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: 2022-0.506.643

Ihr Zeichen: BKA - PDion
(PDion)11859/J-NR/2022

Wien, 8. September 2022

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Rosa Ecker, MBA, Kolleginnen und Kollegen haben am 08.07.2022 unter der Nr. **11859/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 auch nur im Geringsten die Möglichkeit, dass derartige Hackerangriffe mit Datenklau gegen Ihr Ministerium vorgenommen werden und gelingen könnten?
  a. Wenn ja, wie sind Sie konkret auf so einen Zwischenfall vorbereitet?

Angriffsversuche und Angriffe selbst können nie ausgeschlossen werden. Die Aufrechterhaltung des ordentlichen Betriebes hat für die IKT des Bundesministeriums für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft einen sehr hohen Stellenwert. Es werden – den wirtschaftlichen Rahmenbedingungen entsprechend – viele Maßnahmen gesetzt, um die EDV-Infrastruktur sowie alle Systeme und Applikationen am letztmöglichen technischen Sicherheitsstandard zu betreiben. Aus Gründen der IT-Sicherheit des Ressorts können nähere Details nicht bekannt gegeben werden.

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?

Es kam zu keinen Überlastungsangriffen. Angriffe wie zum Beispiel Portscans von extern, unerlaubter Zugriff auf Ressourcen, Spam und Malware werden laufend erfolgreich von den Schutzsystemen des Bundesministeriums für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft abgewehrt.

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 den Technikern 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. 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 SAP, werden zusätzlich über ein eigenes Sicherheitssystem der BRZ GmbH gesichert.

Darüber hinaus wird auf die Beantwortung der parlamentarischen Anfrage Nr. 11856/J vom 8. Juli 2022 durch den Bundesminister für Inneres verwiesen.

Zur Frage 7:

- Welches Gremium ist vorgesehen, wenn so wie im Fall des Bundeslands Kärnten 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.

Zur Frage 8:

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

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, wie im vorliegenden Fall des Bundeslands Kärnten, ein Parallelsystem wieder 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 wie im Fall Kärnten verhindern. Die Durchlaufzeit variiert jedoch abhängig vom Angriffsszenario und dem damit verbundenen Schadensausmaß.

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	2022-09-08T12:07:45+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: http://www.lebensministerium.at/amtssignatur	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-09-08T12:19:47+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	