4913/AB
vom 27.05.2026 zu 5482/J (XXVIII. GP)

Bundesministerium
Bildung

bmb.gv.at

+43 1 531 20-0
Minoritenplatz 5, 1010 Wien

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2026-0.280.114

Die schriftliche parlamentarische Anfrage Nr. 5482/J-NR/2026 betreffend Cybersicherheitsvorfälle und -maßnahmen in den Bundesministerien, die die Abgeordneten zum Nationalrat Süleyman Zorba, Kolleginnen und Kollegen am 27. März 2026 an mich richteten, darf ich anhand der mir vorliegenden Informationen wie folgt beantworten:

Zu Frage 1:

- *Gab es in Ihrem Ressort im Jahr 2025 Cyberangriffe oder Cybersicherheits-Vorfälle?*
  a. Falls ja, um wie viele Angriffe/Vorfälle hat es sich gehandelt?
  b. Bei wie vielen Angriffen konnten die Täter ermittelt werden? Um welche Täter handelte es sich?

Das Bundesministerium für Bildung sieht sich – wie auch andere Ministerien, Unternehmen und Einrichtungen – kontinuierlichen Angriffsversuchen im Cyberraum ausgesetzt. Im Jahr 2025 erfolgten mehrere Überlastungsangriffe auf IT-Verfahren, sogenannte Distributed Denial of Service (DDoS) – Angriffe, in der Dauer von wenigen Minuten bis mehrere Stunden. Die Angriffe konnten aufgrund der getroffenen technischen und organisatorischen Maßnahmen erfolgreich abgewehrt werden.

Das Bundesministerium für Bildung meldet Cyberangriffe den zuständigen Strafverfolgungsbehörden. Die Strafverfolgung von Cyberkriminalität inklusive damit in Zusammenhang stehender Ermittlungsergebnisse fällt jedoch nicht in den Zuständigkeitsbereich des Bundesministeriums für Bildung. Diesbezüglich darf auf das dafür zuständige Bundesministerium für Inneres verwiesen werden.

Zu den Fragen 2 und 3:

- *Welche Präventionsmaßnahmen wurden von Ihrem Ministerium im vergangenen Jahr ergriffen, um sich vor Cyberangriffen und -kriminalität zu schützen?*
  a. Arbeiten Sie mit externen Expertinnen und Experten im Bereich Cybersicherheit zur Verhinderung von Cyberangriffen zusammen?
  b. Wenn ja, um welche Experten handelte es sich im Jahr 2025?
  c. Wie erfolgte die Auswahl?
  d. Arbeiten Sie mit externen Unternehmen im Bereich Cybersicherheit zur Verhinderung von Cyberangriffen zusammen? Wenn ja, mit welchen?
- *Gab es in Ihrem Ressort Risikoanalysen im Hinblick auf Cyberbedrohungen im Jahr 2025 und welche Ergebnisse brachten diese Analysen?*

Für das Bundesministerium für Bildung hat der Schutz der verarbeiteten Daten und der dafür eingesetzten IT-Verfahren und IKT-lnfrastrukturkomponenten eine hohe Priorität. Das Bundesministerium für Bildung verfügt daher über ein kombiniertes Informationssicherheits- und Datenschutz-Managementsystem, welches sich an internationalen Sicherheitsstandards orientiert.

Das Managementsystem sorgt unter anderem dafür, dass die diesbezüglich geltenden Rechtsvorschriften eingehalten und bestehende Risiken systematisch identifiziert, beurteilt und mittels geeigneter technischer und organisatorischer Maßnahmen unter Berücksichtigung des Stands der Technik in den Bereichen Prävention/Erkennung und Reaktion reduziert werden. Es sieht darüber hinaus vor, dass die Aktualität der geltenden Regelungen sowie die Wirksamkeit der getroffenen Maßnahmen sowohl regelmäßig als auch im Anlassfall überprüft, bewertet und evaluiert werden. Dabei wird auch die Expertise externer Stellen genutzt, wie z.B. von Computer-Notfallteams im Sinne des vierten Abschnitts des Netz- und Informationssystemsicherheitsgesetzes (NISG), BGBI. l Nr. 111/2018 idgF, und von qualifizierten Stellen im Sinne des § 3 Z 11 NISG, deren Auswahl entsprechend den gesetzlichen Kriterien erfolgt.

Die Evaluierung und Aktualisierung der diesbezüglichen Erlässe erfolgen laufend. Die öffentlich verfügbaren Sicherheitsstandards spezifizieren dafür umfassende Anforderungs- bzw. Maßnahmenkataloge.

Gemäß den Länderbewertungen des Bundesministeriums für europäische und internationale Angelegenheiten und des Bundesministeriums für Inneres (Direktion Staatsschutz und Nachrichtendienst) werden für Dienstreisen individuelle Schutzmaßnahmen entsprechend den aktuellen Sicherheitsstandards und Good Practices, wie z.B. den Handlungsempfehlungen der Direktion Staatsschutz und Nachrichtendienst gesetzt.

Hinsichtlich der angesprochenen Risikoanalysen werden im Zuge der Etablierung eines gesamtheitlichen Risikomanagementsystems insbesondere auch Aspekte der

Cybersicherheit als integraler Bestandteil der durchzuführenden Risikoanalysen betrachtet. Bereits im Jahr 2025 wurden im Hinblick auf die regulatorischen Anforderungen des NISG 2026 in Umsetzung der NIS-2-Richtlinie entsprechende Vorbereitungsmaßnahmen eingeleitet, um die Gesamtheit der eingesetzten Netz- und Informationssysteme proaktiv bewerten zu können. Diese Analysen erfolgten unter Berücksichtigung des gesetzlich geforderten „All-Gefahren-Ansatzes“, der neben physischen Risiken auch vorwiegend Cyberbedrohungen umfasst. Die Ergebnisse dieser Risikoanalysen dienen der Identifikation kritischer Assets sowie eines angemessenen Schutzniveaus gemäß dem aktuellen Stand der Technik.

Im Hinblick auf die Sicherung der Effektivität der getroffenen Schutzmaßnahmen muss jedoch von einer detaillierten Bekanntgabe Abstand genommen werden.

Zu Frage 4:

- *Gibt es in Ihrem Ministerium Cybersicherheitsbeauftragte?*
  a. Welche Abteilungen oder Teams waren im Jahr 2025 innerhalb Ihres Ministeriums dafür zuständig?
  b. Wie viele Personen waren in Ihrem Ministerium im Jahr 2025 im Bereich Cyber- und IT-Sicherheit tätig?
  c. Welche konkreten Aufgaben nahmen diese Personen wahr?

In der aktuellen Geschäftseinteilung des Bundesministeriums für Bildung ist die Abteilung Präs/9 „IT-Services Zentralstelle“ dafür vorgesehen. Da die Mitarbeiterinnen und Mitarbeiter im Bereich der Informationssicherheit in einem sensiblen Bereich tätig sind, muss aus Gründen der Informationssicherheit und des Datenschutzes von einer Nennung weiterer Details Abstand genommen werden.

Zu Frage 5:

- *Wie hoch war das Budget Ihres Hauses für IT- und Cybersicherheit im Jahr 2025?*

Da IT- und Cybersicherheit eine Querschnittsmaterie darstellen, sind die damit verbundenen Aufwände und Kosten nicht eindeutig zuordenbar.

Zu Frage 6:

- *Gab es im Jahr 2025 konkrete verpflichtende Schulungsangebote in Fragen der IT- und Cybersicherheit für Mitarbeiter:innen Ihres Hauses sowie nachgeordneter Dienststellen?*
  a. Wenn ja, um welche Schulungsangebote handelte es sich?
  b. Wie hoch waren die Kosten für diese Schulungen?

Es werden in regelmäßigen Abständen Schulungen angeboten und abgehalten. Die Schulungen werden auf die unterschiedlichen Bedürfnisse der jeweiligen Personengruppen angepasst. Im Rahmen der Willkommensveranstaltung für neu eingetretene Bedienstete erfolgt eine grundlegende Schulung zu Datenschutz und IT-

Sicherheit. Weiters werden über das Bildungsprogramm der Verwaltungsakademie des Bundes umfassende Aus-, Fort- und Weiterbildungsmaßnahmen für diesen Themenbereich angeboten.

Wien, 27. Mai 2026

Christoph Wiederkehr, MA

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR BILDUNG @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Bildung
	Datum/Zeit	2026-05-27T09:01:29+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	2097799830
	Hinweis	Dieses Dokument wurde amtssigniert.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at. Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.bmb.gv.at/verifizierung.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-05-27T09:07:30+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	