Bundesministerium
Land- und Forstwirtschaft,
Regionen und Wasserwirtschaft

bml.gv.at

Mag. Norbert Totschnig, MSc
Bundesminister für Land- und Forstwirtschaft,
Regionen und Wasserwirtschaft

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2024-0.439.827

Ihr Zeichen: BKA - PDion
(PDion)18801/J-NR/2024

Wien, 12. August 2024

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Rosa Ecker, MBA, Kolleginnen und Kollegen haben am 12. Juni 2024 unter der Nr. **18801/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?
  a. Wenn ja, wie sind Sie auf so einen Fall vorbereitet?

Angriffsversuche und Angriffe selbst auf die IT Systeme des Bundesministeriums für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft können nie ausgeschlossen werden. Das Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft 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?
  a. Wenn ja, wann?
  b. Wenn ja, in welchem Umfang?

Mit dem Internet verbundene IT-Systeme sind grundsätzlich zahlreichen, meist automatisierten Angriffsversuchen ausgesetzt. Diese Angriffe, wie zum Beispiel Portscans von extern, unerlaubter Zugriff auf Ressourcen, Spam und Malware, werden laufend erfolgreich durch die IKT-Sicherheitssysteme des Bundesministeriums für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft abgewehrt.

Es kam vereinzelt zu versuchten Überlastungsangriffen, diese wurden durch geeignete technische Maßnahmen abgeschwächt. Dadurch konnte bei jedem dieser Angriffe ein Schaden abgewendet werden.

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 Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft 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 dem Fachpersonal des Ressorts zeitnahe umgesetzt.

Von einer detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. zum Erhalt eines hohen IKT-Sicherheitsniveaus gemäß dem Netz- und Informationssystemsicherheitsgesetz (NISG), BGBl. I Nr. 111/2018, oder aber auch der 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?
  a. Wenn nein, ist zukünftig ein derartiges Sicherheitssystem geplant?
  b. Wenn ja, wann soll dieses in Betrieb gehen?

Prinzipiell fällt die Sicherung der IKT Systeme in die Verantwortung der zuständigen obersten Organe. Das Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft arbeitet mit dem Government Computer Emergency Response Team (govCERT) der öffentlichen Verwaltung zusammen und erhält regelmäßig Informationen zur aktuellen Bedrohungssituation. Wichtige Querschnittsapplikationen des Bundes, wie ELAK oder Personalmanagement und Haushaltsverrechnung, werden zusätzlich über ein eigenes Sicherheitssystem der BRZ GmbH gesichert. Die IKT-Sicherheitsbeauftragten der Bundesministerien treffen einander unter Schirmherrschaft des Bundeskanzleramtes auf regelmäßiger Basis und teilen Informationen und Best-Practices.

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 NISG geregelt. Treten darüber hinaus die Cyberdimension überschreitende Effekte auf, erfolgt die Koordination der Krise gemäß Bundes-Krisensicherheitsgesetz, BGBl. I Nr. 89/2023.

Zur 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?

Derartige Szenarien werden im Abstand von etwa zwei Jahren im IKT-Sicherheitsvorfall-Team durchgespielt und bei Bedarf weitere Stellen eingebunden.

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. Die Durchlaufzeit zur Herstellung von Parallelsystemen variiert jedoch abhängig vom Angriffsszenario und dem damit verbundenen Schadensausmaß. Der Aufbau erfolgt nach Priorität in sequenzieller Abfolge.

Mag. Norbert Totschnig, MSc

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR LAND- UND FORSTWIRTSCHAFT, REGIONEN UND WASSERWIRTSCHAFT @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft
	Datum/Zeit	2024-08-12T11:16:40+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.	1921487807
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur und des Ausdrucks finden Sie unter: https://www.bml.gv.at/amtssignatur	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-08-12T11:19:00+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	