3261/AB
vom 02.11.2020 zu 3254/J (XXVII. GP)

Bundesministerium
Digitalisierung und
Wirtschaftsstandort

bmdw.gv.at

Dr. Margarete Schramböck
Bundesministerin für Digitalisierung und Wirtschaftsstandort

buero.schramboeck@bmdw.gv.at
Stubenring 1, 1010 Wien

Präsident des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.573.972

Ihr Zeichen: BKA - PDion (PDion)3254/J-NR/2020

In Beantwortung der schriftlichen parlamentarischen Anfrage Nr. 3254/J betreffend "Konsequenzen aus Cyberattacke auf das BMEIA im Jänner/Februar 2020", welche die Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen am 2. September 2020 an mich richteten, stelle ich fest:

Antwort zu Punkt 1 der Anfrage:

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

Im Zuge der Nachbereitung des Cybervorfalls im Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) wurde unter Koordination des Bundeskanzleramtes (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 Netz- und Informationssystemsicherheitsgesetz (NISG) und Österreichischer Strategie für Cybersicherheit (ÖSCS) 2013 in großen Teilen als zielgerichtet und effizient erwiesen. Die im Zuge der "Lessons Identified" festgestellten Verbesserungsmaßnahmen 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 funktionieren.

Die Attacke auf das BMEIA bestätigte die Cyber-Security Strategie meines Ressorts. In dieser ist festgelegt, dass erstens das Computer Emergency Response Team des BMDW als

Notfallorganisation fungiert, welches im Falle einer Cyber-Attacke die Cyber-Abwehr übernimmt. Zur Erhöhung der Sichtbarkeit in Client-, Netzwerk- und Server-Infrastruktur wurde zweitens bereits vor dem Vorfall im BMEIA ein Security Incident and Event Management und ein Security Operation Center (SOC) beauftragt. Drittens wurde ebenfalls bereits vor dem Vorfall im BMEIA beim operativen IT-Dienstleister ein Security-Manager installiert, welcher die eingehenden Findings laufend sichtet, bewertet und einer Lösung zuführt.

Antwort zu Punkt 2 der Anfrage:

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 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 durchgeführt.

Seit Bekanntwerden des Cyber-Angriffs auf das BMEIA wurden in der laufenden Betriebsführung und vom SOC keine gezielten Angriffe gegen die IKT-Infrastruktur meines Ressorts entdeckt, die über das normale quantitative und qualitative Ausmaß wie etwa allgemeine Phishing-Kampagnen, Port-Scans oder Script-Kiddies hinausgehen. Konfigurationsfehler und Sicherheitslücken, welche durch die laufenden Vulnerability-Scans des SOC aufgedeckt werden, werden im Rahmen der Betriebsführung gelöst.

Antwort zu Punkt 3 der Anfrage:

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 den Beantwortungen zu den parlamentarischen Anfragen Nr. 647/J und 1299/J durch den Herrn Bundeskanzler mitgeteilt, erfolgten auf Grundlage der Erkenntnisse und Risikoeinschätzung des interministeriellen Krisenstabs direkte und konkrete Risikominimierungsmaßnahmen. So wurden etwa die jeweiligen Systeme gehärtet und die automatisierten Abwehrmaßnahmen verbessert.

Der IKDOK und die Operative Koordinierungsstruktur erstellen regelmäßig aufgrund von Meldungen gemäß NISG, eigenen Systembeobachtungen und international zur Verfügung gestellten Daten sowohl eine Risikoeinschätzung als auch Empfehlungen zum Schutz der eigenen Systeme.

Die vom IKDOK übermittelten Indicators of Compromise (IOC) wurden in der IKT-Infrastruktur meines Ressorts zur Anwendung gebracht. Konfigurationsänderungen an der Client Endpoint Security sowie der Serverinfrastruktur wurden vorgenommen, um den Angriffsvektor, welcher im BMEIA genutzt wurde, zu erschweren bzw. in der bekannten Form zu verunmöglichen.

Antwort zu den Punkten 4 und 5 der Anfrage:

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 in den Beantwortungen der parlamentarischen Anfragen Nr. 1298/J und 1315/J ausgeführt, wurden durch den Einsatzstab im Zuge der Behandlung des Vorfalls im BMEIA 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 IOCs in der eigenen Sicherheitsarchitektur bis hin zu "excecution-policies" (Verweigerung zur Ausführung) von bestimmten Applikationen.

Die Risikoanalyse und die darauffolgenden Konfigurationsanpassungen wurden laufend und zeitnah mit den Erkenntnissen und Empfehlungen der IKDOK durchgeführt. Die Tätigkeiten erfolgten im Rahmen der Betriebsführung auf Basis des bestehenden Rahmenvertrags mit dem operativen IT-Dienstleister und haben zu keinen Zusatzkosten geführt.

Antwort zu Punkt 6 der Anfrage:

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 Analysen und Verbesserungen der Sicherheit durch Adaptierung bzw. Optimierung bestehender Systeme erfolgen durch die gemäß der Geschäfts- und Personaleinteilung meines Ressorts damit befassten Mitarbeiterinnen und Mitarbeiter im Rahmen der Wahrnehmung ihrer dienstlichen Aufgaben.

Antwort zu den Punkten 7 und 8 der Anfrage:

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 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?

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 lnterpellationsrechts ersucht. Allenfalls ersuchen die Abgeordneten um eine Beantwortung in klassifizierter Weise nach dem Bundesgesetz über die Informationsordnung des Nationalrates und des Bundesrates - lnfOG.

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 Bundesrechenzentrum GmbH wie etwa der ELAK unterliegen dem dort angesiedelten unternehmenseigenen CERT.

Seit 2012 besteht zur Bereitstellung von IT-Dienstleistungen für mein Ressort ein Rahmenvertrag mit einem IT-Dienstleister. Laufende IT-Security-Dienstleistungen, welche in der regulären Betriebsführung zu erbringen sind, stellen einen integrierten Vertrags- und Leistungsgegenstand dar. Über diesen Rahmenvertrag ist das Ressort auch berechtigt, über die im Rahmenvertrag beschriebenen IT-Dienstleistungen hinausgehende zusätzliche IT-Security-Dienstleistungen abzurufen.

Nach Bekanntwerden der technischen Details zum Cyber-Angriff auf das BMEIA wurde im Rahmen der regulären Betriebsführung die Anfälligkeit der IKT-Infrastruktur meines Ressorts, insbesondere der Ressort-Clients, geprüft und mit dem IT-Dienstleister des Ressorts eine Risikobewertung durchgeführt. In den Jahren 2017 und 2019 wurden jeweils externe IT-Security-Audits durchgeführt und eine IT-Security Roadmap auf Basis der dort angegebenen kurz-, mittel- und langfristigen Empfehlungen aufgebaut.

Wien, am 2. November 2020

Dr. Margarete Schramböck

Elektronisch gefertigt

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-11-02T07:49:26+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.	