11541/AB
vom 08.09.2022 zu 11854/J (XXVII. GP)

Bundeskanzleramt

bundeskanzleramt.gv.at

Karl Nehammer
Bundeskanzler

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2022-0.498.821

Wien, am 8. September 2022

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Ecker, MBA, Kolleginnen und Kollegen haben am 8. Juli 2022 unter der Nr. **11854/J** eine schriftliche parlamentarische Anfrage betreffend „mögliche Hackerangriffe auf Ihr Ministerium“ an mich gerichtet.

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

Zu Frage 1:

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. Das Bundeskanzleramt 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:

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 automatisiert abgewehrt.

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

- 2017 – DDoS Angriff auf das BKA mit temporärer Nichterreichbarkeit von Services und Webseiten.
- 2018 – Spear Phishing Attacke auf Bedienstete des Bundeskanzleramtes; technische Systeme haben die Zustellung der Mails verhindert.
- 2018 – DDoS Angriff auf das BKA mit kurzfristiger Nichterreichbarkeit von Webseiten.
- 2018 – Waterholing/ Fingerprinting Angriff auf Bedienstete des Bundeskanzleramtes, eine potentielle Infektion wurde von den technischen Systemen verhindert.
- 2019 – Waterholing/ Fingerprinting Angriff auf Bedienstete des Bundeskanzleramtes; Fortführung der Kampagne aus 2018; durch die im Rahmen der permanenten Anpassung an Vorfälle durchgeführten Härtung der Systeme konnte der zielgerichtete Angriffsvektor nicht wirksam werden.
- 2022 – Zwei DDoS Angriffe auf die Webseite des Bundeskanzleramtes; die automatische Mitigation verhinderte ein Wirksamwerden des Angriffs.

Zu den Fragen 3, 5 und 6:

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

IKT-Sicherheit (und damit auch Datensicherheit) wird im Bundeskanzleramt als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur und der dahinterliegenden

Prozesse 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.

Darüber hinaus muss von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus gemäß des Netz- und Informationssystemsicherheitsgesetz, BGBl. I Nr. 111/2018, oder aber auch der Auflistung einzelner im Einsatz befindlicher Produkte im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Zu Frage 4:

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 Bundeskanzleramt 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 SAP, betreibt die BRZ GmbH zentral ein eigenes Sicherheitssystem.

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

Zu Frage 7:

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 NIS Gesetz geregelt.

Zu Frage 8:

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

Das Bundeskanzleramt und die im Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK) vertretenen Ministerien nehmen an unterschiedlichen, sowohl international als auch national ausgerichteten Übungen statt. Darunter sind:

- Alle zwei Jahre richtet das Bundeskanzleramt zusammen mit der Agentur der Europäischen Union für Cybersicherheit (ENISA) die Übung „Cyber Europe“ aus.
- Alle zwei Jahre nimmt das Bundeskanzleramt an der vom Bundesministerium für Landesverteidigung ausgerichteten „ASDEM“ teil.
- Das Bundeskanzleramt nimmt an dem vom Kompetenzzentrum Sicheres Österreich (KSÖ) organisierten Planspielen zu Cybersicherheit statt.

Zu Frage 9:

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.

Das kontinuierliche Risikomanagement definiert die im Bundeskanzleramt kritischen Prozesse und Dienste. Für diese ist ein Betriebskontinuitätsmanagement eingerichtet. Darüber hinaus wurden Vorkehrungen getroffen, um sowohl technische als auch von Dritten verursachte Ausfälle möglichst zeitnah zu kompensieren.

Karl Nehammer

Unterzeichner	serialNumber=932783133,CN=Bundeskanzleramt,C=AT
Datum/Zeit	2022-09-08T16:40:15+02:00
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bundeskanzleramt.gv.at/verifizierung
Hinweis	Dieses Dokument wurde amtssigniert.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-09-08T16:43:55+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.	