11861/AB
vom 14.11.2022 zu 12153/J (XXVII. GP)

Bundesministerium
Arbeit und Wirtschaft

bmaw.gv.at

Univ.-Prof. Dr. Martin Kocher
Bundesminister

Stubenring 1, 1010 Wien

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2022-0.660.627

Ihr Zeichen: BKA - PDion (PDion)12153/J-NR/2022

Wien, am 14. November 2022

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Katharina Kucharowits und weitere haben am 14.09.2022 unter der **Nr. 12153/J** an mich eine schriftliche parlamentarische Anfrage betreffend **Vorbereitung auf Cyberangriffe innerhalb der österreichischen Bundesverwaltung** gerichtet.

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

Zur Frage 1

- *Gab es in Ihrem Ressort bereits Cyberangriffe?*
    - *Falls ja, bitte um detaillierte Schilderung des Angriffs/der Angriffe, welche Schäden daraus resultierten und welche Gegenmaßnahmen ergriffen wurden?*

Das Bundesministerium für Arbeit und Wirtschaft (BMAW) sieht sich, wie auch andere Ministerien, Unternehmen und Bildungseinrichtungen, kontinuierlich unterschiedlichen Angriffsversuchen im Cyberraum ausgesetzt. Bisher konnten derartige Angriffsversuche abgewehrt und Schäden oder Ausfälle hintangehalten werden.

Die IKT-Sicherheit wird im Bund als fortlaufender Prozess verstanden. Dementsprechend werden, unterstützt durch das Governmental Computer Emergency Response Team

(GovCERT) und den Inneren Kreis der operativen Koordinierungsstruktur (IKDOK), kontinuierlich Anpassungen der IKT-Sicherheitsstruktur vorgenommen, um auch auf sich ändernde Bedrohungsszenarien reagieren zu können.

Zu den Fragen 2, 8 und 9

- *Welche Rolle und welche konkreten Aufgaben fallen Ihrem Ressort in der gesamtstaatlichen Bekämpfung von Cyberkriminalität zu?*
- *Der Rechnungshof sah zudem die Etablierung eines permanent verfügbaren Cyber-Einsatzteam ("Rapid Response Team") sowie die Schaffung eines ebenso permanenten Cyber-lagezentrums zur Bearbeitung von Notfällen als essentiell. Wurden dieses Einsatzteam und das Lagezentrum zum Zeitpunkt der Beantwortung dieser Anfrage bereits geschaffen?*
    - *Falls ja, in welchem Ressort sind diese Strukturen angesiedelt und der Zuständigkeit welcher/welchen Bundesministerin/Bundesministers unterliegen diese?*
- *Zudem forderte der Rechnungshof ein regelmäßig zu erstellendes Cyber-Lagebild, um laufende Bedrohungen und potentielle Gefahrenquellen schneller und effektiver zu identifizieren. Wird ein solches Cyberlagebild in Ihrem Ressort zum Zeitpunkt der Beantwortung dieser Anfrage bereits regelmäßig erstellt?*
    - *Falls ja, seit wann wird ein solches Lagebild in Ihrem Ressort erstellt und in welchen Abständen findet das statt?*
    - *Falls nein, warum wird bisher kein Cyber-Lagebild in Ihrem Ressort erstellt und ab wann planen Sie, ein solches regelmäßig zu erstellen?*

Diese Fragen betreffen keinen Gegenstand der Vollziehung des BMAW.

Zur Frage 3

- *Ergreift Ihr Ressort aktiv konkrete Maßnahmen, um sich präventiv gegen Cyberattacken und Cyberkriminalität angemessen zu schützen?*
    - *Falls ja, welche Maßnahmen sind das im Detail?*
    - *Falls ja, wird in der Vorbereitung auf einen potenziellen Cyberangriff auch die Expertise externer Expert* innen, etwas Personen auf Wissenschaft oder Zivilgesellschaft, hinzugezogen?*
    - *Falls nein, warum gibt es keine Pläne, sich für den Ernstfall eines potenziellen Cyberangriffs zu schützen?*

Die IKT-Sicherheitsmaßnahmen des BMAW unterteilen sich in vier Kategorien:

- Einsatz einer Vielzahl von technischen State-of-the-Art-Sicherheitslösungen, Optimierung entsprechend dem Plan/Do/Check/Act-Zyklus, laufende Evaluierung etwaiger offener Schwachstellen;
- laufende Evaluierung und Weiterentwicklung organisatorischer Richtlinien in Bezug auf IKT- & Informationssicherheit;
- laufende Information der Mitarbeiterinnen und Mitarbeiter über neue Angriffs-Methoden, Schärfung des Bewusstseins für IKT- & Informationssicherheit durch weitere Informationen wie etwa Tipps & Tricks-Artikel, ein Awareness-Quiz etc.;
- Zyklische Prüfung des Härtegrades der IKT-Sicherheit in einem IT-Security-Audit durch unabhängige externe Spezialisten und Einarbeitung der Findings in die IKT-Sicherheitsmaßnahmen.

Zur Vorbereitung auf potenzielle Cyberangriffe wird auch die Expertise externer Expertinnen und Experten herangezogen.

Darüber hinaus muss von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. zum Erhalt eines hohen IKT-Sicherheitsniveaus gemäß Netz- und Informationssystemsicherheitsgesetz und der Auflistung einzelner im Einsatz befindlicher Cybersicherheitsprodukte im Hinblick auf die Sicherung der Effektivität dieser Schutzmaßnahmen Abstand genommen werden.

Zur Frage 4

- *Durch die unterschiedlichen Zuständigkeitsbereiche aller Ressorts der Bundesregierung ergeben sich auch unterschiedliche Risiken in Bezug auf Cyberangriffe, beispielsweise wird es im Bundesministerium für europäische und internationale Angelegenheiten aller Wahrscheinlichkeit nach andere Herausforderungen und Risiken in Bezug auf Cyberkriminalität geben als beispielweise im Bundesministerium für Justiz.*
    - *Gab es eine ressortspezifische Risikoanalyse in Ihrem Ressort?*
        - *Falls nein, warum nicht?*
    - *Welche konkreten Maßnahmen setzen Sie, um den spezifischen Risiken Ihres Ressorts gerecht zu werden?*

Die IKT-Sicherheitsmaßnahmen wurden auf die Services des Ressorts angepasst.

Zur Frage 5

- *Gibt es eine Person oder einen Personenkreis in Ihrem Ressort, die dezidiert als "Cybersichterheitsbeauftrage(r)" fungiert/fungieren?*
    - *Falls ja, wie viele Personen sind zum Zeitpunkt der Beantwortung dieser Anfrage im Bereich Cybersecurity in Ihrem Ressort beschäftigt?*
    - *Falls ja, über welche Expertise verfügt/verfügen diese Person(en)?*
    - *Falls nein, warum gibt es keine(n) "Cybersicherheitsbeauftrage(n)" in Ihrem Ressort?*

Im Verwaltungsbereich Arbeit nimmt der Chief Information Security Officer (CISO) diese Rolle wahr und trägt als Durchführungsverantwortlicher des Informationssicherheitsmanagement-Prozesses die Gesamtverantwortung für das Qualitätsmanagement der IT-Sicherheit. Im Bereich der Cybersecurity ist ein VBÄ beschäftigt.

Im Verwaltungsbereich Wirtschaft sind in Summe drei VBÄ als Informationssicherheitsbeauftragte und IT-Sicherheitsbeauftragte beschäftigt; diese Personen verfügen über mehrjährige Erfahrung im Bereich der IKT- & Informationssicherheit.

Zur Frage 6

- *Bietet Ihr Ressort spezielle Trainings, Webinare, Kurse etc. an, um alle Mitarbeiter*innen im Umgang mit potenziellen Cyberangriffen und der daraus resultierenden Gefahrenlage zu sensibilisieren?*

Die Bediensteten im BMAW werden sensibilisiert, um Gefahren, die zu Cyberangriffen führen können, und Tricks von Cyberkriminellen frühzeitig zu erkennen. Seit mehreren Jahren werden dazu Seminare zu Cyber-Security, IT-Security und IT-Security-Rechtsgrundlagen im internen Bildungsprogramm angeboten. Darüber hinaus wird in bestimmten Modulen bei IT-Schulungen auf die internen Sicherheitsaspekte und Richtlinien eingegangen.

In Entsprechung der Ausführungen im in der Anfrage angeführten Rechnungshof-Bericht wird derzeit an der Ausrollung eines IT- Security-Awareness Quiz gearbeitet, das allen Bediensteten zur Verfügung gestellt werden soll. Zukünftig ist weiters geplant, eine verpflichtende IT-Security Awareness Schulung in die Grundausbildung aufzunehmen.

Zur Frage 7

- *Der Rechnungshofbericht bemängelt unter anderem, dass Krisen-, Kontinuitäts- und Einsatzpläne in Bezug auf Cybersicherheit gänzlich fehlen. Zum Zeitpunkt der*

Beantwortung dieser Anfrage, wurden diese von Ihrem Ressort mittlerweile erstellt?

- *Falls ja, wurden zur Erstellung dieser Pläne auch externe Expert*innen hinzugezogen?*
- *Falls nein, wann ist mit der Fertigstellung dieser Pläne in Ihrem Ressort zu rechnen?*

Die Cybersicherheitsmaßnahmen des BMAW sind nicht Gegenstand des besagten Berichts des Rechnungshofes. Ungeachtet dessen behandelt das Krisenhandbuch des BMAW aber auch konkrete Pläne zum Lagebild "Cyberangriff". Bei der Erstellung dieses Krisenhandbuchs wurde auch externe Expertise herangezogen.

Univ.-Prof. Dr. Martin Kocher

Elektronisch gefertigt

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR ARBEIT UND WIRTSCHAFT @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Arbeit und Wirtschaft
	Datum/Zeit	2022-11-14T07:42:58+01:00
	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	2022-11-14T07:49:22+01:00
	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.	