2533/J
vom 26.06.2020 (XXVII. GP)

Anfrage

der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen an den Bundesminister für europäische und internationale Angelegenheiten betreffend Maßnahmen zur Steigerung der IKT-Sicherheit

Am 4. Jänner 2020 hatte das Außenministerium einen gezielten und hochprofessionellen Cyberangriff gemeldet, der am 13. Februar 2020 offiziell als beendet erklärt wurde. Laut eines FM4-Berichts sei es den Angreifer_innen zwei Tage lang möglich gewesen, unbemerkt Zugriff auf die E-Mail-Server des Außenministeriums zu erlangen, Passwörter von Konten zu sammeln und Korrespondenzen zu exfiltrieren. Dass die Attacke in der Frühphase entdeckt wurde, habe laut FM4 weniger mit Österreichs Cyberabwehr-Strategie als mit "einer Kombination aus günstigen Umständen, der Umsicht und Improvisationsfähigkeit der beteiligten Techniker sowie einem technischen Husarenstreich gegen die Kommunikation der Schadsoftware im Netz des Außenministeriums mit den externen Command-Control-Servern" zu tun. (https://fm4.orf.at/stories/2998771/)

In den Systemen des BMEIA laufen eine Reihe vertraulicher und höchst sensibler Daten zusammen, angefangen von konsularischen persönlichen Daten von Österreicher_innen über vertrauliche EU-Dokumente bis hin zu heiklen außenpolitischen Dokumenten. In den falschen Händen können diese Dokumente dem Staat, seinen internationalen Partner_innen und seinen Bürger_innen massiven Schaden zufügen.

Der Cyberangriff auf das Außenministerium offenbart ernstzunehmende Schwachstellen in der Sicherheits- bzw. Verteidigungsarchitektur der Republik und beeinträchtigt die Integrität und Funktionsfähigkeit einer staatlichen Behörde. In Anbetracht der Tatsache, dass das BMEIA auch in der Vergangenheit bereits wiederholt Cyberangriffen ausgesetzt war, stellen sich Fragen zur IKT-Sicherheit, und hier insbesondere zu den Maßnahmen, die seitens des BMEIA bereits vor dem Cyberangriff zu Beginn dieses Jahres getroffen wurden.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Wann wurde das letzte Cybersecurity-Audit am BMEIA durchgeführt?
    a. Welche Abteilungen des BMEIA nahmen an diesem Audit teil?
        i. Nahmen Führungskräfte der jeweiligen Abteilungen und Sektionen an diesem Audit teil?
            1. Wenn ja, welche?
            2. Wenn nein, warum nicht?
    b. Welches Unternehmen bzw. welche interne Stelle führte dieses Audit durch?
        i. Wurde hier eine Ausschreibung getätigt?
            1. Wenn nein, warum nicht?

c. Wie wurde die Cybersecurity-Ausstattung (sowohl technisch als auch personell) des BMEIA bewertet?
    i. 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.
    ii. Welche Empfehlungen wurden in der Folge des Audits ausgesprochen?
        1. 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.
        2. 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?

d. Wie wurden die zum damaligen Zeitpunkt bereits getroffenen Maßnahmen und Vorkehrungen zur IKT-Sicherheit im Rahmen des Audits bewertet?
    i. Welche Maßnahmen bzw. Vorkehrungen wurden als ausreichend bewertet? Welche nicht? Bitte jeweils für ausreichende und nicht ausreichende Maßnahmen/Vorkehrungen um getrennte Auflistung.
    ii. Welche Empfehlungen wurden in der Folge des Audits ausgesprochen?
        1. 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.
        2. 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?

2. Ist das nächste Cybersecurity-Audit am BMEIA bereits geplant?
    a. Wenn ja, wer wird dieses Audit durchführen?
    b. Wenn ja, wann wird es durchgeführt
    c. Wenn nein, warum ist ein solches Audit - insbesondere in Anbetracht des letzten Cyberangriffs - nicht geplant?
3. Wurden von den intern für Cybersecurity bzw. IT-Sicherheit zuständigen Personen bzw. Abteilungen des BMEIA Maßnahmen zur Erhöhung der IKT-Sicherheit vorgeschlagen?
    a. Wenn ja, wann genau?
    b. Wenn ja, wurden diese Vorschläge jährlich vorgebracht?
4. Falls solche Maßnahmen von den intern für Cybersecurity bzw. IT-Sicherheit zuständigen Personen bzw. Abteilungen vorgeschlagen wurden, waren folgende Maßnahmen in den Vorschlägen enthalten?
    a. SSL-Interception?
        i. Welche Kosten wurden hierfür veranschlagt?
        ii. Welcher personelle Aufwand wurde hierfür veranschlagt?
        iii. Welche Priorität kam dieser Maßnahme zu?
        iv. Wurde die Maßnahme umgesetzt?

1. Wenn ja, wann?
2. Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
3. Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
4. Wenn nein, warum nicht?

b. Einführung einer Security-Information and Event-Management-Lösung?
   i. Welche Kosten wurden hierfür veranschlagt?
   ii. Welcher personelle Aufwand wurde hierfür veranschlagt?
   iii. Welche Priorität kam dieser Maßnahme zu?
   iv. Wurde die Maßnahme umgesetzt?
      1. Wenn ja, wann?
      2. Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
      3. Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
      4. Wenn nein, warum nicht?

c. Active-Threat-Protection bei E-Mails?
   i. Welche Kosten wurden hierfür veranschlagt?
   ii. Welcher personelle Aufwand wurde hierfür veranschlagt?
   iii. Welche Priorität kam dieser Maßnahme zu?
   iv. Wurde die Maßnahme umgesetzt?
      1. Wenn ja, wann?
      2. Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
      3. Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
      4. Wenn nein, warum nicht?

d. Planung/Aufbau eines sicheren, abgeschotteten Systems?
   i. Welche Kosten wurden hierfür veranschlagt?
   ii. Welcher personelle Aufwand wurde hierfür veranschlagt?
   iii. Welche Priorität kam dieser Maßnahme zu?
   iv. Wurde die Maßnahme umgesetzt?
      1. Wenn ja, wann?
      2. Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
      3. Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
      4. Wenn nein, warum nicht?

e. Zentraler Internetzugang?
   i. Welche Kosten wurden hierfür veranschlagt?
   ii. Welcher personelle Aufwand wurde hierfür veranschlagt?
   iii. Welche Priorität kam dieser Maßnahme zu?
   iv. Wurde die Maßnahme umgesetzt?
      1. Wenn ja, wann?

2. Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
3. Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
4. Wenn nein, warum nicht?

f. Penetrationstest zur Erkennung von Sicherheitsschwachstellen?
   i. Welche Kosten wurden hierfür veranschlagt?
   ii. Welcher personelle Aufwand wurde hierfür veranschlagt?
   iii. Welche Priorität kam dieser Maßnahme zu?
   iv. Wurde die Maßnahme umgesetzt?
      1. Wenn ja, wann?
      2. Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
      3. Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
      4. Wenn nein, warum nicht?

g. Audit der Zentrale?
   i. Welche Kosten wurden hierfür veranschlagt?
   ii. Welcher personelle Aufwand wurde hierfür veranschlagt?
   iii. Welche Priorität kam dieser Maßnahme zu?
   iv. Wurde die Maßnahme umgesetzt?
      1. Wenn ja, wann?
      2. Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
      3. Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
      4. Wenn nein, warum nicht?

h. Abspeicherung sensibler Daten im Elektronischen Akt?
   i. Welche Kosten wurden hierfür veranschlagt?
   ii. Welcher personelle Aufwand wurde hierfür veranschlagt?
   iii. Welche Priorität kam dieser Maßnahme zu?
   iv. Wurde die Maßnahme umgesetzt?
      1. Wenn ja, wann?
      2. Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
      3. Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
      4. Wenn nein, warum nicht?

i. Intrusion-Detection/Intrusion-Prevention-System?
   i. Welche Kosten wurden hierfür veranschlagt?
   ii. Welcher personelle Aufwand wurde hierfür veranschlagt?
   iii. Welche Priorität kam dieser Maßnahme zu?
   iv. Wurde die Maßnahme umgesetzt?
      1. Wenn ja, wann?
      2. Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?

3. Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
4. Wenn nein, warum nicht?

j. Awareness-Training für sämtliche Mitarbeiter_innen?
   i. Welche Kosten wurden hierfür veranschlagt?
   ii. Welcher personelle Aufwand wurde hierfür veranschlagt?
   iii. Welche Priorität kam dieser Maßnahme zu?
   iv. Wurde die Maßnahme umgesetzt?
      1. Wenn ja, wann?
      2. Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
      3. Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
      4. Wenn nein, warum nicht?

k. 2-Faktor-Authentifizierung an den IT-Arbeitsplätzen?
   i. Welche Kosten wurden hierfür veranschlagt?
   ii. Welcher personelle Aufwand wurde hierfür veranschlagt?
   iii. Welche Priorität kam dieser Maßnahme zu?
   iv. Wurde die Maßnahme umgesetzt?
      1. Wenn ja, wann?
      2. Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
      3. Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?

l. Neuaufsetzung der Arbeitsplätze?
   i. Welche Kosten wurden hierfür veranschlagt?
   ii. Welcher personelle Aufwand wurde hierfür veranschlagt?
   iii. Welche Priorität kam dieser Maßnahme zu?
   iv. Wurde die Maßnahme umgesetzt?
      1. Wenn ja, wann?
      2. Wenn ja, von welchem Unternehmen bzw. von welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
      3. Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
      4. Wenn nein, warum nicht?

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

5. 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?
    a. Wann wurden diese vorgeschlagen?
    b. Welche Kosten wurden jeweils pro Maßnahme veranschlagt?
    c. Welcher personelle Aufwand wurde jeweils pro Maßnahme veranschlagt?
    d. Welche Priorität kam den Maßnahmen jeweils zu?
    e. Wurden die Maßnahmen jeweils umgesetzt?
        i. Wenn ja, wann?
        ii. Wenn ja, von welchem Unternehmen bzw. welcher internen Stelle? Wurde hier eine Ausschreibung getätigt? Wenn nein, warum nicht?
        iii. Wenn ja, wurden die veranschlagten Kosten über- bzw. unterschritten?
        iv. Wenn nein, warum die jeweiligen Maßnahmen nicht umgesetzt?
6. Wurde im BMEIA - neben der Implementierung von einzelnen Sicherheitsmaßnahmen - auch ein umfassendes Konzept zu Cybersecurity erarbeitet?
    a. Wenn ja, von wem?
    b. Wenn ja, wann?
    c. Wenn ja, welche Punkte umfasst dieses Konzept?
    d. Wurde Personal eigens für die Einhaltung bzw. Umsetzung dieses Konzepts eingesetzt bzw. ist dies in Planung? War bzw. ist hierfür zusätzliches Personal vorgesehen?
    e. Wenn nein, warum nicht?
        i. Ist die Ausarbeitung eines solchen Konzepts in Anbetracht des letzten Cyberangriffs auf das BMEIA in Planung? Wenn nein, warum nicht?

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-07-04T18:55:06+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.	