

# Bundesamt für Cyber-Sicherheit

**Mit dem Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) setzt Österreich einen zentralen Meilenstein zur Stärkung der Cyber-Resilienz. Eines dessen Kernstücke ist die Schaffung des Bundesamts für Cyber-Sicherheit als zentrale nationale Cyber-Sicherheitsbehörde.**

Das Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) dient der Umsetzung der europäischen NIS-2-Richtlinie und damit der Erfüllung Österreichs EU-rechtlicher Pflichten. Ziel ist es, ein hohes gemeinsames Cyber-Sicherheitsniveau in besonders kritischen und gesellschaftlich relevanten Sektoren sicherzustellen – von Energie und Verkehr über Gesundheitswesen und öffentlicher Verwaltung bis hin zu digitaler Infrastruktur und Wasserversorgung.

Das Gesetz regelt die behördlichen Zuständigkeiten, die nationalen Strukturen sowie die Pflichten und Sicherheitsanforderungen für sogenannte wesentliche und wichtige Einrichtungen im Cyber-Sicherheitsbereich. Gleichzeitig wird die nationale Koordinierung im Umgang mit Cyber-Bedrohungen neu organisiert.

Für die öffentliche Verwaltung bedeutet das NISG 2026 einen Paradigmenwechsel. Cyber-Sicherheit wird nicht mehr nur als rein technische Frage behandelt, sondern als verbindliche Führungs- und Organisationsaufgabe. Einrichtungen auf Bundes- und Landesebene sind ausdrücklich vom Anwendungsbereich erfasst und rücken damit stärker in den Fokus staatlicher Sicherheitsvorsorge.

Die zentralen Bestimmungen des Gesetzes treten mit 1. Oktober 2026 in Kraft. Verpflichtungen für die wesentlichen und wichtigen Einrichtungen werden gestaffelt mit Ende 2026 und im Laufe des Jahres 2027 schlagend, um betroffenen

Organisationen ausreichend Zeit für die Umsetzung zu geben.

**Bundesamt für Cyber-Sicherheit.** Eines der Kernstücke des neuen Gesetzes ist die Schaffung des Bundesamts für Cyber-Sicherheit, das als zentrale nationale Cyber-Sicherheitsbehörde fungiert. Die neue Behörde bündelt erstmals strategische Steuerung, operative Koordination und Aufsicht unter einem Dach. Sie ist dem Bundesminister für Inneres unmittelbar nachgeordnet, organisatorisch jedoch eigenständig und bundesweit zuständig.

Zu ihren Aufgaben zählen die Koordination der nationalen Cyber-Sicherheitsstrategie, das Management von Cyber-Sicherheitsvorfällen großen Ausmaßes, die Aufsicht über betroffene Einrichtungen, die Erstellung regelmäßiger Lagebilder sowie die Vertretung Österreichs in EU- und internationalen Gremien. Darüber hinaus betreibt das Bundesamt eine zentrale Anlaufstelle für Meldungen, einen Single Point of Contact (SPOC) zur grenzüberschreitenden Zusammenarbeit sowie das Computer-Notfallteam für den öffentlichen Sektor (Gov CERT).

Mit dieser neuen Struktur sollen die Zuständigkeiten im Bereich der zivilen Cyber-Sicherheit weitestgehend gebündelt und die Cyber-Resilienz von Österreich deutlich erhöht werden. Mit dem Kickoff-Event am 26. Jänner 2026 fiel der Startschuss für das Projekt, das die Aufnahme der operativen Tätigkeit des neuen

Bundesamtes mit 1. Oktober 2026 sicherstellen soll. Mehr als 40 Mitarbeiterinnen und Mitarbeiter aus allen Sektionen nahmen an der Auftaktveranstaltung teil und lassen in den nächsten Monaten ihre Expertise und Erfahrung in das Projekt einfließen.

Als Projektverantwortlicher führte der zuständige Sektionschef Christian Stella gemeinsam mit der Projektleiterin Michaela Jana Löff in die Projektstruktur und die Zielsetzung ein. Ein interaktiver Workshop bot die Möglichkeit, Ideen zu sammeln und Synergien zwischen den beteiligten Bereichen zu identifizieren.

Mit der Weiterentwicklung der bisherigen NIS-Behörde zu einem Bundesamt für Cyber-Sicherheit bereitet sich das Bundesministerium für Inneres auf die zunehmenden Gefahren im digitalen Raum vor. Dadurch soll sowohl in der Verwaltung, als auch im Bereich der kritischen Infrastruktur ein hoher Sicherheitsstandard sichergestellt werden.

**Eckpunkte des NISG 2026.** Das NISG 2026 bringt eine Reihe konkreter und verbindlicher Verpflichtungen mit sich. Im Mittelpunkt steht dabei ein systematischer und nachweisbarer Umgang mit Cyber-Risiken. Das NISG 2026 verpflichtet betroffene Einrichtungen dazu umfassende Risikomanagementmaßnahmen im Bereich der Cyber-Sicherheit zu ergreifen. Dazu zählen technische, operative und organisatorische (Schutz-) Maßnahmen, regelmäßige Sicherheitsüberprüfungen

sowie klare Verantwortlichkeiten auf Leitungsebene. Cyber-Sicherheit wird somit auch zur Chefsache. Leitungsorgane – auch im öffentlichen Bereich – müssen sicherstellen, dass geeignete organisatorische Strukturen, klare Zuständigkeiten und ausreichende Ressourcen vorhanden sind.

Ein ebenfalls zentrales Element sind die reformierten Meldepflichten. Erhebliche Cyber-Sicherheitsvorfälle müssen binnen klar definierter Fristen an das zuständige Computer-Notfallteam (CSIRT) gemeldet werden. Dieses hat die Meldungen an die Cyber-Sicherheitsbehörde weiterzugeben.

Das Gesetz fördert ausdrücklich den strukturierten Informationsaustausch zwischen Behörden, Computer-Notfallteams und anderen relevanten Stellen. Ziel ist es, aus Vorfällen zu lernen, Warnungen rasch weiterzugeben und systemische Sicherheitslücken frühzeitig zu erkennen. Auch die koordinierte Offenlegung von Schwachstellen (CVD) wird gesetzlich geregelt.

Zur Sicherstellung der Einhaltung sieht das NISG 2026 Aufsichts- und Durchsetzungsbefugnisse vor. Das Bundesamt für Cybersicherheit kann Prüfungen veranlassen, Maßnahmen anordnen und schwerwiegende Verstöße bei der zuständigen Bezirksverwaltungsbehörde anzeigen. Für Stellen der öffentlichen Verwaltung sind in diesem Zusammenhang besondere Regelungen vorgesehen, um die Funktionsfähigkeit staatlicher Aufgaben zu gewährleisten.

*Jakob Popper*