18198/AB
vom 12.08.2024 zu 18800/J (XXVII. GP)

Bundesministerium
Arbeit und Wirtschaft

bmaw.gv.at

Univ.-Prof. Dr. Martin Kocher
Bundesminister

Stubenring 1, 1010 Wien

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2024-0.440.863

Ihr Zeichen: BKA - PDion (PDion)18800/J-NR/2024

Wien, am 12. August 2024

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Rosa Ecker, MBA und weitere haben am 12.06.2024 unter der **Nr. 18800/J** an mich eine schriftliche parlamentarische Anfrage betreffend **Mögliche Hackerangriffe auf Ihr Ministerium** gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zur Frage 1

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

Angriffsversuche und Angriffe selbst auf die IKT-Systeme des Ressorts können nie ausgeschlossen werden. Das Bundesministerium für Arbeit und Wirtschaft (BMAW) 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.

Zur Frage 2

- *Gab es in den letzten fünf Jahren sogenannte "Überlastungsangriffe" oder andere, abgewehrte Angriffe?*

- *Wenn ja, wann?*
- *Wenn ja, in welchem Umfang?*

Mit dem Internet verbundene IKT-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. Dazu ist auf die Beantwortung der parlamentarischen Anfrage Nr. 18865/J zu verweisen.

Zu den Fragen 3, 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 BMAW als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz unter Abstützung auf entsprechende Systeme 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 den betriebsführenden Einheiten zeitnah umgesetzt.

Von einer detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. zum Erhalt eines hohen IKT- Sicherheitsniveaus gemäß Netz- und Informationssystemsicherheitsgesetz (NIS-Gesetz) oder einer Auflistung einzelner im Einsatz befindlicher Produkte muss im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Zur Frage 4

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

Prinzipiell fällt die Sicherung der IKT-Systeme in die Verantwortung der zuständigen obersten Organe. Das Ressort 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 Chief Information Security Officer, IKT-Sicherheitsbeauftragten und/oder Informationssicherheitsbeauftragten der Bundesministerien treffen einander unter Schirmherrschaft des Bundeskanzleramtes auf regelmäßiger Basis und teilen Informationen und Best-Practices.

Darüber hinaus ist auf die Beantwortungen der parlamentarischen Anfragen Nr. 11854/J und Nr. 11856/J zu verweisen.

Zur 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 NIS-Gesetz geregelt. Treten darüber hinaus die Cyberdimension überschreitende Effekte auf, erfolgt die Koordination der Krise gemäß Bundes-Krisensicherheitsgesetz.

Zur Frage 8

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

Das BMAW verfügt über einen Notfallplan, der die einzuleitenden Maßnahmen und Zuständigkeiten bei auftretenden Vorfällen im Zusammenhang mit wesentlichen Cyberbedrohungen regelt und führt regelmäßige Notfallübungen in Form von Ausfallstests, Simulationen, Workshops und dergleichen durch.

Zur Frage 9

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

Die technischen Maßnahmen zur Trennung kritischer Systeme sowie die fortlaufenden Anpassungen an sich ändernde Bedrohungen sollen weitreichende Auswirkungen nach Cyberangriffen verhindern.

Univ.-Prof. Dr. Martin Kocher

Elektronisch gefertigt

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR ARBEIT UND WIRTSCHAFT @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Arbeit und Wirtschaft
	Datum/Zeit	2024-08-12T07:52:46+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.	1056650987
	Hinweis	Dieses Dokument wurde amtssigniert.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-08-12T07:55:21+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	