Bundesministerium
Justiz

bmj.gv.at

Dr.in Alma Zadić, LL.M.
Bundesministerin für Justiz

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2020-0.565.180

Ihr Zeichen: BKA - PDion (PDion)3248/J-NR/2020

Wien, am 2. November 2020

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 02. September 2020 unter der Nr. **3248/J-NR/2020** 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 den Fragen 1 und 3:

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

Im Zuge der Nachbereitung des in der Anfrage relevierten Vorfalles wurde unter Koordination des Bundeskanzleramts (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. Die im Zuge der Erstellung des „Lessons Identified“-Dokumentes festgestellten zweckmäßigen Verbesserungen werden im Wege der Novellierung des NISG und bei der Überarbeitung der ÖSCS adressiert werden. Grundsätzlich kann festgestellt werden, dass die Strukturen und Abläufe sowie die Zusammenarbeit der unterschiedlichen Stakeholder sehr gut funktioniert.

Die konkrete Umsetzung der Empfehlungen obliegt jedem Ministerium selbst, wobei das BKA im Zuge seiner Rollenwahrnehmung als strategisches Koordinationselement die Etablierung von leitenden Informationssicherheitsbeauftragten (CISOs) vorantreibt.

Auf die angenommenen Anträge von NEOS und ÖVP/Grüne zur Cybersicherheit in der NSR-Sitzung vom 28. Februar 2020 sowie auf das Regierungsprogramm 2020 – 2024 der österreichischen Bundesregierung darf hingewiesen werden.

Basierend auf den Erkenntnissen und der Risikoeinschätzung des interministeriellen Krisenstabs erfolgten direkte und konkrete Risikominimierungsmaßnahmen. Gestützt auf die Erkenntnisse aus dem Vorfall wurden auch die jeweiligen Systeme gehärtet bzw. die (automatisierten) Abwehrmaßnahmen verbessert.

Der Innere Kreis der operativen Koordinierungsstruktur bzw. die Operative Koordinierungsstruktur (IKDOK/OPKOORD) erstellt regelmäßig basierend auf Meldungen gemäß den NISG-eigenen Systembeobachtungen und international zur Verfügung gestellten Daten sowohl eine Risikoeinschätzung als auch Empfehlungen zum Schutz der eigenen Systeme. Die Umsetzung der Empfehlungen erfolgt als Routinemaßnahme in enger Abstimmung mit dem Bundesrechenzentrum. Die Evaluierung und Anpassungen der ressortinternen Maßnahmen erfolgt laufend in enger Abstimmung mit dem Bundesrechenzentrum.

Zur 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.

Im Bundesministerium für Justiz (BMJ) wurden seit dem Vorfall keine Angriffe, welche über Standard- und Routinevorfälle hinausgehen, festgestellt.

Zu den Fragen 4 und 5:

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

Im Zuge der Vorfallsbehandlung im Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) wurde durch den Einsatzstab sowohl eine laufende Risikoeinschätzung als auch Empfehlungen für konkrete Absicherungen der eigenen Netze erstellt und kommuniziert. 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.

Alle diese Maßnahmen wurden zeitnah in enger Abstimmung mit dem Bundesrechenzentrum umgesetzt. Darüber hinaus hat das BMJ das Bundesrechenzentrum mit dem laufenden Betrieb sowie der Weiterentwicklung der IT-Sicherheitskomponenten beauftragt. Im Rahmen dieser Tätigkeit findet eine laufende Evaluierung und Verbesserung der eingesetzten Systeme statt.

Zur Frage 6:

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

Die mit Cybersicherheitsagenden betrauten Stellen sowie die Anzahl der dort eingeteilten Personen sind den jeweiligen Geschäftseinteilungen zu entnehmen. Die Analysen und Verbesserungen der Sicherheit (Adaptierung bzw. Optimierung bestehender Systeme)

erfolgen durch das eingeteilte Personal im Rahmen der routinemäßigen Aufgabenwahrnehmung.

Zu den Fragen 7 und 8:

- *7. Welche externen Experten bzw. Unternehmen wurden für die Analyse und Verbesserung der Sicherheit in Ihrem Ressort in welcher Weise und wann jeweils zugezogen?*
- *8. Verfügt Ihr Ressort über einen Rahmenvertrag mit externen Exptert_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 im NISG festgeschriebene Expertengruppen, 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. Das Bundesrechenzentrum ist der zentrale IKT-Dienstleister der österreichischen Justiz und nimmt sohin auch Analysen zur Identifikation von Verbesserungen im Bereich der IT-Sicherheit vor.

Darüber hinaus können bei konkreten Vorfällen und Bedarf externe Expertinnen und Experten sowie Unternehmen beauftragt werden.

Dr.in Alma Zadić, LL.M.

REPUBLIK ÖSTERREICH BMJ SIGNATUR	**Datum/Zeit**	2020-11-02T15:45:50+01:00
	Hinweis	Dieses Dokument wurde elektronisch signiert. Auch ein Ausdruck dieses Dokuments hat die Beweiskraft einer öffentlichen Urkunde.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: www.justiz.gv.at/amtssignatur

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-11-02T16:28:11+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.	