3268/AB
vom 02.11.2020 zu 3246/J (XXVII. GP)

Bundesministerium
Arbeit, Familie und Jugend

bmafj.gv.at

Mag. (FH) Christine Aschbacher
Bundesministerin

christine.aschbacher@bmafj.gv.at
+43 1 711 00-0
Untere Donaustraße 13-15, 1020 Wien

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.562.122

Ihr Zeichen: BKA - PDion (PDion)3246/J-NR/2020

Wien, am 02. November 2020

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 02.09.2020 unter der **Nr. 3246/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:

Einleitend darf festgehalten werden, dass mit Inkrafttreten der Bundesministeriengesetz-Novelle 2020 am 29. Jänner 2020 das Bundesministerium für Arbeit, Familie und Jugend neu gegründet wurde. Dabei ist das Bundesministerium für Arbeit, Familie und Jugend aus verschiedenen Organisationseinheiten des Bundes neu entstanden.

Im Rahmen der IT-Konsolidierung im Bund soll die IT-Infrastruktur meines Ressorts durch die Bundesrechenzentrum GmbH neu aufgebaut und betrieben werden.

Zur Frage 1

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

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 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.

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 der Beantwortung zu den parlamentarischen Anfragen Nr. 647/J und Nr. 1299/J an das Bundeskanzleramt 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?*
    - *Wenn ja, welche?*
    - *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 Arbeit, Familie und Jugend 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.

Zur 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 im Cyberbereich zu verbessern?*

Wie schon in der Beantwortung zu den parlamentarischen Anfragen Nr. 647/J und Nr. 1299/J an das Bundeskanzleramt 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 Umsetzung der Empfehlungen erfolgt als Routinemaßnahme durch die jeweils verantwortlichen Technikerinnen und Techniker im Bundesministerium für Arbeit, Familie und Jugend. Darüber hinaus erfolgt eine kontinuierliche Marktbeobachtung, um auf neue Trends im Bereich der IKT-Sicherheit reagieren zu können.

Zur 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 zu den parlamentarischen Anfragen Nr. 1299/J und Nr. 1314/J an das Bundeskanzleramt aus dem laufenden Jahr ausgeführt 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 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.

Darüber hinaus darf ich dazu auf meine einleitende Bemerkung verweisen.

Zur Frage 5

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

Auf die Beantwortung zu Frage 4 wird verwiesen.

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 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?*
    - *Wenn ja, seit wann mit welchen Expert_innen/Unternehmen?*
    - *Wenn nein, weshalb nicht?*

Sollte eine detaillierte Beantwortung einzelner Fragen aus Geheimhaltungsgründen

nicht möglich sein, so wird dennoch um eine Beantwortung mit möglichst hohem Informationsgehalt im Sinne des parlamentarischen Interpellationsrechts ersucht. Allenfalls ersuchen die Abgeordneten um eine Beantwortung in klassifizierter Weise nach dem Bundesgesetz über die Informationsordnung des Nationalrates und des Bundesrates - InfOG

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. (FH) Christine Aschbacher

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR ARBEIT, FAMILIE UND JUGEND @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Arbeit, Familie und Jugend
	Datum/Zeit	2020-11-02T10:15:43+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.	743463191
	Hinweis	Dieses Dokument wurde amtssigniert.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-11-02T10:42:23+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.	