3273/AB
vom 02.11.2020 zu 3250/J (XXVII. GP)

bmi.gv.at

Bundesministerium
Inneres

Karl Nehammer, MSc
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.572.668

Wien, am 2. November 2020

Sehr geehrter Herr Präsident!

Der Abgeordnete zum Nationalrat Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 2. September 2020 unter der Nr. **3250/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 den Fragen 1 und 3:

- *Welche Lehren und Konsequenzen zogen Sie für Ihr Ressort aus der Attacke auf das BMEIA?*
- *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 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 NISG und Österreichische Strategie für Cybersicherheit (ÖSCS) 2013 in großen Teilen als zielgerichtet und effizient erwiesen. Die im Zuge des Lessons Identified festgestellten

zweckmäßigen Verbesserungen werden im Wege der Novellierung des NISG als auch 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.

Weiters wird auf die angenommen Anträge NEOS und ÖVP/Grüne zur Cybersicherheit in der NSR-Sitzung vom 28. Februar 2020 sowie auf das Regierungsprogramm 2020 – 2024 der österreichischen Bundesregierung hingewiesen.

Wie schon in den Beantwortungen der parlamentarischen Anfragen 647/J und 1299/J aus dem laufenden Jahr mitgeteilt erfolgten basierend auf den Erkenntnissen und der Risikoeinschätzung des interministeriellen Krisenstabs direkte und konkrete Risikominimierungsmaßnahmen. Basierend auf den Erkenntnissen des Vorfalles 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 gem. dem NISG eigenen Systembeobachtungen und international zur Verfügung gestellten Daten sowohl eine Risikoeinschätzung als auch Empfehlungen zum Schutz der eigenen Systeme.

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 eingesetzt?*

Nein es wurden seit Bekanntwerden des Angriffs keine Fehler und Sicherheitslücken entdeckt.

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 den Fragen 4 und 5:

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

Wie zu den parlamentarischen Anfragen 1299/J und 1314/J aus dem laufenden Jahr ausgeführt wurden im Zuge der Vorfallsbehandlung im BMEIA 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.

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.

Zur 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 Expertengruppen, 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.

Zur Frage 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 von allen Ressorts zugegriffen werden kann. Die Shared Services des Bundes in der BRZ (z.B. ELAK) unterliegen dem dort angesiedelten unternehmenseigenen CERT.

Karl Nehammer, MSc

	Datum/Zeit	2020-11-02T15:39:22+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.	148769640
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-11-02T15:43:10+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.	