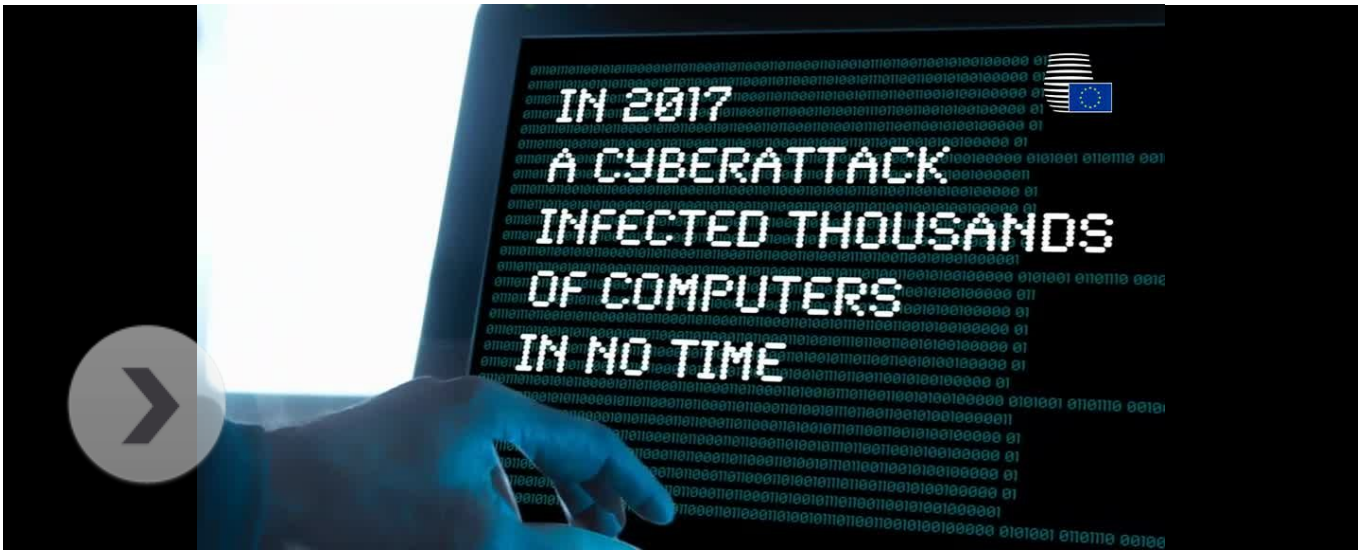
Angesichts stetig wachsender Herausforderungen im Bereich der Cybersicherheit muss die EU dafür sorgen, dass Cyber-Angriffe gegen Mitgliedstaaten oder EU-Institutionen stärker wahrgenommen und entschlossener bekämpft werden.

Das "Internet der Dinge" ist schon heute Realität; **bis 2020 wird mit Dutzenden Milliarden vernetzter digitaler Geräte in der EU gerechnet.**

Dabei können die heutigen IT-Systeme durch Sicherheitsvorfälle wie technische Störungen und Viren ernsthaft beeinträchtigt werden. Derartige sicherheitsrelevante IT-Vorfälle (NIS-Vorfälle) treten immer häufiger auf und sind immer schwerer in den Griff zu bekommen.

Darüber hinaus **betragen die Kosten von Cyberangriffen für die Weltwirtschaft geschätzt jährlich rund 400 Mrd. €**.

› Informationsblatt zur Cybersicherheit (Europäische Kommission)



Die EU fordert vertrauenswürdige Netze zum Schutz gegen Cyberkriminalität

Cybersicherheit: Chancen und Gefahren

- Die Zahl der Sicherheitsvorfälle in der gesamten Wirtschaft **ist 2015 um 38 % gestiegen**.
- 80 % aller europäischen Unternehmen haben 2015 **mindestens einen Cybersicherheitsvorfall** erlebt.
- 86 % aller Europäerinnen und Europäer betrachten **Cyberkriminalität als wachsende Bedrohung**.

Quelle: Europäische Kommission

EU-weit hängen viele Unternehmen und staatliche Einrichtungen bei der Erbringung ihrer Kernaufgaben von digitalen Netzen und Infrastrukturen ab. Dies bedeutet, dass **NIS-Vorfälle** durch Beeinträchtigung von Dienstangeboten und Unterbrechung von Geschäftsvorgängen massive Auswirkungen haben können.

Außerdem kann ein NIS-Vorfall in einem Land Auswirkungen in anderen Ländern oder sogar in der ganzen EU haben. Sicherheitsvorfälle können auch das **Vertrauen der Verbraucher** in Online-Zahlungssysteme und IKT-Netze **untergraben**.

Trotz der wachsenden Bedrohung fehlen beim Thema Cybersicherheit nach wie vor Wissen und Bewusstsein:

- **51 % der europäischen Bürgerinnen und Bürger fühlen sich** in Bezug auf Cyber-Bedrohungen **nicht ausreichend informiert**
- **69 % der Unternehmen fehlt ein grundlegendes Verständnis** ihrer Verwundbarkeit durch Cyber-Bedrohungen.

Im Rat

Die EU-Institutionen haben am 20. Dezember 2017 einen wichtigen Schritt zur Verstärkung ihrer **Zusammenarbeit bei der Abwehr von Cyberangriffen** getan.

Mit einer interinstitutionellen Vereinbarung wurde ein ständiges **IT-Notfallteam** für alle Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) eingerichtet.

CERT-EU wird eine koordinierte Reaktion der EU auf Cyberangriffe gegen ihre Institutionen sicherstellen. Hierzu wird das Notfallteam eng mit den IT-Sicherheitsteams der EU-Institutionen und Mitgliedstaaten zusammenarbeiten. Es wird auch mit den entsprechenden Stellen der NATO zusammenarbeiten.

Der Rat "Allgemeine Angelegenheiten" hat auf seiner Tagung am 20. November 2017 zu einer **Verbesserung der Cybersicherheit in Europa** und zu einer **Stärkung der Abwehrfähigkeit gegen Cyberangriffe** in der gesamten EU aufgerufen. Diese Ziele stehen im Einklang mit den Prioritäten, die der Europäische Rat im Oktober 2017 festgelegt hat.

Die Ministerinnen und Minister betonten, dass alle Länder der EU die erforderlichen Ressourcen und Investitionen bereitstellen müssen, um die Cybersicherheit zu verbessern. Sie hoben auch die wichtige Verbindung zwischen dem **Vertrauen in das digitale Europa** und der Abwehrfähigkeit gegen Cyberangriffe in der EU hervor.

Der Rat "Telekommunikation" einigte sich am 24. Oktober 2017 darauf, einen **Aktionsplan** für die Reform der Cybersicherheit in der EU auszuarbeiten. Er hob hervor, dass die Online-Sicherheit von wesentlicher Bedeutung für die europäische Bevölkerung und für europäische Unternehmen ist.

› EU-Institutionen verstärken Zusammenarbeit gegen Cyberangriffe (Pressemitteilung, 20.12.2017)
› EU plant Stärkung der Cybersicherheit (Pressemitteilung, 20.11.2017)
› Rat "Telekommunikation", 24.10.2017

Im Einzelnen

Zertifizierungssystem für Cybersicherheit

In ihrem Reformpaket vom September 2017 schlägt die Europäische Kommission die Einführung EU-weiter Zertifizierungssysteme für IKT-Produkte, -Dienstleistungen und -Prozesse vor. Diese Initiative soll das Wachstum des Marktes für Cybersicherheit in der EU ermöglichen.

Die Zertifizierungssysteme sollen als Vorschriften, technische Anforderungen und Verfahren Gestalt annehmen. Ziel ist es, die Marktfragmentierung zu verringern, regulatorische Hindernisse auszuräumen und Vertrauen zu schaffen. Sie sollen in allen Mitgliedstaaten anerkannt werden und Unternehmen damit den grenzüberschreitenden Handel erleichtern.

› EU-Rahmen für die Zertifizierung der Cybersicherheit (Europäische Kommission)

Von Kompetenzförderung bis Betrugsbekämpfung

Weitere Initiativen im Vorschlag der Kommission zur Stärkung der Cybersicherheit in der EU sind:

- ein Konzept für den Umgang mit Großangriffen im Cyberraum
- ein europäisches Kompetenzzentrum für Cybersicherheitsforschung, verbunden mit einem Netz nationaler Zentren
- eine wirksamere strafrechtliche Verfolgung von Cyberkriminalität durch eine neue Richtlinie zur Bekämpfung von Betrug und Fälschung im bargeldlosen Zahlungsverkehr
- die Stärkung der globalen Stabilität durch internationale Zusammenarbeit.

› Koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (Europäische Kommission)

Eine stärkere EU-Agentur für Cybersicherheit

Nach einem weiteren Vorschlag der Kommission soll die bestehende Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) zu einer schlagkräftigeren EU-Agentur für Cybersicherheit ausgebaut werden. Ihre Aufgabe soll es sein, Mitgliedstaaten, EU-Institutionen und Unternehmen zu helfen, sich gegen Cyberangriffe zu wehren.

› Die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA)

NIS-Richtlinie auf der Liste der Prioritäten

Die Mitgliedstaaten haben bis Mai 2018 Zeit, die Cybersicherheitsstrategie in nationales Recht umzusetzen, und bis Dezember 2018, die Betreiber wesentlicher Dienste zu ermitteln.

Im Mai 2016 hatte der Rat EU-weit geltende Regeln für die Cybersicherheit verabschiedet. Sie traten im August 2016 in Kraft.

Die **Richtlinie über Netz- und Informationssicherheit (NIS-Richtlinie)** wurde erlassen, um die Zusammenarbeit zwischen den Mitgliedstaaten in der zentralen Frage der Cybersicherheit zu verstärken. Sie enthält Sicherheitspflichten für Betreiber wesentlicher Dienste (in kritischen Sektoren wie Energie, Verkehr, Gesundheit und Finanzen) und Anbieter digitaler Dienste (Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste).

Zudem verpflichtet die NIS-Richtlinie jedes EU-Land, eine oder mehrere nationale Behörden zu benennen und eine Strategie zur Bewältigung von Bedrohungen durch Cyberkriminalität festzulegen.

› NIS-Richtlinie (Amtsblatt der EU)
› Rat nimmt Vorschriften über Cybersicherheit an (Pressemitteilung, 17.5.2016)

Sicherheit im digitalen Binnenmarkt

Cybersicherheit kann Innovationen erleichtern und dazu beitragen, **Daten als "das neue Öl der Wirtschaft"** in den Mittelpunkt zu rücken. Europas digitale Zukunft zu sichern kann auch bedeuten,

- Gefahren für Online-Plattformen zu bekämpfen und sie in die Lage zu versetzen, einen positiven Beitrag zur Gesellschaft zu leisten,
- die Wettbewerbsfähigkeit kleiner und mittlerer Unternehmen in der digitalen Wirtschaft zu unterstützen,
- in die Nutzung künstlicher Intelligenz und den Einsatz von Supercomputern in Bereichen wie Medizin und Energieeffizienz zu investieren.

› Halbzeitüberprüfung der Strategie für einen digitalen Binnenmarkt (Europäische Kommission, Pressemitteilung)

Verwandte Webseiten

› Agenda der EU-Führungsspitzen
› Brexit

- Verlegung der derzeit im Vereinigten Königreich ansässigen EU-Agenturen
- Der digitale Binnenmarkt für Europa
- EU-Haushaltsplan 2018
- EU-Handelspolitik
- Suche nach Lösungen für Migrationsdruck
- EU-Terrorismusbekämpfung
- Sanktionen: Wann und wie die EU restriktive Maßnahmen verhängt
- Zusammenarbeit der EU im Bereich der Sicherheit und Verteidigung
- Östliche Partnerschaft
- Bekämpfung des Klimawandels in der EU
- Der Kampf der EU gegen die organisierte Kriminalität
- Humanitäre Hilfe
- EU-Krisenreaktion (IPCR)