2557/AB
vom 26.08.2020 zu 2533/J (XXVII. GP)

Bundesministerium
Europäische und internationale Angelegenheiten

bmeia.gv.at

Mag. Alexander Schallenberg
Bundesminister

Minoritenplatz 8, 1010 Wien, Österreich

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrates
Parlament
1017 Wien

Geschäftszahl: 2020-0.420.813

Wien, am 26. August 2020

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 26. Juni 2020 unter der Zl. 2533/J-NR/2020 an mich eine schriftliche parlamentarische Anfrage betreffend „Maßnahmen zur Steigerung der IKT-Sicherheit“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zu den Fragen 1 bis 5:

- *Wann wurde das letzte Cybersecurity-Audit am BMEIA durchgeführt?*
  Welche Abteilungen des BMEIA nahmen an diesem Audit teil?
  Nahmen Führungskräfte der jeweiligen Abteilungen und Sektionen an diesem Audit teil?
  Wenn ja, welche?
  Wenn nein, warum nicht?
  Welches Unternehmen bzw. welche interne Stelle führte dieses Audit durch?

Wurde hier eine Ausschreibung getätigt?
Wenn nein, warum nicht?
Wie wurde die Cybersecurity-Ausstattung (sowohl technisch als auch personell) des BMEIA bewertet?
Welche Komponenten der technischen bzw. personellen Ausstattung wurden im Rahmen des Audits als ausreichend bewertet? Welche nicht? Bitte jeweils für ausreichende und nicht ausreichende Komponenten um Auflistung und um differenzierte Darstellung nach Personal und EDV-Ausrüstung.
Welche Empfehlungen wurden in der Folge des Audits ausgesprochen?
Welche dieser Empfehlungen wurden umgesetzt? Wann genau und welche Kosten sind hierfür angefallen? Wurden die veranschlagten Kosten über- bzw. unterschritten? Bitte um Aufschlüsselung pro Maßnahme.
Die Umsetzung welcher dieser Empfehlungen ist noch ausständig und warum wurden diese Empfehlungen nicht umgesetzt? Ist es geplant, diese Empfehlungen umzusetzen und wenn ja, wann?
Wie wurden die zum damaligen Zeitpunkt bereits getroffenen Maßnahmen und Vorkehrungen zur IKT-Sicherheit im Rahmen des Audits bewertet?
Welche Maßnahmen bzw. Vorkehrungen wurden als ausreichend bewertet? Welche nicht? Bitte jeweils für ausreichende und nicht ausreichende Maßnahmen/Vorkehrungen um getrennte Auflistung.
Welche Empfehlungen wurden in der Folge des Audits ausgesprochen?
Welche dieser Empfehlungen wurden in der Folge des Audits umgesetzt? Wann genau, von wem, gab es hierfür Ausschreibungen und welche Kosten sind angefallen? Wurden die veranschlagten Kosten über- bzw. unterschritten? Bitte um Aufschlüsselung pro Maßnahme.
Die Umsetzung welcher dieser Empfehlungen ist noch ausständig und warum wurden diese Empfehlungen nicht umgesetzt? Ist es geplant, diese Empfehlungen umzusetzen und wenn ja, wann?

- *Ist das nächste Cybersecurity-Audit am BMEIA bereits geplant?*
  Wenn ja, wer wird dieses Audit durchführen?
  Wenn ja, wann wird es durchgeführt?
  Wenn nein, warum ist ein solches Audit - insbesondere in Anbetracht des letzten Cyberangriffs - nicht geplant?
- *Wurden von den intern für Cybersecurity bzw. IT-Sicherheit zuständigen Personen bzw. Abteilungen des BMEIA Maßnahmen zur Erhöhung der IKT-Sicherheit vorgeschlagen?*
  Wenn ja, wann genau?
  Wenn ja, wurden diese Vorschläge jährlich vorgebracht?

- *Falls solche Maßnahmen von den intern für Cybersecurity bzw. IT-Sicherheit zuständigen Personen bzw. Abteilungen vorgeschlagen wurden, waren folgende Maßnahmen in den Vorschlägen enthalten?*
  SSL-Interception?
  Welche Kosten wurden hierfür veranschlagt?
  Welcher personelle Aufwand wurde hierfür veranschlagt?
  Welche Priorität kam dieser Maßnahme zu?
  Wurde die Maßnahme umgesetzt?
  Wenn ja, wann?
  Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
  Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
  Wenn nein, warum nicht?
  Einführung einer Security-Information and Event-Management-Lösung?
  Welche Kosten wurden hierfür veranschlagt?
  Welcher personelle Aufwand wurde hierfür veranschlagt?
  Welche Priorität kam dieser Maßnahme zu?
  Wurde die Maßnahme umgesetzt?
  Wenn ja, wann?
  Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
  Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
  Wenn nein, warum nicht?
  Active-Threat-Protection bei E-Mails?
  Welche Kosten wurden hierfür veranschlagt?
  Welcher personelle Aufwand wurde hierfür veranschlagt?
  Welche Priorität kam dieser Maßnahme zu?
  Wurde die Maßnahme umgesetzt?
  Wenn ja, wann?
  Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
  Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
  Wenn nein, warum nicht?
  Planung/Aufbau eines sicheren, abgeschotteten Systems?
  Welche Kosten wurden hierfür veranschlagt?
  Welcher personelle Aufwand wurde hierfür veranschlagt?
  Welche Priorität kam dieser Maßnahme zu?
  Wurde die Maßnahme umgesetzt?

Wenn ja, wann?
Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
Wenn nein, warum nicht?
Zentraler Internetzugang?
Welche Kosten wurden hierfür veranschlagt?
Welcher personelle Aufwand wurde hierfür veranschlagt?
Welche Priorität kam dieser Maßnahme zu?
Wurde die Maßnahme umgesetzt?
Wenn ja, wann?
Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
Wenn nein, warum nicht?
Penetrationstest zur Erkennung von Sicherheitsschwachstellen?
Welche Kosten wurden hierfür veranschlagt?
Welcher personelle Aufwand wurde hierfür veranschlagt?
Welche Priorität kam dieser Maßnahme zu?
Wurde die Maßnahme umgesetzt?
Wenn ja, wann?
Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
Wenn nein, warum nicht?
Audit der Zentrale?
Welche Kosten wurden hierfür veranschlagt?
Welcher personelle Aufwand wurde hierfür veranschlagt?
Welche Priorität kam dieser Maßnahme zu?
Wurde die Maßnahme umgesetzt?
Wenn ja, wann?
Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
Wenn nein, warum nicht?
Abspeicherung sensibler Daten im Elektronischen Akt?
Welche Kosten wurden hierfür veranschlagt?
Welcher personelle Aufwand wurde hierfür veranschlagt?

Welche Priorität kam dieser Maßnahme zu?
Wurde die Maßnahme umgesetzt?
Wenn ja, wann?
Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
Wenn nein, warum nicht?
Intrusion-Detection/Intrusion-Prevention-System?
Welche Kosten wurden hierfür veranschlagt?
Welcher personelle Aufwand wurde hierfür veranschlagt?
Welche Priorität kam dieser Maßnahme zu?
Wurde die Maßnahme umgesetzt?
Wenn ja, wann?
Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
Wenn nein, warum nicht?
Awareness-Training für sämtliche Mitarbeiter_innen?
Welche Kosten wurden hierfür veranschlagt?
Welcher personelle Aufwand wurde hierfür veranschlagt?
Welche Priorität kam dieser Maßnahme zu?
Wurde die Maßnahme umgesetzt?
Wenn ja, wann?
Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
Wenn nein, warum nicht?
2-Faktor-Authentifizierung an den IT-Arbeitsplätzen?
Welche Kosten wurden hierfür veranschlagt?
Welcher personelle Aufwand wurde hierfür veranschlagt?
Welche Priorität kam dieser Maßnahme zu?
Wurde die Maßnahme umgesetzt?
Wenn ja, wann?
Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
Neuaufsetzung der Arbeitsplätze?
Welche Kosten wurden hierfür veranschlagt?

Welcher personelle Aufwand wurde hierfür veranschlagt?
Welche Priorität kam dieser Maßnahme zu?
Wurde die Maßnahme umgesetzt?
Wenn ja, wann?
Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
Wenn nein, warum nicht?
Networking mit anderen Außenministerien/Erkundung des Markts?
Welche Kosten wurden hierfür veranschlagt?
Welcher personelle Aufwand wurde hierfür veranschlagt?
Welche Priorität kam dieser Maßnahme zu?
Wurde die Maßnahme umgesetzt?
Wenn ja, wann?
Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
Wenn nein, warum nicht?

- *Falls Maßnahmen von den intern für Cybersecurity bzw. IT-Sicherheit zuständigen Personen bzw. Abteilungen vorgeschlagen wurden, welche anderen Maßnahmen außer jenen in Frage 4 a-m genannten wurden vorgeschlagen?*
  Wann wurden diese vorgeschlagen?
  Welche Kosten wurden jeweils pro Maßnahme veranschlagt?
  Welcher personelle Aufwand wurde jeweils pro Maßnahme veranschlagt?
  Welche Priorität kam den Maßnahmen jeweils zu?
  Wurden die Maßnahmen jeweils umgesetzt?
  Wenn ja, wann?
  Wenn ja, von welchem Unternehmen bzw. welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
  Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
  Wenn nein, warum wurden die jeweiligen Maßnahmen nicht umgesetzt?

Nach dem massiven Cyberangriff auf das interne IT-System des Bundesministeriums für europäische und internationale Angelegenheiten (BMEIA), wurden weitere Maßnahmen zur Erhöhung der IKT-Sicherheit getroffen. Diese basieren auf konkreten Bedarfs- und Sicherheitsanalysen. Die seit dem Cyberangriff gewonnenen Erfahrungen lieferten uns dabei wichtige Erkenntnisse, welche in unsere Arbeit zur weiteren Verbesserung der IT-Sicherheit

einfliessen. Die Maßnahmen werden laufend evaluiert und den sich ändernden Erfordernissen angepasst.

Diese Maßnahmen sind im Besonderen die Abspeicherung sensibler Daten im ELAK, Active Threat Protection, Artificial Intelligence für IT-Security, Endpoint Detection and Response, Erweitertes Mobile Device Management, Härtung Active Directory, Intrusion Prevention System, Logging System, Mehr-Faktor-Authentifizierung, Netzwerksegmentierung, Planung/Aufbau eines sicheren abgeschotteten Systems, Security Information and Event Management, Security Operating Center sowie SSL-Interception.

Des Weiteren kann ich noch hervorheben, dass von externen, ordnungsgemäß beauftragten Unternehmen regelmäßig Cybersecurity-Audits durchgeführt werden, insbesondere nach der Implementierung von neuen Systemen, um unmittelbar Schwachstellen erkennen zu können. So ist Ende d. J. bzw. Anfang 2021 ein weiteres Audit geplant, welches von der IKT-Abteilung zusammen mit der Sicherheitsabteilung beauftragt und durchgeführt wird. Erkenntnisse daraus fließen unmittelbar in die Systemkonzeption ein und werden in Folge umgesetzt.

Ein besonderer Fokus liegt auf dem Bereich der Sensibilisierung für IKT-Sicherheitsfragen („Security-Awareness“). Bereits ab Dienstantritt neuer Mitarbeiterinnen und Mitarbeiter werden diese entsprechend intensiv eingeschult. Im Rahmen der verpflichtenden vor einer Auslandsversetzung zu absolvierenden Sicherheitsgespräche werden diese Aspekte in Einzelgesprächen vertieft. Darüber hinaus werden IKT-sicherheitsrelevante Verhaltensregelungen anlässlich der IKT-Sicherheitskontrollen an den österreichischen Vertretungsbehörden im Ausland laufend in Erinnerung gerufen. Anlassbezogen werden mit Unterstützung externer Expertinnen und Experten auch Mitarbeiterinnen und Mitarbeiter der Zentrale fortgebildet.

Zudem halte ich fest, dass gerade bei der Cyber-Security eine EU-weite Zusammenarbeit und ein diesbezüglicher Informationsaustausch zwingend erforderlich sind, um den aktuellen Bedrohungen erfolgreich entgegentreten zu können. Dies hat sich insbesondere durch den jüngsten Cyberangriff bewahrheitet. Deshalb ist beispielsweise das BMEIA im Rahmen des österreichischen „Government Computer Emergency Response Team“ (GovCERT Austria) mit dem „Computer Emergency Response Team for the EU Institutions, bodies and agencies“ (CERT-EU) vernetzt, welches mit den CERTs der Mitgliedstaaten und mit spezialisierten IT-Sicherheitsunternehmen zusammenarbeitet, um auf Vorfälle im Bereich der Informationssicherheit und Cyber-Bedrohungen zu reagieren. Gleichzeitig ist es angezeigt, den Markt für IKT-Sicherheitsdienstleistungen laufend zu beobachten und mit den Marktteilnehmern in einem ständigen Austausch zu bleiben, um dem Stand der Technik

entsprechen zu können. Die Kontaktnahme erfolgt dabei sowohl durch einzelne Unternehmen als auch proaktiv durch das BMEIA.

Schließlich ersuche ich um Verständnis, dass weitere Details nicht bekannt gegeben werden können, um die Effizienz der Maßnahmen nicht zu gefährden. Ebenso kann zu sicherheitsrelevanten Vorkehrungen und Maßnahmen im Bereich der IKT-Sicherheit im Sinne des Art. 20 Abs. 3 des Bundes-Verfassungsgesetzes keine Auskunft gegeben werden.

Zu Frage 6:

- *Wurde im BMEIA - neben der Implementierung von einzelnen Sicherheitsmaßnahmen - auch ein umfassendes Konzept zu Cybersecurity erarbeitet?*
  Wenn ja, von wem?
  Wenn ja, wann?
  Wenn ja, welche Punkte umfasst dieses Konzept?
  Wurde Personal eigens für die Einhaltung bzw. Umsetzung dieses Konzepts eingesetzt bzw. ist dies in Planung? War bzw. ist hierfür zusätzliches Personal vorgesehen?
  Wenn nein, warum nicht?
  Ist die Ausarbeitung eines solchen Konzepts in Anbetracht des letzten Cyberangriffs auf das BMEIA in Planung? Wenn nein, warum nicht?

IKT-Sicherheit wird als zentraler und fortlaufender Prozess gesehen, wobei Maßnahmen und Konzepte einer permanenten dem aktuellen Stand der Technik entsprechenden Evaluierung und Anpassung unterliegen. In diesen Prozess sind insbesondere jene Erkenntnisse, die sich nach dem letzten Cyberangriff ergeben haben, umfassend eingeflossen.

Mag. Alexander Schallenberg

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR EUROPÄISCHE UND INTERNATIONALE ANGELEGENHEITEN @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für europäische und internationale Angelegenheiten
	Datum/Zeit	2020-08-26T16:10:21+02:00
	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.	789818819
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.bmeia.gv.at/verifizierung	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-08-26T16:14:54+02:00
	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.	