3265/AB
vom 02.11.2020 zu 3253/J (XXVII. GP)

Bundeskanzleramt

bundeskanzleramt.gv.at

Sebastian Kurz
Bundeskanzler

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2020-0.561.780

Wien, am 2. November 2020

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 2. September 2020 unter der Nr. **3253/J** eine schriftliche parlamentarische Anfrage betreffend „Konsequenzen aus Cyberattacke auf das BMEIA im Jänner/Februar 2020“ an mich 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 BMEIA-Cybervorfalles wurde unter Koordination des Bundeskanzleramts 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 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 Bundeskanzleramt im Zuge seiner Rollenwahrnehmung als strategisches Koordinationselement die Etablierung von leitenden Informationssicherheitsbeauftragten (CISOs) vorantreibt.

Weiters darf ich auf die angenommen Anträge von NEOS sowie ÖVP und Grüne zur Cybersicherheit in der Sitzung des Nationalen Sicherheitsrats vom 28. Februar 2020 sowie auf das Regierungsprogramm 2020 – 2024 der österreichischen Bundesregierung hinweisen.

Wie schon in der Beantwortung zu den parlamentarischen Anfragen Nr. 647/J vom 24. Jänner 2020 und Nr. 1299/J vom 25. März 2020 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 basierend auf Meldungen gem. dem NISG, eigenen Systembeobachtungen und international zur Verfügung gestellten Daten regelmäßig sowohl eine Risikoeinschätzung als auch Empfehlungen zum Schutz der eigenen Systeme.

Die Anpassungen der ressortinternen Prozesse erfolgt risikobasiert und permanent. Das Sicherheitskonzept des Bundeskanzleramts wird unter Einbindung von Experten des GovCERT ständig auf die aktuellen technologischen Anforderungen hin angepasst.

Die Umsetzung der Empfehlungen erfolgt als Routinemaßnahme durch die jeweils verantwortlichen Technikerinnen und Techniker im Bundeskanzleramt. Darüber hinaus erfolgt eine kontinuierliche Marktbeobachtung, um auf neue Trends im Bereich der IKT-Sicherheit reagieren zu können.

Zu Frage 2:

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 Bundeskanzleramt wurden seit dem Vorfall keine Angriffe, welche über Standard- und Routinevorfälle hinausgehen, festgestellt. Den Bund und die kritische Infrastruktur betreffende Sicherheitsvorfälle werden im nationalen Cyber-Lagebild laufend im ELAK dokumentiert. Empfehlungen und resultierende Maßnahmen aus dem jeweiligen Cyber-Lagebild werden zeitnah evaluiert und je nach Ressourcen- und Budgetverfügbarkeit umgesetzt.

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?*

Wie schon in der Beantwortung zu den parlamentarischen Anfragen Nr. 647/J vom 24. Jänner 2020 und Nr. 1299/J vom 25. März 2020 mitgeteilt, wurden im Zuge der Vorfallsbehandlung im Bundesministerium für europäische und internationale Angelegenheiten durch den Einsatzstab sowohl eine laufende Risikoeinschätzung als auch Empfehlungen für konkrete Absicherungen der eigenen Netze erstellt und kommuniziert. Diese Maßnahmen reichten von der Scriptimplementierung zum Scannen nach im Bundesministerium für europäische und internationale Angelegenheiten festgestellter Malware über das Einspielen von Indicators of Compromise (IOCs) in der eigenen Sicherheitsarchitektur bis hin zu Blacklisting (Verweigerung zur Ausführung) von bestimmten Applikationen.

Darüber hinaus wurden im Bundeskanzleramt Begleit- und Awareness-Maßnahmen getroffen. All diese Maßnahmen wurden zeitnah durch die verantwortlichen Technikerinnen und Techniker im Bundeskanzleramt umgesetzt.

Ich bitte um Verständnis, dass von einer detaillierten Quantifizierung konkreter Aufwendungen aus Sicherheitsgründen Abstand genommen werden muss, da etwaige Angaben Rückschlüsse auf Umfang, Art und Weise der getroffenen Gegenmaßnahmen zulassen würden.

Zu Frage 6:

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.

Wie zu den parlamentarischen Anfragen Nr. 1299/J vom 25. März 2020 und Nr. 1314/J vom 26. März 2020 ausgeführt, ist im Bundeskanzleramt die Abteilung I/8 für Cybersicherheit verantwortlich.

Das GovCERT stellt das nationale Computer Emergency Response Team (CERT) für die öffentliche Verwaltung.

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

Konkrete Maßnahmen im Bundeskanzleramt sind der Beantwortung zu Frage 4 zu entnehmen. Die Ergebnisse fanden Niederschlag in der Optimierung der eigenen Schutzmechanismen.

Sebastian Kurz

REPUBLIK ÖSTERREICH BUNDESKANZLERAMT AMTSSIGNATUR	Unterzeichner	serialNumber=932783133,CN=Bundeskanzleramt,C=AT
	Datum/Zeit	2020-11-02T09:12:53+01:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bundeskanzleramt.gv.at/verifizierung
	Hinweis	Dieses Dokument wurde amtssigniert.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-11-02T09:19:32+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.	