3275/AB
vom 02.11.2020 zu 3252/J (XXVII. GP)

Bundesministerium
Bildung, Wissenschaft
und Forschung

bmbwf.gv.at

+43 1 531 20-0
Minoritenplatz 5, 1010 Wien

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.563.638

Die schriftliche parlamentarische Anfrage Nr. 3252/J-NR/2020 betreffend Konsequenzen aus Cyberattacke auf das BMEIA im Jänner/Februar 2020, die die Abg. Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen am 2. September 2020 an mich richteten, wird wie folgt beantwortet:

Zu 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 Cybervorfalles im Bundesministerium für europäische und internationale Angelegenheiten wurde unter Koordination des Bundeskanzleramtes 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.

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 zur Parlamentarischen Anfrage Nr. 1311/J-NR/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 (IKDOK) bzw. die Operative Koordinierungsstruktur (OPKOORD) erstellt regelmäßig basierend auf Meldungen gemäß dem NISG eigenen Systembeobachtungen und international zur Verfügung gestellten Daten sowohl eine Risikoeinschätzung als auch Empfehlungen zum Schutz der eigenen Systeme.

Die Anpassungen der ressortinternen Prozesse erfolgt risikobasiert und permanent. Das Sicherheitskonzept des Bundesministeriums für Bildung, Wissenschaft und Forschung wird ständig auf die aktuellen technologischen Anforderungen und der IKT-Sicherheit hin angepasst.

Zu 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 Government Computer Emergency Response Team (GovCERT) und den 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 Bundesministerium für Bildung, Wissenschaft und Forschung wurden seit dem Vorfall keine Angriffe, welche über Standard- und Routinevorfälle hinausgehen, festgestellt. Die kritische Infrastruktur betreffende Sicherheitsvorfälle werden entsprechend dokumentiert. Empfehlungen und resultierende Maßnahmen aus dem jeweiligen Cyber-Lagebild werden zeitnah evaluiert und je nach Ressourcen- und Budgetverfügbarkeit umgesetzt.

Zu 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 in der Beantwortung zur Parlamentarischen Anfrage Nr. 1311/J-NR/2020 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 der im Bundesministerium für europäische und internationale Angelegenheiten festgestellten Malware über das Einspielen von Indicators of Compromise (IOCs) in der eigenen Sicherheitsarchitektur bis hin zu Blacklists (Verweigerung zur Ausführung) von bestimmten Applikationen.

Die aus der Vorfallsbehandlung bezogenen Informationen wurden im Bundesministerium für Bildung, Wissenschaft und Forschung zum proaktiven Scan und zur nachhaltigen Verbesserung der Absicherung der IT-Infrastruktur genutzt. Bereits vor dem Angriff auf das Bundesministerium für europäische und internationale Angelegenheiten wurden im Bundesministerium für Bildung, Wissenschaft und Forschung spezielle Sicherheitslösungen, wie Application Whitelisting und 2-Faktor Authentifizierung, eingesetzt. Die Anschaffungskosten für das Application Whitelisting beziffern sich auf EUR 84.000 und laufende Kosten von EUR 19.200 pro Jahr. Die Kosten für die 2-Faktor Authentifizierung belaufen sich auf Einmalkosten in der Höhe von EUR 51.000 und laufende Kosten von EUR 12.000 pro Jahr.

Die nach dem Angriff zusätzlich geleisteten Aufwände setzen sich aus einem nicht näher bezifferbaren internen Personenaufwand bzw. pauschalierten Dienstleistungsrahmenvereinbarungen und rund EUR 15.000 für sicherheitstechnische Prüfungen zusammen.

Zu 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 der Geschäftseinteilung zu entnehmen. Die Analysen und Verbesserungen der Sicherheit (Adaptierung bzw. Optimierung bestehender Systeme) erfolgen durch das eingeteilte Personal im Rahmen der routinemäßigen Aufgabenwahrnehmung.

Zu Fragen 7 und 8:

- *Welche externen Experten bzw. Unternehmen wurden für die Analyse und Verbesserung der Sicherheit in Ihrem Ressort in welcher Weise und wann jeweils zugezogen?*
- *Verfügt Ihr Ressort über einen Rahmenvertrag mit externen Exptert_innen*[sic]*/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. Die Shared Services des Bundes in der BRZ (z.B. ELAK) unterliegen dem dort angesiedelten unternehmenseigenen CERT. Darüber hinaus können bei konkreten Vorfällen und Bedarf externe Expertinnen und Experten sowie Unternehmen beauftragt werden.

Wien, 2. November 2020
Der Bundesminister:

Univ.-Prof. Dr. Heinz Faßmann eh.

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR BILDUNG, WISSENSCHAFT UND FORSCHUNG @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Bildung, Wissenschaft und Forschung
	Datum/Zeit	2020-11-02T16:12:31+01:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	285175223
	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.bmbwf.gv.at/verifizierung.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-11-02T16:19:14+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.	