Artikel
13-02-2023 - 16:58
20221103STO48002

Europäisches Parlament

Neue Gesetze im Kampf gegen Cyberkriminalität

Das Parlament hat Maßnahmen für ein sichereres Online-Umfeld beschlossen.
https://multimedia.europarl.europa.eu/x_N01_AFPS_221109_CYBS_ev?p_p_state=pop_up&lang=de&autoplay=off

Das Parlament hat neue Gesetze zur Stärkung der Cybersicherheit in Schlüsselbereichen verabschiedet. Erfahren Sie, wie die neue Gesetzgebung zum Schutz der EU-Bürger beitragen wird.

Mit der rasant zunehmenden Digitalisierung des täglichen Lebens, die durch die COVID-19-Pandemie noch beschleunigt wurde, ist der Schutz vor Cyber-Bedrohungen für ein reibungsloses Funktionieren der Gesellschaft unerlässlich geworden.

Cyberangriffe können sehr kostspielig sein. Nach Angaben der Europäischen Kommission werden die jährlichen Kosten der Cyberkriminalität für die Weltwirtschaft bis Ende 2020 auf 5,5 Billionen Euro geschätzt.

Im November 2022 aktualisierte das Europäische Parlament das EU-Recht, um Investitionen in eine starke Cybersicherheit für wichtige Dienste und kritische Infrastrukturen zu fördern und die EU-weiten Vorschriften zu stärken. Das Parlament verstärkte am 22. November 2022 auch den Schutz der kritischen Infrastrukturen der EU, einschließlich der digitalen Infrastrukturen, indem es die Rechtsvorschriften zur Verschärfung der Risikobewertungen und der Meldepflichten für kritische Akteure in elf wichtigen Bereichen endgültig verabschiedete.

Erfahren Sie mehr darüber, wie die EU den digitalen Wandel gestaltet.

Verschärfung der Cybersicherheitsverpflichtungen -

die NIS2-Richtlinie

Mit der Richtlinie zur Netz- und Informationssicherheit (NIS2) werden neue Regeln eingeführt, um ein hohes gemeinsames Niveau der Cybersicherheit in der EU zu fördern – sowohl für Unternehmen als auch für Länder. Durch die Richtlinie werden auch die Cybersicherheitsanforderungen für mittlere und große Unternehmen, die in Schlüsselsektoren tätig sind und Dienstleistungen anbieten, verschärft.

Die Aktualisierung der NIS-Richtlinie aus dem Jahr 2016 zielt darauf ab, die Klarheit und Umsetzung zu verbessern und die rasanten Entwicklungen in diesem Bereich zu berücksichtigen. Sie deckt mehr Sektoren und Tätigkeiten als zuvor ab, strafft die Berichtspflichten und geht auf die Sicherheit der Lieferkette ein.

Nach der Verabschiedung durch das Parlament und die Mitgliedstaaten im Rat im November 2022 haben die EU-Länder 21 Monate Zeit, um die Richtlinie umzusetzen.

Erfahren Sie mehr über die wichtigsten neuen Cyber-Bedrohungen.

Mehr Sektoren einbezogen

Mit dem neuen Gesetz wird der Geltungsbereich auf Sektoren und Aktivitäten ausgeweitet, die für Wirtschaft und Gesellschaft von entscheidender Bedeutung sind, darunter Energie, Verkehr,

Banken, Gesundheit, digitale Infrastruktur, öffentliche Verwaltung und Raumfahrt. Es erstreckt sich jedoch nicht auf die nationale und öffentliche Sicherheit, die Strafverfolgung und das Justizwesen. Das Gesetz gilt für die öffentliche Verwaltung auf zentraler und regionaler Ebene, nicht aber für Parlamente und Zentralbanken.

Unter der neuen Gesetzgebung sind mehr Einrichtungen und Sektoren dazu verpflichtet, Maßnahmen zum Management von Cybersicherheitsrisiken zu ergreifen, darunter Anbieter von öffentlichen elektronischen Kommunikationsdiensten, Betreiber sozialer Medien, Hersteller kritischer Produkte (einschließlich medizinischer Geräte) sowie Post- und Kurierdienste.

Strengere Verpflichtungen für Länder

Das Gesetz legt strengere Cybersicherheitsverpflichtungen für EU-Mitgliedstaaten fest, wenn es um Überwachung geht. Auch wird die Durchsetzung dieser Verpflichtungen verbessert, unter anderem durch die Harmonisierung von Sanktionen in den Mitgliedstaaten. Außerdem soll die Zusammenarbeit zwischen den EU-Ländern unter dem Dach der Agentur der Europäischen Union für Cybersicherheit (ENISA) verbessert werden, auch bei groß angelegten Vorfällen.

Schutz des Finanzsystems der EU – DORA

Da der Finanzsektor immer stärker von Software und digitalen Prozessen abhängig ist, muss er auch stärker geschützt werden. Die Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA) wird dafür sorgen, dass der EU-Finanzsektor widerstandsfähiger gegen schwerwiegende Betriebsstörungen und Cyberangriffe ist. Das Parlament hat die Gesetzgebung, die zuvor mit dem Rat vereinbart wurde, am 10. November 2022 endgültig verabschiedet.

Durch das Gesetz werden Anforderungen an die digitale Widerstandsfähigkeit des Finanzdienstleistungssektors in der EU eingeführt und harmonisiert. Die Unternehmen müssen sicherstellen, dass sie allen Arten von Störungen und Bedrohungen im Zusammenhang mit der Informations- und Kommunikationstechnologie (IKT) standhalten, darauf reagieren und sich davon erholen können.

Die neuen Vorschriften gelten für alle Unternehmen, die Finanzdienstleistungen erbringen, wie Banken, Zahlungsdienstleister, E-Geld-Anbieter, Wertpapierfirmen, Anbieter von Krypto-Vermögenswerten sowie für kritische IKT-Drittanbieter.

Die nationalen Behörden werden die Umsetzung überwachen und durchsetzen.

Erfahren Sie, was die EU unternimmt, um den digitalen Wandel zu gestalten:

- KI-Regeln: Wofür das Europäische Parlament eintritt
- Europäische Datenstrategie – was das Parlament fordert
- Das Gesetz über digitale Märkte und das Gesetz über digitale Dienste – einfach erklärt

- Die Gefahren von Kryptowährungen und der Nutzen der EU-Gesetzgebung
- Europäisches Chip-Gesetz – Wie die EU die Halbleiterknappheit überwinden will

Weitere Informationen

Ein hohes gemeinsames Cybersicherheitsniveau – NIS2
Pressemitteilung: Kommission begrüßt politische Einigung über neue Vorschriften für die Cybersicherheit von Netz- und Informationssystemen (13.05.2022)
Legislativfahrplan: Überprüfung der Richtlinie über die Sicherheit von Netz- und Informationssystemen (auf Englisch)
Verordnung über digitale Betriebsstabilität (DORA)
Legislativfahrplan: Digitale operationelle Widerstandsfähigkeit für den Finanzsektor (auf Englisch)
Europäische Kommission: Digitales Finanzwesen