Kurzinformation

Kurzinformation

Ziele

- Optimierte Rahmenbedingungen für ein hohes Cybersicherheitsniveau in Österreich
- Synergieeffekte innerhalb der zivilen staatlichen Cybersicherheits-Strukturen in Österreich
- Schutz und Prävention gegenüber Angriffen auf Netz- und Informationssysteme in Österreich

Inhalt

- Errichtung eines nationalen Cybersicherheitszentrums (NCSZ) zur Bündelung der Kompetenzen
- Umsetzung und Durchführung von Unionsrechtsakten im Bereich der Cybersicherheit
- Weiterentwicklung und Koordination einer neuen nationalen Cybersicherheitsstrategie
- Benennung einer zentralen Anlaufstelle für Cybersicherheit (SPOC)
- Benennung einer nationalen Behörde für das Management von Cybersicherheitsvorfällen großen Ausmaßes
- Benennung von Computer-Notfallteams (CSIRTs) zur Unterstützung der wesentlichen und wichtigen Einrichtungen
- Vorschriften zum Austausch von Cybersicherheitsinformationen
- Pflicht zur Setzung geeigneter Aufsichts- und Durchsetzungsmaßnahmen
- Pflicht zur Setzung geeigneter Risikomanagementmaßnahmen und Berichtspflichten
- Pflicht zur Führung eines Registers der wesentlichen und wichtigen Einrichtungen

---

Hauptgesichtspunkte des Entwurfs

Mit diesem Bundesgesetz sollen das Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) erlassen und das Telekommunikationsgesetz 2021 geändert werden.

Die zunehmende Durchdringung nahezu aller Bereiche der Gesellschaft und des täglichen Lebens mit digitaler Technologie bietet erhebliche Chancen und Möglichkeiten. Gleichzeitig wird die Gesellschaft dadurch aber auch angreifbarer und abhängiger von der Vertraulichkeit, Verfügbarkeit und Integrität digital verarbeiteter und gespeicherter Informationen. Staaten, Gruppierungen und kriminellen Akteuren eröffnen sich neue Wege, die digitale Vernetzung für Spionage, Sabotage oder andere kriminelle Aktivitäten nutzbar zu machen. Dabei können schon die Fähigkeiten einzelner krimineller Individuen genügen, um Cyberangriffe mit nicht abschätzbaren Folgen für die Sicherheit Österreichs durchzuführen. Immer mehr österreichische Unternehmen wurden in den vergangenen Jahren Opfer von Cyberattacken, wie insbesondere von Datenverschlüsselungsangriffen (Ransomware-Attacken) und Angriffen auf die Verfügbarkeit ihrer IT-Systeme (DDoS-Attacken) (für eine nähere Darstellung der Cyberlage im Jahr 2022 siehe den Bericht Cybersicherheit für das Jahr 2022). Im Lichte dieser Entwicklungen wird deutlich, dass moderne Demokratien ein entsprechendes organisatorisches, personelles und finanzielles Fundament benötigen, um die wachsende Bedeutung von Cybersicherheit gesamtstaatlich

abbilden zu können.

Aufgrund der zunehmenden Bedeutung von Cybersicherheit hat die Europäische Union (EU) Rechtsakte erlassen, die der unionsweiten Erhöhung der Cybersicherheit dienen: Einerseits die Verordnung (EU) zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie, welche die Benennung von nationalen Koordinationszentren durch die Mitgliedstaaten vorsieht. Andererseits die Richtlinie (EU) über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union (NIS2-Richtlinie), mit der beaufsichtigende Einrichtungen gesteigert und das Aufgabenspektrum der NIS-Behörden ausgeweitet wurden.

Das NISG errichtet das nationale Koordinierungszentrum für Cybersicherheit und setzt die NIS-2-Richtlinie um.

Redaktion: oesterreich.gv.at
Stand: 03.04.2024

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-04-04T11:36:57+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	