3276/AB
vom 02.11.2020 zu 3249/J (XXVII. GP)

Bundesministerium
Europäische und internationale
Angelegenheiten

bmeia.gv.at

Mag. Alexander Schallenberg
Bundesminister

Minoritenplatz 8, 1010 Wien, Österreich

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrates
Parlament
1017 Wien

Geschäftszahl: 2020-0.569.188

Wien, am 2. November 2020

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 2. September 2020 unter der Zl. 3249/J-NR/2020 an mich eine schriftliche parlamentarische Anfrage betreffend „Konsequenzen aus Cyberattacke im Februar 2020“ gerichtet.

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

Zu den Fragen 1 und 2:

- *Welche Fehler und Sicherheitslücken wurden seit Bekanntwerden des Angriffs entdeckt und analysiert?*
  Welche Konsequenzen zogen Sie daraus?
  Bitte um Erläuterung der jeweils entsprechenden Vorgangsweise.
- *Welche konkreten Maßnahmen wurden seit Bekanntwerden des Angriffes a.) geplant und b.) umgesetzt, um die Verteidigungsfähigkeit und Sicherheit der Republik im Cyberbereich zu verbessern?*

Die IKT-Sicherheit im Bund wird als fortlaufender Prozess verstanden. Dementsprechend werden, unterstützt durch das Government Computer Emergency Response Team (GovCERT) und den Inneren Kreis der operativen Koordinierungsstruktur (IKDOK), 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 Zuge der Nachbereitung der Cyberattacke 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 Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (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 angenommenen 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 meiner Beantwortung der parlamentarischen Anfragen 646/J-NR/2020 vom 24. Jänner 2020 und in der Beantwortung der parlamentarischen Anfrage 1299/J-NR/2020 vom 25. März 2020 durch den Bundeskanzler mitgeteilt, erfolgten basierend auf den Erkenntnissen und der Risikoeinschätzung des interministeriellen Krisenstabs direkte und konkrete Risikominimierungsmaßnahmen. Basierend auf den Erkenntnissen der Cyberattacke 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.

Zu Frage 3:

- *Welche konkreten Abwehrmaßnahmen und Schritte wurden jeweils wann genau zur Analyse, Bekämpfung und Abwehr des Angriffs von wem getroffen und mit welchem konkreten Ergebnis/Erfolg? (Bitte um detaillierte Erläuterung und Unterscheidung der Maßnahmen vor sowie nach Bekanntwerden des Angriffs.)*

Die Erkennung des Angriffs auf die IT-Systeme meines Ressorts im Frühstadium ermöglichte es sofort Gegenmaßnahmen einzuleiten, wodurch ein möglicher großer Schaden abgewendet werden konnte. Die Bereinigung der Systeme erforderte umfassende technische und vor allem organisatorische Vorbereitungen und konnte am 9. Februar 2020 abgeschlossen werden. Ich ersuche um Verständnis, dass es gerade im Hinblick auf die weitere Gewährleistung der Effektivität der getroffenen, erfolgreichen Abwehrmaßnahmen nicht möglich ist, diese, beziehungsweise deren Umfang im Detail öffentlich mitzuteilen.

Die seit der Cyberattacke auf das Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) gewonnenen Erfahrungen lieferten wichtige Erkenntnisse, welche in unsere Arbeit zur weiteren Verbesserung der IT-Sicherheit einfließen. Diese Maßnahmen werden laufend evaluiert und den sich ändernden Erfordernissen angepasst.

Zu den Fragen 4 und 5:

- *Welche (Zeit-)Aufwendungen sind Ihrem Ressort durch die Analyse, Bekämpfung und Abwehr des Angriffs bisher entstanden? (Bitte um detaillierte Erläuterung und Unterscheidung der Maßnahmen vor sowie nach Bekanntwerden des Angriffs.)*
- *Welche bezifferbaren Kosten sind Ihrem Ressort seit Bekanntwerden des Angriffs durch die Analyse, Bekämpfung und Abwehr des Angriffs bisher entstanden?*

Ich verweise auf die Beantwortungen der parlamentarischen Anfragen Zl. 1299/J-NR/2020 vom 25. März 2020 und Zl. 1314/J-NR/2020 vom 26. März 2020 durch den Bundeskanzler, wonach im Zuge der Behandlung der Cyberattacke im BMEIA durch den Einsatzstab sowohl laufende Risikoeinschätzung als auch Empfehlungen erstellt wurden.

Die Aufwendungen umfassen allerdings nicht nur die erfolgte Bereinigung der Systeme, sondern auch Sicherheitsvorkehrungen für den fortlaufenden Betrieb oder die Arbeit zu mehr Resilienz der IKT-Systeme des BMEIA. Ein besonderer Fokus liegt auf dem Bereich der Sensibilisierung für IKT-Sicherheitsfragen („Security-Awareness“) für die Mitarbeiterinnen und

Mitarbeiter meines Ressorts, die laufend in IKT-sicherheitsrelevante Verhaltensregelungen geschult werden. Anlassbezogen erfolgt dies auch mit Unterstützung externer Expertinnen und Experten.
Von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus gem. dem Netz- und Informationssystemsicherheitsgesetzes, BGBl. I Nr. 111/2018, muss ich in Hinblick auf die Sicherung der Effektivität dieser Maßnahmen Abstand nehmen.

Zu Frage 6:

- *Welche Stellen und wie viele Personen Ihres Ressorts sind bzw. waren in die Analyse, Bekämpfung und Abwehr des Angriffes 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 Frage 7:

- *Welche externen Experten bzw. Unternehmen wurden für die Analyse, Bekämpfung und Abwehr des Angriffes 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. Ich verweise zusätzlich auf meine Beantwortung der parlamentarischen Anfrage 646/J-NR/2020 vom 24. Jänner 2020.

Zu Frage 8:

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

Mag. Alexander Schallenberg

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR EUROPÄISCHE UND INTERNATIONALE ANGELEGENHEITEN @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für europäische und internationale Angelegenheiten
	Datum/Zeit	2020-11-02T16:30:58+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.	789818819
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: http://www.bmeia.gv.at/verifizierung	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-11-02T16:37:30+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.	