3249/J XXVII. GP

Eingelangt am 02.09.2020

Anfrage

der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen an den Bundesminister für europäische und internationale Angelegenheiten betreffend Konsequenzen aus Cyberattacke im Februar 2020

Im Jänner 2020 wurde bekannt, dass zu dieser Zeit ein gezielter und hochprofessioneller Cyberangriff auf das österreichische Außenministerium stattfand. Dieser Angriff offenbarte ernstzunehmende Schwachstellen in der Sicherheits- bzw. Verteidigungsarchitektur der Republik, beeinträchtigte die Integrität und Funktionsfähigkeit einer staatlichen Behörde und schadete damit der nationalen Sicherheit.

In der Beantwortung unserer Anfrage (685/AB) gaben Sie an, dass "*spezifische Sicherheitsvorkehrungen zum Schutze der IKT-Systeme des Ressorts gegen Angriffe iSd § 118a Strafgesetzbuch (StGB) eingesetzt*" würden. Nun ist einer so kritischen Infrastruktur die Sicherheit naturgemäß essenziell. Umso wichtiger sind daher besonders nach einem erfolgten Angriff die Schlussfolgerungen und Lehren, die daraus gezogen wurden, um gegen erneute Attacken verlässlich gewappnet zu sein. Im Interesse der nationalen Sicherheit müssen daher eine umfassende Fehleranalyse und die entsprechenden Konsequenzen daraus gewährleistet und zuverlässig kontrolliert werden.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

1. Welche Fehler und Sicherheitslücken wurden seit Bekanntwerden des Angriffs entdeckt und analysiert?
    a. Welche Konsequenzen zogen Sie daraus?
    b. Bitte um Erläuterung der jeweils entsprechenden Vorgangsweise.
2. Welche konkreten Maßnahmen wurden seit Bekanntwerden des Angriffes a.) geplant und b.) umgesetzt, um die Verteidigungsfähigkeit und Sicherheit der Republik im Cyberbereich zu verbessern?
3. Welche konkreten Abwehrmaßnahmen und Schritte wurden jeweils wann genau zur Analyse, Bekämpfung und Abwehr des Angriffs von wem getroffen und mit

welchem konkreten Ergebnis/Erfolg? (Bitte um detaillierte Erläuterung und Unterscheidung der Maßnahmen **vor** sowie **nach** Bekanntwerden des Angriffs.)

4. Welche (Zeit-)Aufwendungen sind Ihrem Ressort durch die Analyse, Bekämpfung und Abwehr des Angriffs bisher entstanden? (Bitte um detaillierte Erläuterung und Unterscheidung der Maßnahmen **vor** sowie **nach** Bekanntwerden des Angriffs.)
5. Welche bezifferbaren Kosten sind Ihrem Ressort seit Bekanntwerden des Angriffs durch die Analyse, Bekämpfung und Abwehr des Angriffs bisher entstanden?
6. Welche Stellen und wie viele Personen Ihres Ressort sind bzw. waren in die Analyse, Bekämpfung und Abwehr des Angriffes in welcher Weise und wann jeweils eingebunden?
7. Welche externen Experten bzw. Unternehmen wurden für die Analyse, Bekämpfung und Abwehr des Angriffes in welcher Weise und wann jeweils zugezogen?
8. Verfügt Ihr Ressort über einen Rahmenvertrag mit externen Exptert_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 Interpellationsrechts ersucht. Allenfalls ersuchen die Abgeordneten um eine Beantwortung in klassifizierter Weise nach dem Bundesgesetz über die Informationsordnung des Nationalrates und des Bundesrates - InfOG.