3271/AB
vom 02.11.2020 zu 3245/J (XXVII. GP)

Bundesministerium
Landwirtschaft, Regionen
und Tourismus

bmlrt.gv.at

Elisabeth Köstinger
Bundesministerin für
Landwirtschaft, Regionen und Tourismus

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2020-0.564.133

Ihr Zeichen: BKA - PDion
(PDion)3245/J-NR/2020

Wien, 02.11.2020

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 02.09.2020 unter der Nr. **3245/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:

Zur Frage 1:

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

Im Zuge der Nachbereitung des Cybervorfalles im Bundesministerium für europäische und internationale Angelegenheiten 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 dem Netz- und Informationssicherheitsgesetz (NISG) und der Österreichischen 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 (Chief Information Security Officers, CISOs) vorantreibt.

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

Wie schon in den Beantwortungen des Herrn Bundeskanzlers zu den parlamentarischen Anfragen 647/J vom 24. Januar 2020 und 1299/J vom 25. März 2020 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 (IKDOK) bzw. die Operative Koordinierungsstruktur (OPKOORD) erstellt regelmäßig, basierend auf Meldungen nach dem NISG, nach eigenen Systembeobachtungen und international zur Verfügung gestellten Daten sowohl eine Risikoeinschätzung als auch Empfehlungen zum Schutz der eigenen Systeme.

Die Anpassungen der ressortinternen Prozesse erfolgen risikobasiert und permanent. Das Sicherheitskonzept des Bundesministeriums für Landwirtschaft, Regionen und Tourismus wird unter Einbindung von Expertinnen bzw. Experten des Government Computer Emergency Response Team (GovCERT) ständig auf die aktuellen technologischen Anforderungen hin angepasst.

Zur 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 Sicherheit der Informations- und Kommunikationstechnologie (IKT) im Bund wird als fortlaufender Prozess verstanden. Dementsprechend werden, unterstützt durch das GovCERT und den IKDOK, kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur vorgenommen. Dies betrifft sowohl die Beschaffung der 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 Landwirtschaft, Regionen und Tourismus wurden seit dem Vorfall keine Angriffe, welche über Standard- und Routinevorfälle hinausgehen, festgestellt. Bei Bedarf kann das Bundesministerium für Landwirtschaft, Regionen und Tourismus Sicherheitsvorfälle dem GovCERT melden.

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?

Die Umsetzung der Empfehlungen des IKDOK bzw. der OPKOORD erfolgt als Routinemaßnahme durch die jeweils verantwortlichen Technikerinnen und Techniker im Bundesministerium für Landwirtschaft, Regionen und Tourismus. Außerdem erfolgt eine kontinuierliche Marktbeobachtung, um auf neue Trends im Bereich der IKT-Sicherheit reagieren zu können. Für die Aufrechterhaltung des ordentlichen Betriebes werden laufend und zyklisch Aktualisierungen der IT-Systeme (Einspielen von Softwareaktualisierung) vorgenommen.

Darüber hinaus darf auf die Beantwortung der Frage 1 verwiesen werden.

Zu den 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 der parlamentarischen Anfrage 1299/J vom 25. März 2020 aus dem laufenden Jahr durch den Herrn Bundeskanzler 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 Bundesministerium für europäische und internationale Angelegenheiten 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 diese Maßnahmen wurden zeitnah durch die verantwortlichen Technikerinnen und Techniker im Bundesministerium für Landwirtschaft, Regionen und Tourismus umgesetzt. Darüber hinaus wurden im Bundesministerium für Landwirtschaft, Regionen und Tourismus folgende Aufwendungen getätigt:

- Einbindung des Internetproviders zur Abwehr von Cyberangriffen (zyklisch)
- Laufende Aktualisierung der bestehenden technischen Schutzmechanismen und IT-Sicherheitslösungen (zyklisch)
- Laufende Überarbeitung der organisatorischen IT-Sicherheitsmaßnahmen (zyklisch)
- Analyse und Auswahl von Dienstleisterinnen bzw. Dienstleistern und deren Portfolio zum Abruf im Anlassfall unter Zusammenarbeit mit den koordinierenden Stellen des Bundes (nach Bekanntwerden des Cyberangriffs)
- Evaluierung und Vorbereitung einer erweiterten technischen Sicherheitsüberprüfung (zyklisch)

Zur 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?

Für den Bereich Cybersicherheit ist im Bundesministerium für Landwirtschaft, Regionen und Tourismus die Abteilung IKT-Grundsatzangelegenheiten und IKT-Management verantwortlich. Die Anzahl der dort eingeteilten Personen ist der Geschäfts- und Personaleinteilung zu entnehmen. Die Analysen und Verbesserungen der Sicherheit (Adaptierung bzw. Optimierung bestehender Systeme) erfolgen durch das zuständige Personal im Rahmen der routinemäßigen Aufgabenwahrnehmung.

Das GovCERT stellt das nationale Computer Emergency Response Team (CERT) für die öffentliche Verwaltung. Darüber hinaus bedient sich das Bundesministerium für Landwirtschaft, Regionen und Tourismus externer Dienstleistung des Internetanbieters zur Abwehr von Cyberangriffen.

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 Expertinnengruppen bzw. 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 Landwirtschaft, Regionen und Tourismus sind der Beantwortung der Fragen 1, 4 und 5 zu entnehmen. Die Ergebnisse fanden Niederschlag in der Optimierung der eigenen Schutzmechanismen.

Zur 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 Expertinnengruppen bzw. 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 Bundesrechenzentrum GmbH (BRZ) (z. B. ELAK) unterliegen dem dort angesiedelten unternehmenseigenen CERT.

Elisabeth Köstinger

	Unterzeichner	Bundesministerium für Landwirtschaft, Regionen und Tourismus
	Datum/Zeit	2020-11-02T11:23:31+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.	1506369323
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur und des Ausdrucks finden Sie unter: http://www.bmlrt.gv.at/amtssignatur	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-11-02T11:25:13+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.	