**18203/AB**
**vom 12.08.2024 zu 18819/J (XXVII. GP)**

Bundesministerium
Soziales, Gesundheit, Pflege
und Konsumentenschutz

sozialministerium.at

**Johannes Rauch**
Bundesminister

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrates
Parlament
1017 Wien

Geschäftszahl: 2024-0.444.881

Wien, 24.7.2024

Sehr geehrter Herr Präsident!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 18819/J der Abgeordneten Ecker betreffend Mögliche Hackerangriffe auf Ihr Ministerium** wie folgt:

**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 Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK) können nie ausgeschlossen werden. Das BMSGPK 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.

**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. Überlastungsangriffe von kleinerem oder größerem Ausmaß sind im betrieblichen Alltag daher Gang und Gäbe. Diese werden durch die IKT-Sicherheitssysteme ebenso weitestgehend automatisiert abgewehrt.

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

- Angriffe bis 2022: siehe Anfragebeantwortung 11423/AB vom 07.09.2022
- Angriffe 2023:
    - Zwei DDoS Angriffe auf Services des BMSGPK; die automatisierten Abwehrsysteme verhinderten ein Wirksamwerden der Angriffe.
    - Angriff auf ein Shared Service des ICT Service Providers unter Ausnutzung einer Schwachstelle mit dem höchstmöglichen CVSS (Common Vulnerability Scoring System) Score von 10; das mehrstufige Sicherheitssystem sowie das manuelle Eingreifen durch die Sicherheitsexperten verhinderten das Wirksamwerden des Angriffs bis zum Zeitpunkt der Verfügbarkeit eines Herstellerpatches.
- Angriffe 2024:
    - Angriff auf die Sicherheitssysteme des BMSGPK unter Ausnutzung einer Zero-Day-Lücke; das mehrstufige Sicherheitssystem sowie das manuelle Eingreifen durch die Sicherheitsexperten verhinderten das Wirksamwerden des Angriffs bis zum Zeitpunkt der Verfügbarkeit eines Herstellerpatches.
    - Angriff auf ein IKT-System des BMSGPK durch automatisierte Anfragen; das mehrstufige Sicherheitssystem sowie das manuelle Eingreifen durch die Sicherheitsexperten verhinderten das Wirksamwerden des Angriffs.

**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?*

Das Thema Datensicherheit wird in meinem Ressort sowohl auf organisatorischer als auch technischer Ebene adressiert. Die gesetzliche Verpflichtung hierzu erwächst aus § 22 Netz- und Informationssystemsicherheitsgesetz (NISG), BGBl. I Nr. 111/2018.

IKT-Sicherheit (und damit auch Datensicherheit) wird im BMSGPK 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 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.

**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 BMSGPK 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 Officers (CISOs) bzw. IKT-Sicherheitsbeauftragten und Informationssicherheitsbeauftragten der Bundesministerien treffen einander unter Schirmherrschaft des Bundeskanzleramtes auf regelmäßiger Basis und teilen Informationen und Best-Practices. Zudem ermöglicht das NISG dem Bundesministerium für Inneres den Betrieb eines IOC-basierten Frühwarnsystems.

Darüber hinaus darf auf die Beantwortung der parlamentarischen Anfragen Nr. 11856/J vom 8. Juli 2022 durch den Bundesminister für Inneres sowie unsere Anfragebeantwortung 11423/AB vom 7. September 2022 verwiesen werden.

**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 B-KSG.

**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?*

Das BMSGPK verfügt über einen Notfallplan, der die einzuleitenden Maßnahmen und Zuständigkeiten bei auftretenden Vorfällen im Zusammenhang mit wesentlichen Cyberbedrohungen regelt.

Mein Ressort nimmt an unterschiedlichen, sowohl international als auch national ausgerichteten Übungen teil. Darunter sind:

- ENISA Übungen (ENISA (europa.eu))
- Cybersicherheitsübungen mit weiteren EU-Mitgliedsstaaten, welche aus Cybersicherheitsgruppen des Gesundheitssektors bestehen
- Nationale Gesundheitsarbeitsgruppen wie der Cybersicherheitsausschuss für eHealth, in dem Bund und Länder vertreten sind

**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.

Das kontinuierliche Risikomanagement definiert die in meinem Ressort kritischen Prozesse und Dienste. Darüber hinaus wurden Vorkehrungen getroffen, um sowohl technische als auch von Dritten verursachte Ausfälle möglichst zeitnah zu kompensieren.

Mit freundlichen Grüßen

Johannes Rauch

| | | |
|---|---|---|
| REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR SOZIALES, GESUNDHEIT, PFLEGE UND KONSUMENTENSCHUTZ @ AMTSSIGNATUR | Unterzeichner | Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz |
| | Datum/Zeit | 2024-08-12T08:00:48+02:00 |
| | Aussteller-Zertifikat | CN=a-sign-corporate-05,OU=a-sign-corporate-05,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT |
| | Serien-Nr. | 2098721075 |
| Hinweis | Dieses Dokument wurde amtssigniert. | |
| Prüfinformation | Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at<br>Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.sozialministerium.at/site/Ministerium/Willkommen_im_Ministerium/Amtssignatur/Amtssignatur | |

| | | |
|---|---|---|
| | **Unterzeichner** | Parlamentsdirektion |
| | **Datum/Zeit-UTC** | 2024-08-12T08:07:14+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 | |