**3235/AB**
**vom 30.10.2020 zu 3244/J (XXVII. GP)**

Bundesministerium
Kunst, Kultur,
öffentlicher Dienst und Sport

bmkoes.gv.at

**Mag. Werner Kogler**
Vizekanzler
Bundesminister für Kunst, Kultur,
öffentlichen Dienst und Sport

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.571.181

Wien, am 30. Oktober 2020

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 2. September unter der Nr. **3244/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Konsequenzen aus Cyberattacke auf das BMEIA im Jänner/Februar 2020“ gerichtet.

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

**Zu Frage 1:**

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

Im Zuge der Nachbereitung des BMEIA-Cybervorfalles wurde unter Koordination des BKA ein strategisches Lessons Identified Dokument erstellt. Darin wurden kurz-, mittel- und langfristige Ziele zur Erhöhung der Widerstandsfähigkeit im Fall von Cybersicherheitsbedrohungen erarbeitet. Gleichzeitig haben sich die Prozesse gemäß Netz- und Informationssystemsicherheitsgesetz (NISG) und Österreichische Strategie für Cybersicherheit (ÖSCS) 2013 in großen Teilen als zielgerichtet und effizient erwiesen. Grundsätzlich kann festgestellt werden, dass die Strukturen und Abläufe sowie die Zusammenarbeit der unterschiedlichen Stakeholder sehr gut funktionieren.

Wie schon in der Beantwortung der parlamentarischen Anfrage Nr. 1308/J vom 25. März 2020 ausgeführt, erfolgten basierend auf den Erkenntnissen und der Risikoeinschätzung des interministeriellen Krisenstabs direkte und konkrete Risikominimierungsmaßnahmen.

**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?*

Die IKT-Sicherheit im Bund wird als fortlaufender Prozess verstanden. Dementsprechend werden, unterstützt durch das GovCERT und den IKDOK (Inneren Kreis der operativen Koordinierungsstruktur), kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur 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 bewusstseinsbildende Maßnahmen (Awareness) durchgeführt.

**Zu Frage 3:**

- *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?*

Es werden spezifische Sicherheitsvorkehrungen zum Schutz der IKT-Systeme des Ressorts gegen Angriffe im Sinne des § 118a StGB eingesetzt. Ich bitte um Verständnis, dass es gerade im Hinblick auf die Effektivität dieser Maßnahmen nicht möglich ist, diese im Detail darzustellen.

**Zu Frage 4:**

- *Welche (Zeit-)Aufwendungen sind Ihrem Ressort durch die Analyse und Verbesserung der Sicherheit bisher entstanden? (Bitte um detaillierte Erläuterung und Unterscheidung der Maßnahmen vor sowie nach Bekanntwerden des Angriffs.)*

Im Zuge der Vorfallsbehandlung im BMEIA durch den Einsatzstab wurden sowohl eine laufende Risikoeinschätzung als auch Empfehlungen für konkrete Absicherungen der eigenen Netze erstellt und kommuniziert. Diese Maßnahmen reichten 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. Auch hier darf aber um Verständnis gebeten werden, dass es aus Sicherheitsgründen und im Hinblick auf die Effektivität dieser Maßnahmen nicht möglich ist, diese im Detail bekannt zu geben.

**Zu Frage 5:**

- *Welche bezifferbaren Kosten sind Ihrem Ressort durch die Analyse und Verbesserung der Sicherheit bisher entstanden?*

Es darf auf die Beantwortung der Frage 4 verwiesen 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?*

Zu den mit Cybersicherheitsagenden betrauten Stellen sowie der Anzahl der dort eingeteilten Personen darf auf die Geschäftseinteilung des BMKÖS verwiesen werden: https://www.bmkoes.gv.at/dam/jcr:19b58635-473d-47b5-a6ea-69d81a79c984/prov.%20Gesch%C3%A4ftseinteilung%20zum%201.8.2020.pdf

Die Analysen und Verbesserungen der Sicherheit (Adaptierung bzw. Optimierung bestehender Systeme) erfolgen durch das zuständige Personal im Rahmen der routinemäßigen Aufgabenwahrnehmung.

**Zu den Fragen 7 und 8:**

- *Welche externen Experten bzw. Unternehmen wurden für die Analyse und Verbesserung der Sicherheit in Ihrem Ressort in welcher Weise und wann jeweils zugezogen?*
- *Verfügt Ihr Ressort über einen Rahmenvertrag mit externen ExpertInnen/Unternehmen für die rasche Bewältigung von IT-Vorfällen dieser Art?*
    - *i. Wenn ja, seit wann mit welchen ExpertInnen/Unternehmen?*
    - *ii. Wenn nein, weshalb nicht?*

Der Bund verfügt mit dem GovCERT und dem IKDOK über im NISG festgeschriebene ExpertInnengruppen, 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 Shared Services des Bundes im BRZ (z. B. ELAK) unterliegen dem dort angesiedelten unternehmenseigenen CERT.

Mag. Werner Kogler

| | | |
|---|---|---|
| REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR KUNST, KULTUR, ÖFFENTLICHEN DIENST UND SPORT @ AMTSSIGNATUR | Unterzeichner | Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport |
| | Datum/Zeit | 2020-10-30T10:48:12+01:00 |
| | 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. | 2099471880 |
| | 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** | 2020-10-30T10:49:26+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. | |