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: 2025-0.257.505

Die schriftliche parlamentarische Anfrage Nr. 865/J-NR/2025 betreffend Mögliche Hackerangriffe auf Ihr Ministerium, die die Abgeordneten zum Nationalrat Rosa Ecker, MBA, Kolleginnen und Kollegen am 27. März 2025 an mich richteten, darf ich anhand der mir vorliegenden Informationen wie folgt beantworten:

Eingangs wird darauf hingewiesen, dass es aufgrund der Bundesministeriengesetz-Novelle 2025 zum Teil zu erheblichen Veränderungen in der Zusammensetzung der Bundesministerien kam. Nach den Bestimmungen des Bundesministeriengesetzes in der nunmehr geltenden Fassung, BGBl. I Nr. 10/2025, bin ich zur Beantwortung dieser parlamentarischen Anfrage für den Bereich Bildung zuständig.

Zu Frage 1:

- *Besteht aktuell die Gefahr, dass Hackerangriffe gegen Ihr Ministerium vorgenommen werden und gelingen könnten?*
  a. Wenn ja, wie sind Sie aktuell auf so einen Fall vorbereitet?

Angriffe und Angriffsversuche auf mit dem Internet verbundene IT-Systeme können nie ausgeschlossen werden. Das Bundesministerium (Bereich Bildung) ist zur Abwehr solcher Versuche durch technische und organisatorische Sicherheitsmaßnahmen auf dem Stand der Technik in den Bereichen Prävention, Absicherung, Erkennung und Incident-Response vorbereitet.

Zu Frage 2:

- *Gab es im Jahr 2024 sogenannte „Überlastungsangriffe" oder andere abgewehrte Angriffe?*
  a. Wenn ja, wann?
  b. Wenn ja, in welchem Umfang?

Auch im Jahr 2024 gab es eine Vielzahl von Überlastungsangriffen (DDoS), deren Auswirkungen durch eine Kombination von automatischer Mitigierung und manuellem Eingriff minimiert werden konnten. Allgemein wird festgehalten, dass DDoS-Angriffe, die eine Dauer von einigen Minuten bis Stunden aufweisen, als alltäglich angesehen werden müssen und Teil jeder Standardrisikobewertung sind. Ergänzend darf auf die Beantwortung der Parlamentarischen Anfrage Nr. 564/J-NR/2025 vom 26. Februar 2025 verwiesen werden.

Zu Frage 3:

- *Wie wird seitens Ihres Ministeriums aktuell für die Datensicherheit gesorgt?*
  a. Wer kann auf die von Ihnen verarbeiteten Daten zugreifen?

Im Bundesministerium (Bereich Bildung) wird sowohl technisch als auch organisatorisch für Datensicherheit gesorgt. IKT-Sicherheit (und damit auch Datensicherheit) wird als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden mittels risikobasiertem Ansatz kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur und der dahinterliegenden Prozesse vorgenommen. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Technikerinnen und Technikern des Ressorts zeitnahe umgesetzt. Zugriffsberechtigungen erfolgen nach dem Bedarfsprinzip unter Berücksichtigung der Sensibilität der Daten.

Zu Frage 4:

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

Seitens des Bundesministeriums (Bereich Bildung) konnten zuletzt keine Datenlecks festgestellt werden.

Zu den Fragen 5 und 6:

- *Welche internen/externen Sicherheitssysteme überwachen derzeit die vorhandenen Daten, Betriebssysteme und elektronischen Einheiten?*
  a. Welche Kosten entstehen für diese Systeme jährlich? (Einkauf, Installation, Wartung, Betreuung, Ausbau etc)
  b. Welche Kosten sind 2023 und 2024 entstanden?
- *In welchem zeitlichen Abstand werden diese Sicherheitssysteme auf die neuesten Entwicklungen und Bedrohungen angepasst und adaptiert?*

Im Bundesministerium (Bereich Bildung) werden basierend auf erfolgten Risikobewertungen und Bedrohungsanalysen unterschiedliche Sicherheitssysteme zum Einsatz gebracht. Neben technischen Maßnahmen zum Update und Upgrade bestehender Systeme erfolgt zyklisch eine risikobasierte Beurteilung auf zum Einsatz zu bringende Sicherheitssysteme hin.

Von einer detaillierten Auflistung der Maßnahmen oder der Auflistung einzelner im Einsatz befindlicher Produkte muss im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Zu Frage 7:

- *Wie ist die vorgeschriebene Vorgehensweise, wenn so ein Hackingangriff erfolgreich ist und Maßnahmen ergriffen werden müssen?*
  a. Ist diese Vorgehensweise in allen Ministerien einheitlich?
  b. Wie oft werden derartige Szenarien durchgespielt und Vorkehrungen getroffen?

Das Netz- und Informationssystemsicherheitsgesetz (NISG), BGBI. l Nr. 111/2018, regelt Grundsätzliches, den Ministerien obliegt das organisationsspezifische Vorgehen im eigenen Verantwortungsbereich. Im Bundesministerium (Bereich Bildung) regeln Notfallpläne das Vorgehen im Falle von Cyberangriffen. Darüber hinaus wird auf die Ausführungen zu den Fragen 5 und 6 hingewiesen.

Wien, 27. Mai 2025

Christoph Wiederkehr, MA

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR BILDUNG
@ AMTSSIGNATUR

Unterzeichner	Bundesministerium für Bildung
Datum/Zeit	2025-05-27T09:57:10+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	2025-05-27T10:58:39+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	