18214/AB
vom 12.08.2024 zu 18802/J (XXVII. GP)

Bundeskanzleramt

bundeskanzleramt.gv.at

Karl Nehammer
Bundeskanzler

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2024-0.440.313

Wien, am 12. August 2024

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Ecker, MBA, Kolleginnen und Kollegen haben am 12. Juni 2024 unter der Nr. **18802/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 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 auf die IT-Systeme des Bundeskanzleramtes können nie ausgeschlossen werden. Das Bundeskanzleramt ist zur Abwehr dieser Gefahren 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 weitestgehend automatisiert abgewehrt.

In Einzelfällen kommt es außerdem zu darüber hinaus gehenden Angriffsversuchen. In den letzten Jahren waren dies insbesondere folgende gezielte Aktionen:

- Angriffe 2023:
  - Sieben DDoS Angriffe auf Services des Bundeskanzleramtes - die automatisierten Abwehrsysteme des Bundeskanzleramtes verhinderten ein Wirksamwerden der Angriffe.
  - Angriff auf die Systeme des Bundeskanzleramtes unter Ausnutzung einer Zero-Day-Lücke - das mehrstufige Sicherheitssystem sowie das manuelle Eingreifen durch die Sicherheitsexpertinnen und -experten verhinderten das Wirksamwerden des Angriffs bis zum Zeitpunkt der Verfügbarkeit eines Herstellerpatches.
- Angriffe 2024:
  - DDoS Angriff auf das Rechtsinformationssystem des Bundes (RIS) - das manuelle Eingreifen der Sicherheitsexpertinnen und -experten verhinderte das Wirksamwerden des Angriffs.
  - DDoS Angriff auf Services des Bundeskanzleramtes - die automatisierten Abwehrsysteme des Bundeskanzleramtes verhinderten ein Wirksamwerden des Angriffs.

Darüber hinaus verweise ich auf die Beantwortung der parlamentarischen Anfrage Nr. 11854/J vom 8. Juli 2022.

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 somit auch Datensicherheit) wird im Bundeskanzleramt als fortlaufender und umfassender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz unter Abstützung auf entsprechende Systeme 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 Stärkung 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 von 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. *Wenn ja, 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 IT-Personalmanagement und Haushaltsverrechnung betreibt die BRZ GmbH zentral ein eigenes Sicherheitssystem.

IKT-Sicherheitsbeauftragte und/oder Informationssicherheitsbeauftragte der Bundesministerien treffen einander unter der Schirmherrschaft des Bundeskanzleramtes auf regelmäßiger Basis und teilen Informationen und Best-Practices.

Darüber hinaus verweise ich auf die Beantwortung der parlamentarischen Anfragen Nr. 11856/J vom 8. Juli 2022 durch den Bundesminister für Inneres und Nr. 11854/J ebenfalls vom 8. Juli 2022.

Zu Frage 7:

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. Im Falle von Auswirkungen, die eine Gefahr außergewöhnlichen Ausmaßes für das Leben oder die Gesundheit der Bevölkerung oder eines großen Personenkreises, für die öffentliche Gesundheit, für die öffentliche Ordnung und Sicherheit im Inneren, für die nationale Sicherheit, für die Umwelt oder für das wirtschaftliche Wohl der Republik darstellen und deren Abwehr oder Bewältigung die unverzügliche Anordnung, Durchführung oder Koordination von Maßnahmen im Zuständigkeitsbereich des Bundes dringend erforderlich macht, sind die Krisenkoordinationsregelungen gem. B-KSG anzuwenden.

Zu Frage 8:

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 Bundeskanzleramt 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 Simulationen, Planspielen, Workshops und dergleichen durch.

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

- Alle zwei Jahre richtet das Bundeskanzleramt zusammen mit der Agentur der Europäischen Union für Cybersicherheit (ENISA) die Übung „Cyber Europe“ aus. Die diesjährige Cyber Europe fand am 18. und 19. Juni 2024 statt und hatte den Sektor Energie im Fokus.
- 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 teil.

Zu Frage 9:

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.

Karl Nehammer

REPUBLIK ÖSTERREICH BUNDESKANZLERAMT AMTSSIGNATUR	Unterzeichner	serialNumber=734173660,CN=Bundeskanzleramt,C=AT
	Datum/Zeit	2024-08-12T09:37:58+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.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-08-12T09:44:01+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	