3228/AB
vom 30.10.2020 zu 3251/J (XXVII. GP)

Bundesministerium
Soziales, Gesundheit, Pflege
und Konsumentenschutz

sozialministerium.at

Rudolf Anschober
Bundesminister

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrates
Parlament
1017 Wien

Geschäftszahl: 2020-0.644.888

Wien, 19.10.2020

Sehr geehrter Herr Präsident!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 3251/J des Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen, betreffend Konsequenzen aus Cyberattacke auf das BMEIA im Jänner/Februar 2020** wie folgt:

Frage 1: *Welche Lehren und Konsequenzen zogen sie für Ihr Ressort aus der Attacke auf das BMEIA?*

Grundsätzlich kann festgestellt werden, dass die Strukturen und Abläufe sowie die Zusammenarbeit der unterschiedlichen Stakeholder sehr gut funktioniert haben. 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. Der Cyberangriff auf das BMEIA hat die Notwendigkeit bestätigt, der IKT-Sicherheit in meinem Ressort weiterhin einen hohen Stellenwert einzuräumen und die diesbezüglichen Erfordernisse in allen Bereichen der Informations- und Kommunikationstechnologie zu berücksichtigen.

Auf die angenommenen Anträge von NEOS und ÖVP/Grüne zur Cybersicherheit in der Sitzung des Nationalen Sicherheitsrates vom 28. Februar 2020 sowie auf das Regierungsprogramm 2020 – 2024 der österreichischen Bundesregierung wird hingewiesen.

Wie schon in der Beantwortung der parlamentarischen Anfrage Nr. 1305/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.

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 Cybersicherheits-bedrohungen erarbeitet.
Gleichzeitig haben sich die Prozesse gemäß dem Netz- und Informationssystemsicherheits-gesetz (NISG) und der Österreichischen Strategie für Cybersicherheit (ÖSCS) 2013 in großen Teilen als zielgerichtet und effizient erwiesen. Die im Zuge des „Lessons- Identified-Dokuments“ festgestellten zweckmäßigen Verbesserungen werden im Wege der Novellierung des NISG als auch der Überarbeitung der ÖSCS adressiert werden.

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.

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 Österreich im Cyberbereich zu verbessern?*

Wie schon in der Beantwortung der parlamentarischen Anfrage Nr. 1305/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.

Die Empfehlungen wurden zeitnah durch die verantwortlichen Technikerinnen und Techniker des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz umgesetzt und als Routinemaßnahmen weitergeführt. Darüber hinaus erfolgt eine kontinuierliche Marktbeobachtung, um auf neue Trends im Bereich der IKT-Sicherheit reagieren zu können.

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.)*

Wie zur parlamentarischen Anfrage Nr. 1305/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.

Alle Maßnahmen wurden zeitnah durch die verantwortlichen Technikerinnen und Techniker des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz umgesetzt und als Routinemaßnahmen weitergeführt.
Darüber hinaus erfolgte die Beauftragung und Durchführung eines externen Schwachstellenscans und eines technischen Audits.

Frage 5: *Welche bezifferbaren Kosten sind Ihrem Ressort durch die Analyse und Verbesserung der Sicherheit bisher entstanden?*

Das Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz hat neben den in der Beantwortung der Frage 4 angeführten Maßnahmen weitere Projekte zur Steigerung der IKT-Sicherheit in Planung und Umsetzung. Die Themenfelder zur Weiterentwicklung der IKT-Sicherheit im BMSGPK reichen von weiteren Awarnessmaßnahmen über die Aktualisierung der ressortspezifischen IKT-Benutzungsrichtlinien bis zum Pilotprojekt eines neuen umfassenden Information Security Management System-Systems („Managementsystem für Informationssicherheit) für das Ressort.

Im IT-Bereich Gesundheit wird aufgrund der sensiblen bzw. besonders schützenswerten Daten und unabhängig von allfälligen Vorkommnissen für ein kontinuierlich hohes Sicherheitsniveau gesorgt. Daher sind im Kontext des BMEIA-Vorfalles keine bezifferbaren Mehrkosten entstanden.
Darüber hinaus können nähere Angaben zu Maßnahmen und Leistungen sowie den damit verbundenen Kosten nicht gemacht werden, da eine öffentliche Bekanntgabe dem evidenten Interesse an der Wahrung der wesentlichen äußeren und inneren Sicherheitsinteressen der Republik Österreich zuwiderlaufen würde.

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 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.

Das GovCERT stellt das nationale Computer Emergency Response Team (CERT) für die öffentliche Verwaltung und ist als Unterstützung auch für das BMSGPK ein wichtiger Partner. Darüber hinaus bedient sich das BMSGPK auch externer Dienstleister, wie die Bundesrechenzentrum GmbH, für proaktive Abwehr von Cyberangriffen.

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.

Konkrete Maßnahmen im Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz sind der Beantwortung zu Frage 4 zu entnehmen. Die Ergebnisse fanden Niederschlag in der Optimierung der eigenen Schutzmechanismen.

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 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 Computer Emergency Response Team (CERT).

Mit freundlichen Grüßen

Rudolf Anschober

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR SOZIALES, GESUNDHEIT, PFLEGE UND KONSUMENTENSCHUTZ @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
	Datum/Zeit	2020-10-30T08:36:36+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.	2098721075
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.sozialministerium.at/site/Ministerium/Willkommen_im_Ministerium/Amtssignatur/Amtssignatur	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-10-30T08:44:49+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.	