11545/AB
vom 08.09.2022 zu 11852/J (XXVII. GP)

Bundesministerium
Arbeit und Wirtschaft

bmaw.gv.at

Univ.-Prof. Dr. Martin Kocher
Bundesminister

martin.kocher@bmaw.gv.at
+43 1 711 00-0
Stubenring 1, 1010 Wien

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2022-0.499.216

Ihr Zeichen: BKA - PDion (PDion)11852/J-NR/2022

Wien, am 08. September 2022

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Rosa Ecker und weitere haben am 08.07.2022 unter der **Nr. 11852/J** an mich, in meiner vorherigen Funktion als Bundesminister für Arbeit, eine schriftliche parlamentarische Anfrage betreffend **mögliche Hackerangriffe auf Ihr Ministerium** gerichtet.

Diese Anfrage beantworte ich für den Bereich Arbeit 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?*
    - *Wenn ja, wie sind Sie konkret auf so einen Zwischenfall vorbereitet?*

Es werden spezifische Sicherheitsvorkehrungen zum Schutz der IKT-Systeme gegen Angriffe im Sinne von § 118a StGB getroffen, bei denen es sich vorwiegend um Absicherungen technischer und organisatorischer Natur handelt. Um die Effektivität dieser Maßnahmen nicht zu schmälern, ist es jedoch leider nicht möglich, dazu weitere Details bekanntzugeben.

Zur Frage 2

- *Gab es in den letzten fünf Jahren sogenannte „Überlastungsangriffe“ oder andere, abgewehrte Angriffe?*
    - *Wenn ja, wann?*

- *Wenn ja, in welchem Umfang?*

Seit 2021 wurden keine Überlastungsangriffe mit relevanten Auswirkungen auf die Service-Verfügbarkeit des Ressorts in der Bundesrechenzentrum GmbH (BRZ) aufgezeichnet.

Es gibt Versuche, durch Überlastungsangriffe die Systeme des Ressorts für Bürgerinnen und Bürger sowie Unternehmen unerreichbar zu machen. Bisherige Angriffe waren nicht geschäftsbeeinträchtigend bzw. wurden stets erfolgreich abgewehrt. Zum Schutz der IKT-Systeme des Ressorts gegen derartige Angriffe werden spezifische Sicherheitsvorkehrungen getroffen.

Zur Frage 3

- *Wie wird seitens Ihres Ministeriums für die Datensicherheit gesorgt?*

Für die Datensicherung sorgen spezifische organisatorische und technische Sicherheitsvorkehrungen.

Zur Frage 4

- *Gibt es ein übergeordnetes Sicherheitssystem, das über alle Bundesministerien und die vorhandenen Daten wacht?*
  - *Wenn nein, ist zukünftig ein derartiges Sicherheitssystem geplant?*
  - *Wann soll dieses in Betrieb gehen?*

Aufgrund der Heterogenität der im Einsatz befindlichen IKT-Infrastrukturen in den Ressorts ist ein derart übergeordnetes Sicherheitssystem nicht sinnvoll. Prinzipiell fällt die Sicherung der IKT Systeme in die Verantwortung der zuständigen obersten Organe. Das NIS Gesetz ermöglicht dem Bundesministerium für Inneres jedoch den Betrieb eines IOC basierten Frühwarnsystems. Für Details zur Umsetzung darf ich auf die Beantwortung der Parlamentarischen Anfrage Nr. 11856/J vom 8. Juli 2022 durch den Bundesminister für Inneres verweisen.

Zu den Fragen 5 und 6

- *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?*

In meinem Ressort gibt es mehrere technische Sicherheitssysteme, welche laufend nach den Geboten der Sparsamkeit, Zweckmäßigkeit, Wirtschaftlichkeit und dem Stand der Technik angepasst und adaptiert werden.

Es wird ein standardisierter Client mit entsprechenden Hardening-Maßnahmen eingesetzt, individuelle Maßnahmen (wie Passwort-Richtlinie) werden nach Bedarf implementiert. Das beauftragte Rechenzentrum ist im BRZ ISO 27001 zertifiziert.

Die BRZ setzt jene technischen und organisatorischen Maßnahmen, die vom Ressort angefordert werden. Dabei besitzt die BRZ grundsätzlich ein ebenso nach ISO 27001 zertifiziertes Informationssicherheitsmanagement, welches sämtliche IT-Systeme umfasst.

Zur Frage 7

- *Welches Gremium ist vorgesehen, wenn so wie im Fall des Bundeslands Kärnten ein Angriff erfolgreich ist und Maßnahmen ergriffen werden müssen?*

Um sich adäquat gegen Angriffe schützen zu können, wurde ein ressorteigenes Krisenteam eingerichtet.
Parallel sorgt eine eigene Organisationseinheit für die Planung, Überwachung, Weiterentwicklung und Bereitstellung von Informationstechnologie in den Arbeitsinspektoraten. Das Sicherheitsmanagement-Team für die Arbeitsinspektorate ist ein internes Gremium aus Führungskräften sowie Expertinnen und Experten mit einer beratenden Tätigkeit in allen Belangen der IT-Sicherheit.

Zur Frage 8

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

Derartige Szenarien werden in unterschiedlichen Konstellationen und mit fiktiven Ausgangssituationen (auch interministeriell) regelmäßig geübt und mit externen Expertinnen und Experten durchgesprochen. Teilbereiche werden auch laufend in der Praxis getestet. Danach werden die Vorkehrungen entsprechend angepasst.

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 erforderlichen Prozedere sind im Notfallplan definiert. Die Durchlaufzeit eines Wiederaufbaus hängt vom betroffenen Service sowie vom Umfang und den Auswirkungen des Angriffs ab und kann Zeitfenster von ein paar Stunden bis hin zu mehreren Tagen betragen.

Univ.-Prof. Dr. Martin Kocher

Unterzeichner	Bundesministerium für Arbeit und Wirtschaft
Datum/Zeit	2022-09-08T15:38:02+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.	1056650987
Hinweis	Dieses Dokument wurde amtssigniert.
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-09-09T09:14:10+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.	