5622/AB
vom 31.07.2026 zu 6214/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: 2026-0.468.725

Die schriftliche parlamentarische Anfrage Nr. 6214/J-NR/2026 betreffend Hacking-Angriffe auf Ministerien – Daten 2025, die die Abgeordneten zum Nationalrat Rosa Ecker, MBA, Kolleginnen und Kollegen am 1. Juni 2026 an mich richteten, darf ich anhand der mir vorliegenden Informationen wie folgt beantworten:

Zu Frage 1:

- *Wie beurteilen Sie die aktuelle Gefahr, dass Hackerangriffe gegen Ihr Ressort vorgenommen werden und gelingen könnten?*

Einleitend wird festgehalten, dass von einer detaillierten Darstellung einzelner technischer Schutzmaßnahmen, eingesetzter Systeme oder konkreter Abläufe im Hinblick auf die Sicherung der Effektivität dieser Maßnahmen Abstand genommen werden muss.

Angriffe und Angriffsversuche auf mit dem Internet verbundene IT-Systeme können grundsätzlich nie ausgeschlossen werden. Das Bundesministerium für Bildung sieht sich – wie andere öffentliche Stellen, Unternehmen und Einrichtungen auch – laufend Angriffsversuchen im Cyberraum ausgesetzt.

Die Gefahr wird daher als fortlaufend bestehendes Risiko beurteilt, dem mit technischen und organisatorischen Sicherheitsmaßnahmen nach dem Stand der Technik begegnet wird. Diese Maßnahmen umfassen insbesondere die Bereiche Prävention, Absicherung, Erkennung sowie Incident-Response und werden im Rahmen eines risikobasierten Ansatzes laufend weiterentwickelt.

Ziel der getroffenen Maßnahmen ist es, Risiken zu reduzieren, Angriffe möglichst frühzeitig zu erkennen, deren Auswirkungen zu begrenzen sowie im Anlassfall rasch und strukturiert reagieren zu können.

Zu Frage 2:

- *Inwieweit ist Ihr Ressort auf mögliche Hackerangriffe vorbereitet?*

Das Bundesministerium für Bildung ist auf mögliche Hackerangriffe durch technische und organisatorische Sicherheitsmaßnahmen nach dem Stand der Technik vorbereitet. Diese Maßnahmen umfassen insbesondere die Bereiche Prävention, Absicherung, Erkennung und Reaktion auf Sicherheitsvorfälle.

IKT-Sicherheit und Datensicherheit werden dabei als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden die IKT-Sicherheitsstruktur sowie die dahinterliegenden Prozesse im Rahmen eines risikobasierten Ansatzes laufend überprüft, bewertet und angepasst. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den zuständigen technischen Stellen zeitnah berücksichtigt.

Für den Anlassfall bestehen organisationsspezifische Vorgehensweisen und Notfallpläne. Darüber hinaus werden Sicherheitsmaßnahmen regelmäßig evaluiert; dabei wird erforderlichenfalls auch externe Expertise beigezogen.

Zu Frage 3:

- *Gab es im Jahr 2025 sogenannte „Überlastungsangriffe" oder andere abgewehrte Angriffe?*
  a. Wenn ja, wann?
  b. Wenn ja, in welchem Umfang?
  c. Wenn ja, kennen Sie den Ursprung dieser Hacking-Angriffe?

Im Jahr 2025 erfolgten mehrere Überlastungsangriffe auf IT-Verfahren des Bundesministeriums, sogenannte Distributed-Denial-of-Service- bzw. DDoS-Angriffe. Diese Angriffe konnten aufgrund der getroffenen technischen und organisatorischen Sicherheitsmaßnahmen erfolgreich abgewehrt werden.

Die Angriffe im Jahr 2025 wiesen jeweils eine Dauer von wenigen Minuten bis zu mehreren Stunden auf. Eine darüberhinausgehende detaillierte zeitliche oder technische Aufschlüsselung wird im Hinblick auf die Sicherung der Effektivität der getroffenen Schutzmaßnahmen nicht vorgenommen.

Cyberangriffe werden den zuständigen Strafverfolgungsbehörden gemeldet. Die Strafverfolgung von Cyberkriminalität sowie damit zusammenhängende Ermittlungsergebnisse, insbesondere zur Herkunft oder zu möglichen Täterinnen und Tätern, fallen nicht in den Zuständigkeitsbereich des Bundesministeriums für Bildung. Diesbezüglich wird auf das zuständige Bundesministerium für Inneres verwiesen.

Zu Frage 4:

- *Wie wird seitens Ihres Ressorts aktuell für die Datensicherheit gesorgt?*

Im Bundesministerium für Bildung wird sowohl durch technische als auch durch organisatorische Maßnahmen für Datensicherheit gesorgt. Der Schutz der verarbeiteten Daten sowie der dafür eingesetzten IT-Verfahren und IKT-Infrastrukturkomponenten hat hohe Priorität.

IKT-Sicherheit und damit auch Datensicherheit werden als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden bestehende Risiken systematisch identifiziert, beurteilt und durch geeignete technische und organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik reduziert. Die IKT-Sicherheitsstruktur sowie die dahinterliegenden Prozesse werden im Rahmen eines risikobasierten Ansatzes laufend überprüft, bewertet und angepasst.

Das Ressort verfügt über ein kombiniertes Informationssicherheits- und Datenschutz-Managementsystem, das sich an internationalen Sicherheitsstandards orientiert. Dieses dient insbesondere der Einhaltung der einschlägigen Rechtsvorschriften, der laufenden Bewertung bestehender Risiken sowie der Überprüfung der Wirksamkeit der getroffenen Maßnahmen.

Zugriffsberechtigungen auf verarbeitete Daten erfolgen nach den Grundsätzen der DSGVO (insbesondere Rechtmäßigkeit, Zweckbindung und Datenminimierung) unter Berücksichtigung der jeweiligen Sensibilität der Daten. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den zuständigen technischen Stellen zeitnah berücksichtigt. Die IT-Abteilungen, die Arbeitsgruppe Datenschutz und der Datenschutzbeauftragte des Bundesministeriums für Bildung arbeiten eng abgestimmt, um ein hohes Niveau des Datenschutzes und der Datensicherheit zu gewährleisten.

Zu Frage 5:

- *Wer kann wie auf die von Ihnen verarbeiteten Daten aktuell zugreifen?*

Der Zugriff auf die im Bundesministerium für Bildung verarbeiteten Daten erfolgt grundsätzlich nach dem Bedarfsprinzip (vgl. auch Frage 4) und unter Berücksichtigung der jeweiligen Sensibilität der Daten. Es ist sichergestellt, dass nur Bedienstete des Hauses, bzw. DSGVO-konform beauftragte Auftragsverarbeiter auf Daten des Ressorts im Rahmen ihrer gesetzlichen Zuständigkeiten zugreifen.

Soweit Auftragsverarbeiter eingebunden sind, erhalten diese einen Zugriff ausschließlich im jeweils erforderlichen Umfang und auf Grundlage der einschlägigen vertraglichen, datenschutzrechtlichen und sicherheitsrelevanten Vorgaben. Auch hierbei gilt das Prinzip der Erforderlichkeit.

Die Vergabe, Änderung und Entziehung von Zugriffsberechtigungen erfolgt im Rahmen der dafür vorgesehenen Berechtigungs- und Administrationsprozesse. Von einer detaillierten Darstellung einzelner Berechtigungsmodelle, Systeme oder konkreter Zugriffspfade muss im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Zu Frage 6:

- *Konnten im Jahr 2025 durch Ihr Ressort Datenlecks festgestellt werden?*
  a. Wenn ja, wie konnte es dazu kommen?
  b. Wenn ja, welche Daten waren betroffen?

Für den Bereich der Zentralstelle des Bundesministeriums für Bildung konnten im Jahr 2025 keine Datenlecks festgestellt werden.

Zu Frage 7:

- *Welche internen/externen Sicherheitssysteme überwachen derzeit die vorhandenen Daten, Betriebssysteme und elektronischen Einheiten?*
  a. Wie hoch sind die aktuellen jährlichen Kosten hierfür (Einkauf, Installation, Wartung, Betreuung, Ausbau etc.)?
  b. Welche Kosten sind 2025 entstanden?

Im Bundesministerium für Bildung kommen auf Grundlage laufender Risiko- und Bedrohungsbeurteilungen unterschiedliche interne und externe Sicherheitssysteme sowie zugehörige Sicherheitsdienstleistungen zum Einsatz. Diese dienen insbesondere der Absicherung, Überwachung, Erkennung und Behandlung sicherheitsrelevanter Ereignisse im Bereich der eingesetzten Daten, Betriebssysteme, IT-Verfahren, Netz- und Informationssysteme sowie sonstiger elektronischer Einheiten.

Die eingesetzten Systeme bezwecken keine inhaltliche Überwachung von Daten, sondern dienen der Gewährleistung von Informationssicherheit, Datensicherheit, Systemverfügbarkeit sowie der Erkennung und Abwehr sicherheitsrelevanter Ereignisse.

Die eingesetzten Maßnahmen und Systeme werden entsprechend dem Stand der Technik sowie auf Grundlage der jeweiligen Bedrohungslage laufend überprüft, angepasst und weiterentwickelt. Von einer detaillierten Auflistung einzelner Sicherheitssysteme, Produkte, Hersteller, technischer Komponenten oder konkreter Einsatzbereiche muss im Hinblick auf die Sicherung der Effektivität der getroffenen Schutzmaßnahmen Abstand genommen werden.

IT- und Cybersicherheit ist eine Querschnittsmaterie. Die damit verbundenen Aufwände und Kosten sind daher nicht durchgehend eindeutig einzelnen Sicherheitssystemen oder ausschließlich dem Bereich Cybersicherheit zuordenbar. Entsprechende Aufwände sind sachlich bei einschlägigen IT- bzw. ADV-Aufwänden, Werkleistungen, Betriebs-, Wartungs-, Betreuungs- und Ausbaukosten mitumfasst.

Eine isolierte und vollständige Auswertung der aktuellen jährlichen Kosten sowie der im Jahr 2025 entstandenen Kosten ausschließlich für die genannten Sicherheitssysteme ist daher aus den bestehenden haushalts- und verrechnungstechnischen Strukturen nicht möglich.

Zu Frage 8:

- *In welchem zeitlichen Abstand werden diese Sicherheitssysteme auf die neuesten Entwicklungen und Bedrohungen angepasst und adaptiert?*

Die Anpassung und Adaptierung der eingesetzten Sicherheitssysteme erfolgt nicht in einem einheitlichen starren Zeitintervall, sondern laufend, anlassbezogen sowie im Rahmen zyklischer risikobasierter Beurteilungen.

Neben technischen Maßnahmen zum Update und Upgrade bestehender Systeme erfolgt eine regelmäßige risikobasierte Bewertung der eingesetzten bzw. künftig zum Einsatz zubringenden Sicherheitssysteme. Dabei werden insbesondere aktuelle Bedrohungslagen, Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess, technische Entwicklungen, einschlägige Sicherheitsstandards sowie organisationsspezifische Risiken berücksichtigt.

Darüber hinaus werden die Aktualität der geltenden Regelungen sowie die Wirksamkeit der getroffenen Maßnahmen regelmäßig und im Anlassfall überprüft, bewertet und erforderlichenfalls angepasst.

Von einer detaillierten Darstellung konkreter Aktualisierungszyklen, eingesetzter Produkte oder technischer Abläufe muss im Hinblick auf die Sicherung der Effektivität der getroffenen Schutzmaßnahmen Abstand genommen werden.

Zu Frage 9:

- *Wer ist mit der Instandhaltung der ministeriellen Sicherheitssysteme beauftragt?*

Die Instandhaltung der ministeriellen Sicherheitssysteme erfolgt im Zusammenwirken der jeweils zuständigen internen Organisationseinheiten des Bundesministeriums für Bildung, insbesondere im Bereich IT-Services und Informationssicherheit, sowie – soweit erforderlich – durch vertraglich gebundene externe IT- und Sicherheitsdienstleister.

Die laufende Betreuung umfasst insbesondere den sicheren Betrieb, die Wartung, Aktualisierung, Anpassung und Weiterentwicklung der eingesetzten Sicherheitskomponenten sowie die Berücksichtigung aktueller Risiko- und Bedrohungsbeurteilungen. Für bestimmte bundesweite Querschnittsanwendungen und zentral betriebene IT-Verfahren erfolgen Betrieb und sicherheitsrelevante Betreuung im Rahmen der dafür bestehenden Zuständigkeiten und Leistungsbeziehungen, insbesondere durch zentrale IT-Dienstleister des Bundes.

Die Auswahl und Beauftragung externer Dienstleister erfolgt nach den jeweils einschlägigen rechtlichen, vergabe- und sicherheitsrelevanten Vorgaben. Soweit externe Stellen eingebunden sind, erfolgt dies nur im jeweils erforderlichen Umfang und unter Berücksichtigung der einschlägigen datenschutz- und informationssicherheitsrechtlichen Anforderungen.

Von einer detaillierten Nennung einzelner Personen, konkreter Dienstleister, Produkte, Wartungsmodelle oder technischer Zuständigkeiten muss im Hinblick auf Datenschutz, Informationssicherheit und die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Zu Frage 10:

- *Wie ist die derzeitige Vorgabe im Umgang mit Hacking-Angriffen?*
  a. Ist diese Vorgehensweise in allen Resorts einheitlich?
  b. Wie oft werden derartige Szenarien durchgespielt und Vorkehrungen getroffen?

Das Netz- und Informationssystemsicherheitsgesetz regelt grundlegende Anforderungen im Bereich der Netz- und Informationssystemsicherheit. Das konkrete Vorgehen im Fall eines Hacking-Angriffs obliegt dem jeweiligen Ressort im eigenen Verantwortungsbereich.

Im Bundesministerium für Bildung bestehen für derartige Fälle organisationsspezifische Vorgaben und Notfallpläne. Diese regeln insbesondere die strukturierte Behandlung von Sicherheitsvorfällen, die interne Eskalation, die Einbindung der zuständigen technischen und organisatorischen Stellen sowie erforderlichenfalls die Meldung an die zuständigen Behörden. Die Maßnahmen orientieren sich an den Bereichen Prävention, Erkennung, Reaktion und Wiederherstellung.

Die Wirksamkeit der getroffenen Maßnahmen sowie die Aktualität der zugrunde liegenden Regelungen wird regelmäßig und im Anlassfall überprüft, bewertet und erforderlichenfalls angepasst. Entsprechende Vorkehrungen und Szenarien werden risikobasiert behandelt. Von einer detaillierten Darstellung konkreter Abläufe, Eskalationswege, Übungsinhalte oder Zeitpläne muss im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Wien, 31. Juli 2026

Christoph Wiederkehr, MA

Unterzeichner	Bundesministerium für Bildung
Datum/Zeit	2026-07-31T09:31:12+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	2026-07-31T09:42:54+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	