3059/AB
vom 08.10.2020 zu 3255/J (XXVII. GP)

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

bmk.gv.at

Leonore Gewessler, BA
Bundesministerin

leonore.gewessler@bmk.gv.at
+43 1 711 62-658000
Radetzkystraße 2, 1030 Wien
Österreich

An den
Präsident des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 W i e n

Geschäftszahl: 2020-0.562.209

. Oktober 2020

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 02. September 2020 unter der **Nr. 3255/J** an mich eine schriftliche parlamentarische Anfrage betreffend Konsequenzen aus Cyberattacke auf das BMEIA im Jänner/Februar 2020 gerichtet.

Diese Anfrage beantworte ich wie folgt:

Zu Frage 1:

- *Welche Lehren und Konsequenzen zogen Sie für Ihr Ressort aus der Attacke auf das BMEIA?*

Basierend auf den Erkenntnissen und der Risikoeinschätzung des interministeriellen Krisenstabs erfolgten direkte und konkrete Risikominimierungsmaßnahmen. Es wurden die jeweiligen Systeme gehärtet bzw. die Abwehrmaßnahmen verbessert.
Die Anpassungen der ressortinternen Prozesse erfolgt risikobasiert und permanent. Die IKT Sicherheit des BMK wird unter Einbindung von Expert_innen ständig auf die aktuellen technologischen Anforderungen hin angepasst.

Zu Frage 2:

- *Wurden in Ihrem Ressort seit Bekanntwerden des Angriffs Fehler und Sicherheitslücken entdeckt?*
    a. *Wenn ja, welche?*
    b. *Wenn ja, welche konkreten Maßnahmen wurden von Ihnen zur Analyse und Bekämpfung gesetzt?*

Im BMK wurden seit dem Vorfall keine Angriffe, welche über Standard- und Routinevorfälle hinausgehen, festgestellt.

Zu Fragen 3, 4 und 5:

- *Welche konkreten Maßnahmen wurden seit Bekanntwerden des Angriffes in Ihrem Ressort allgemein a.) geplant und b.) umgesetzt, um die Verteidigungsfähigkeit und Sicherheit der Republik im Cyberbereich zu verbessern?*
- *Welche (Zeit-)Aufwendungen sind Ihrem Ressort durch die Analyse und Verbesserung der Sicherheit bisher entstanden? (Bitte um detaillierte Erläuterung und Unterscheidung der Maßnahmen **vo**r sowie **nach** Bekanntwerden des Angriffs.)*
- *Welche bezifferbaren Kosten sind Ihrem Ressort durch die Analyse und Verbesserung der Sicherheit bisher entstanden?*

Basierend auf den Erkenntnissen des Vorfalles wurden die jeweiligen Systeme gehärtet bzw. die (automatisierten) Abwehrmaßnahmen verbessert.
Der Innere Kreis der operativen Koordinierungsstruktur bzw. die Operative Koordinierungsstruktur (IKDOK/OPKOORD) erstellt regelmäßig sowohl eine Risikoeinschätzung als auch Empfehlungen zum Schutz der eigenen Systeme. Die Evaluierung und Umsetzung relevanter Empfehlungen erfolgt als Routinemaßnahme durch die verantwortlichen Technikerinnen und Techniker im BMK.
Darüber hinaus erfolgt eine kontinuierliche Marktbeobachtung, um auf neue Trends im Bereich der IKT-Sicherheit reagieren zu können.
Weiters werden basierend auf den aktuellen Bedrohungslagen bewusstseinsbildende Maßnahmen (Awareness) durchgeführt.
Die während der Vorfallsbehandlung im BMEIA entwickelten Empfehlungen und Maßnahmen wurden zeitnah durch die verantwortlichen Technikerinnen und Techniker im BMK umgesetzt. Diese Maßnahmen reichten beginnend von konkreten Scripts zum Scannen nach im BMEIA festgestellter Malware über das Einspielen von Indicators of Compromise (IOCs) in der eigenen Sicherheitsarchitektur bis hin zu Blacklists (Verweigerung zur Ausführung) von bestimmten Applikationen.
Darüber hinaus wurden im BMK folgende Maßnahmen getroffen um Systeme zu härten:

- KI-basierter zentraler Schutz auf Basis der externen Namesauflösung
- Beauftragung der Durchführung eines externen Schwachstellenscans
- Einsatz eines Schwachstellen- und Monitoringsystems

Genaue Zeitaufwendungen und Kosten sind nicht bezifferbar, weil die Umsetzung von IT-Sicherheitsmaßnahmen Teil der routinemäßigen Aufgabenabwicklung ist und die diesbezüglichen Aufwendungen im Detail nicht explizit erfasst werden.

Zu Frage 6:

- *Welche Stellen und wie viele Personen Ihres Ressorts sind bzw. waren in die durch die Analyse und Verbesserung der Sicherheit in welcher Weise und wann jeweils eingebunden?*

Die mit Cybersicherheitsagenden betrauten Stellen im BMK sind primär die Präsidialabteilungen I/Pr.3 - Recht und Koordination und I/Pr.4 - Informations- und Kommunikationstechnik. Die Analysen und Verbesserungen der Sicherheit (Adaptierung bzw. Optimierung bestehender Systeme) erfolgen durch das eingeteilte Personal im Rahmen der routinemäßigen Aufgabenwahrnehmung.

Zu Frage 7:

- *Welche externen Experten bzw. Unternehmen wurden für die Analyse und Verbesserung der Sicherheit in Ihrem Ressort in welcher Weise und wann jeweils zugezogen?*

Der Bund verfügt mit dem GovCERT und dem IKDOK über im NISG festgeschriebene Expert_innengruppen, auf welche sowohl in der routinemäßigen Risikoanalyse als auch im konkreten Anlassfall zugegriffen werden kann. Darüber hinaus können bei konkreten Vorfällen und Bedarf externe Expertinnen und Experten sowie Unternehmen beauftragt werden.
Die konkreten Maßnahmen im BMK sind der Beantwortung zu Punkt 4 zu entnehmen. Die Ergebnisse fanden Niederschlag in der Optimierung der eigenen Schutzmechanismen.

Zu Frage 8:

- *Verfügt Ihr Ressort über einen Rahmenvertrag mit externen Expert_innen/Unternehmen für die rasche Bewältigung von IT-Vorfällen dieser Art?*
  - *i. Wenn ja, seit wann mit welchen Expert_innen/Unternehmen?*
  - *ii. Wenn nein, weshalb nicht?*

Der Bund verfügt mit dem GovCERT und dem IKDOK über Expert_innengruppen, auf welche sowohl in der routinemäßigen Risikoanalyse, als auch im konkreten Anlassfall zugegriffen werden kann. Die Shared Services des Bundes in der BRZ (z.B. ELAK) unterliegen dem dort angesiedelten unternehmenseigenen CERT. Außerdem stehen im Bedarfsfall weitere externe Expert_innen für technische Unterstützungen zur Verfügung.
Das BMK verfügt über keinen expliziten eigenen Rahmenvertrag für die Bewältigung von IT-Sicherheitsvorfällen, im Bedarfsfall wird auf die o.a. Expert_innen zurückgegriffen.

Leonore Gewessler, BA

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR KLIMASCHUTZ, UMWELT, ENERGIE, MOBILITÄT, INNOVATION UND TECHNOLOGIE
AMTSSIGNATUR

Hinweis	Dieses Dokument wurde amtssigniert.
Datum	2020-10-08T13:19:47+02:00
Seriennummer	1871969199
Aussteller-Zertifikat	CN=a-sign-corporate-05,OU=a-sign-corporate-05,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at/

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-10-08T13:54:30+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.	