18219/AB
vom 12.08.2024 zu 18816/J (XXVII. GP)

Bundesministerium
Bildung, Wissenschaft
und Forschung

bmbwf.gv.at

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

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2024-0.441.562

Die schriftliche parlamentarische Anfrage Nr. 18816/J-NR/2024 betreffend Mögliche Hackerangriffe auf Ihr Ministerium, die die Abgeordneten zum Nationalrat Rosa Ecker, MBA, Kolleginnen und Kollegen am 12. Juni 2024 an mich richteten, darf ich anhand der mir vorliegenden Informationen wie folgt beantworten:

Zu Frage 1:

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

Angriffsversuche auf die IT-Systeme des Bundesministeriums für Bildung, Wissenschaft und Forschung können nie ausgeschlossen werden. Das Bundesministerium für Bildung, Wissenschaft und Forschung ist zur Abwehr solcher Versuche allerdings durch technische und organisatorische Sicherheitsmaßnahmen in den Bereichen Prävention, Absicherung, Erkennung und Incident Response vorbereitet.

Zu Frage 2:

- *Gab es in den letzten fünf Jahren sogenannte „Überlastungsangriffe" oder andere, abgewehrte Angriffe?*
  a. Wenn ja, wann?
  b. Wenn ja, in welchem Umfang?

Mit dem Internet verbundene IT-Systeme sind grundsätzlich zahlreichen, meist automatisierten Angriffsversuchen ausgesetzt. Diese werden durch die IKT-Sicherheitssysteme ebenso weitestgehend automatisiert abgewehrt.

In Einzelfällen kommt es zu Angriffsversuchen, welche über diesem „Grundrauschen“ liegen. In den letzten Jahren waren dies insbesondere folgende gezielten Aktionen:

- Angriffe bis 2022: Dazu wird auf die Beantwortung der Parlamentarischen Anfrage Nr. 11851/J-NR/2022 vom 8. Juli 2022 verwiesen.
- Angriffe 2023: Drei DDoS Angriffe auf Services des Bundesministeriums für Bildung, Wissenschaft und Forschung; die automatisierten Abwehrsysteme des Bundesministeriums für Bildung, Wissenschaft und Forschung verhinderten ein Wirksamwerden der Angriffe.
- Angriffe 2024: Zwei DDoS Angriffe auf Services des Bundesministeriums für Bildung, Wissenschaft und Forschung; die automatisierten Abwehrsysteme des Bundesministeriums für Bildung, Wissenschaft und Forschung verhinderten ein Wirksamwerden der Angriffe.

Zu den Fragen 3 sowie 5 und 6:

- *Wie wird seitens Ihres Ministeriums für die Datensicherheit gesorgt?*
- *Gibt es zusätzlich ein eigenes Sicherheitssystem für Ihr Ministerium?*
- *In welchem zeitlichen Abstand werden diese Sicherheitssysteme auf die neuesten Entwicklungen und Bedrohungen angepasst und adaptiert?*

IKT-Sicherheit (und damit auch Datensicherheit) wird im Bundesministerium für Bildung, Wissenschaft und Forschung als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur und den dahinterliegenden Prozessen vorgenommen. Dies betrifft sowohl die Beschaffung von State-of-the-Art IKT-Sicherheitsinfrastruktur als auch die permanente Evaluierung und Anpassung der Prozesse. Darüber hinaus werden basierend auf den aktuellen Bedrohungslagen Maßnahmen zur Hebung der Awareness durchgeführt. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Technikerinnen und Technikern des Ressorts zeitnahe umgesetzt.

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 4:

- *Gibt es ein übergeordnetes Sicherheitssystem, das über alle Bundesministerien und die vorhandenen Daten wacht?*
  a. Wenn nein, ist zukünftig ein derartiges Sicherheitssystem geplant?
  b. Wenn ja, wann soll dieses in Betrieb gehen?

Die Sicherung der IKT-Systeme fällt grundsätzlich in die Verantwortung der zuständigen obersten Organe. Das Bundesministerium für Bildung, Wissenschaft und Forschung arbeitet u.a. über das Computer-Notfallteam der öffentlichen Verwaltung (govCERT) eng

mit anderen Ressorts zusammen, wobei es einen fortlaufenden Austausch über das aktuelle Lagebild gibt. Für die wichtigen Querschnittsapplikationen des Bundes, wie ELAK oder IT-Personalmanagement und Haushaltsverrechnung, betreibt die BRZ GmbH zentral ein eigenes Sicherheitssystem. Die IKT-Sicherheitsbeauftragten und/oder Informationssicherheitsbeauftragten der Bundesministerien treffen einander unter Schirmherrschaft des Bundeskanzleramtes auf regelmäßiger Basis und teilen Informationen und Best-Practices.

Darüber hinaus darf auf die Beantwortung der Parlamentarischen Anfrage Nr. 11856/J-NR/2022 vom 8. Juli 2022 durch den Bundesminister für Inneres sowie die Beantwortung der Parlamentarischen Anfrage Nr. 11851/J-NR/2022 vom 8. Juli 2022 verwiesen werden.

Zu Frage 7:

- *Welches Gremium ist vorgesehen, wenn so ein Angriff erfolgreich ist und Maßnahmen ergriffen werden müssen?*

Sollte ein Cyberangriff krisenhafte Auswirkungen verursachen, tritt das Cyberkrisenmanagement in Kraft. Die Strukturen und Zuständigkeiten sind im Netz- und Informationssystemsicherheitsgesetz geregelt. Treten darüber hinaus die Cyberdimension überschreitende Effekte auf, erfolgt die Koordination der Krise gemäß Bundes-Krisensicherheitsgesetz (B-KSG).

Zu Frage 8:

- *Werden derartige Szenarien durchgespielt und Vorkehrungen getroffen?*
  a. Wenn ja, wie oft?
  b. Wenn ja, in welchem Umfang?
  c. Wenn nein, warum nicht?

Das Bundesministerium für Bildung, Wissenschaft und Forschung verfügt über einen Notfallplan, der die einzuleitenden Maßnahmen und Zuständigkeiten bei auftretenden Vorfällen im Zusammenhang mit wesentlichen Cyberbedrohungen regelt, und nimmt an Notfallübungen in Form von Planspielen teil.

Es erfolgt zudem ein regelmäßiger Austausch mit den fachlich zuständigen Ministerien und den in Österreich existierenden Arbeitskreisen sowohl im Bundesumfeld als auch im tertiären (Bildungs-)Bereich.

Zu Frage 9:

- *Wie lange würde es voraussichtlich dauern, um ein Parallelsystem herstellen zu können, um auch weiterhin einsatzfähig zu sein?*

Ziel des Bundesministeriums für Bildung, Wissenschaft und Forschung ist es, durch technische Maßnahmen zur Trennung kritischer Systeme sowie durch die fortlaufenden Anpassungen an sich ändernde Bedrohungen weitreichende Auswirkungen nach Cyberangriffen zu verhindern.

Wien, 12. August 2024

Ao. Univ.-Prof. Dr. Martin Polaschek

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR BILDUNG, WISSENSCHAFT UND FORSCHUNG @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Bildung, Wissenschaft und Forschung
	Datum/Zeit	2024-08-12T10:10:00+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.	1977932242
	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.bmbwf.gv.at/verifizierung.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-08-12T10:25:18+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	