11863/AB
vom 14.11.2022 zu 12152/J (XXVII. GP)

Bundesministerium
Bildung, Wissenschaft
und Forschung

bmbwf.gv.at

+43 1 531 20-0
Minoritenplatz 5, 1010 Wien

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2022-0.661.849

Die schriftliche parlamentarische Anfrage Nr. 12152/J-NR/2022 betreffend Vorbereitung auf Cyberangriffe innerhalb der österreichischen Bundesverwaltung, die die Abgeordneten zum Nationalrat Katharina Kucharowits, Kolleginnen und Kollegen am 14. September 2022 an mich richteten, darf ich anhand der mir vorliegenden Informationen wie folgt beantworten:

Zu Frage 1:

- *Gab es in Ihrem Ressort bereits Cyberangriffe?*
  Falls ja, bitte um detaillierte Schilderung des Angriffs/der Angriffe, welche Schäden daraus resultierten und welche Gegenmaßnahmen ergriffen wurden?

Das Bundesministerium für Bildung, Wissenschaft und Forschung sieht sich, wie auch andere Ministerien, Unternehmen und Bildungseinrichtungen, kontinuierlichen Angriffsversuchen im Cyberraum ausgesetzt. Im Bundesministerium für Bildung, Wissenschaft und Forschung konnten bisher derartige Angriffsversuche abgewehrt sowie Ausfälle hintangehalten werden.

Die IKT-Sicherheit wird im Bund als fortlaufender Prozess verstanden. Dementsprechend werden, unterstützt durch das Governmental Computer Emergency Response Team (GovCERT, angesiedelt im Bundeskanzleramt) und die fachlich zuständigen Ressorts, kontinuierlich Anpassungen der IKT-Sicherheitsstruktur vorgenommen, um auf sich ändernde Bedrohungen rasch reagieren zu können.

Zu Frage 2:

- *Welche Rolle und welche konkreten Aufgaben fallen Ihrem Ressort in der gesamtstaatlichen Bekämpfung von Cyberkriminalität zu?*

Die Aufgabenwahrnehmung zur Bekämpfung von Cyberkriminalität obliegt dem Bundesministerium für Inneres, dem Bundesministerium für Justiz sowie dem Bundesministerium für Landesverteidigung.

Im Bundesministerium für Bildung, Wissenschaft und Forschung ist das gemäß der Geschäftseinteilung zuständige Referat für Cybersicherheit verantwortlich, das folgende Aufgaben wahrnimmt: Internes (Cyber-)Sicherheitsmanagement sowie Informationsaustausch bzw. Schnittstelle zu NIS Behörde, govCERT, ATC-gov, Arbeitsgruppen aus dem tertiären Bildungsbereich, Cyber Sicherheitssteuerungsgruppe CSS bzw. Cyber Sicherheitsplattform (CSP).

Zu Frage 3:

- *Ergreift Ihr Ressort aktiv konkrete Maßnahmen, um sich präventiv gegen Cyberattacken und Cyberkriminalität angemessen zu schützen?*
  a. Falls ja, welche Maßnahmen sind das im Detail?
  *b. Falls ja, wird in der Vorbereitung auf einen potenziellen Cyberangriff auch die Expertise externer Expert*innen, etwas* [sic] *Personen auf* [sic] *Wissenschaft oder Zivilgesellschaft, hinzugezogen?*
  c. Falls nein, warum gibt es keine Pläne, sich für den Ernstfall eines potenziellen Cyberangriffs zu schützen?

Im Bundesministerium für Bildung, Wissenschaft und Forschung werden zur Gewährleistung der Cybersicherheit Maßnahmen auf strategischer, operativer und technischer Ebene auf dem Stand der aktuellen Technik ergriffen. Das Ministerium bedient sich zur Überprüfung der getroffenen Maßnahmen auch externer (Security-)Unternehmen. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Technikern des Ressorts zeitnahe umgesetzt.

Darüber hinaus muss von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus gemäß Netz- und Informationssystemsicherheitsgesetz (NISG), BGBl. I Nr. 111/2018, aber auch der Auflistung einzelner im Einsatz befindlicher Cybersicherheitsprodukte, im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen, Abstand genommen werden.

Nicht unerwähnt sollte jedoch bei dieser Thematik bleiben, dass sich auch österreichische Universitäten am Forschungsbereich Cyber Security weltweit in führender Rolle beteiligen.

Zu Frage 4:

- *Durch die unterschiedlichen Zuständigkeitsbereiche aller Ressorts der Bundesregierung ergeben sich auch unterschiedliche Risiken in Bezug auf Cyberangriffe, beispielsweise wird es im Bundesministerium für europäische und internationale Angelegenheiten aller Wahrscheinlichkeit nach andere Herausforderungen und Risiken in Bezug auf Cyberkriminalität geben als beispielweise im Bundesministerium für Justiz.*
  a. Gab es eine ressortspezifische Risikoanalyse in Ihrem Ressort?
  i. Falls nein, warum nicht?
  b. Welche konkreten Maßnahmen setzen Sie, um den spezifischen Risiken Ihres Ressorts gerecht zu werden?

Im Bundesministerium für Bildung, Wissenschaft und Forschung werden die individuellen Risiken vor allem aus den Bereichen Datenschutz und IT-Sicherheit einem laufenden Monitoring unterzogen. Identifizierten Risiken wird mittels geeigneter technischer und organisatorischer Maßnahmen gegengesteuert.

Im Zuge der Umsetzung der NIS RL (Richtlinie (EU) 2016/1148, über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystem) durch das NISG wurden die kritischen Dienste identifiziert und mit entsprechenden Prozessen zur Aufrechterhaltung bzw. zur Weiterführung der Kernaufgaben nach Systemausfällen hinterlegt.

Darüber hinaus darf auf die Beantwortung der Fragen 1 und 3 verwiesen werden.

Zu Frage 5:

- *Gibt es eine Person oder einen Personenkreis in Ihrem Ressort, die dezidiert als „Cybersichterheitsbeauftrage(r)" fungiert/fungieren?*
  a. Falls ja, wie viele Personen sind zum Zeitpunkt der Beantwortung dieser Anfrage im Bereich Cybersecurity in Ihrem Ressort beschäftigt?
  b. Falls ja, über welche Expertise verfügt/verfügen diese Person(en)?
  c. Falls nein, warum gibt es keine(n) „Cybersicherheitsbeauftrage(n)" in Ihrem Ressort?

Die genannten bzw. vergleichbaren Aufgaben werden vom zuständigen Referat wahrgenommen.

Dazu gehören die Stärkung des Bewusstseins für IT-Sicherheit im Managementbereich, die Einbringung von IT-Sicherheits-Projektanträgen, die Gewährleistung der IT-Sicherheit im laufenden Betrieb sowie die Durchführung der notwendigen Risikoanalysen und Bewertungen und daraus folgende Maßnahmenableitung.

Darüber hinaus kann auf einzelne Personen im Hinblick auf den Schutz vor Ausspähung und der Sicherung der Effektivität der Maßnahmen nicht eingegangen werden.

Zu Frage 6:

- *Bietet Ihr Ressort spezielle Trainings, Webinare, Kurse etc. an, um alle Mitarbeiter*innen im Umgang mit potenziellen Cyberangriffen und der daraus resultierenden Gefahrenlage zu sensibilisieren?*

Im Bundesministerium für Bildung, Wissenschaft und Forschung erfolgt im Rahmen der Grundausbildung eine grundlegende Schulung im Rahmen des Fachs Datenschutz und IT-Sicherheit. Darüber hinaus informiert die zuständige IKT-Abteilung routinemäßig und proaktiv zu Cybersicherheitsthemen inklusive konkreter Handlungsanleitungen. Weiters werden Angebote für Schulungen des Bundesministeriums für Inneres für oberste Organe in Anspruch genommen.

- *Die folgenden Fragen ergeben sich aus dem Bericht des Rechnungshofs (https://bit.ly/3cEOpHK), der einigen Aufholbedarf im Bereich der Cybersicherheit verortet.*

Zu den Fragen 7 und 8:

- *Der Rechnungshofbericht bemängelt unter anderem, dass Krisen-, Kontinuitäts- und Einsatzpläne in Bezug auf Cybersicherheit gänzlich fehlen. Zum Zeitpunkt der Beantwortung dieser Anfrage, wurden diese von Ihrem Ressort mittlerweile erstellt?*
  a. Falls ja, wurden zur Erstellung dieser Pläne auch externe Expert innen hinzugezogen?*
  b. Falls nein, wann ist mit der Fertigstellung dieser Pläne in Ihrem Ressort zu rechnen?
- *Der Rechnungshof sah zudem die Etablierung eines permanent verfügbaren Cyber-Einsatzteam („Rapid Response Team") sowie die Schaffung eines ebenso permanenten Cyberlagezentrums zur Bearbeitung von Notfällen als essentiell. Wurden dieses Einsatzteam und das Lagezentrum zum Zeitpunkt der Beantwortung dieser Anfrage bereits geschaffen?*
  a. Falls ja, in welchem Ressort sind diese Strukturen angesiedelt und der Zuständigkeit welcher/welchen Bundesministerin/Bundesministers unterliegen diese?

Im Bundesministerium für Bildung, Wissenschaft und Forschung werden Handbücher und standardisierte Vorgehensweisen für diverse IT-Notfallszenarien für die Infrastruktur im Rahmen eines kontinuierlichen Verbesserungsprozesses angepasst bzw. weiterentwickelt.

Das Bundesministerium für Bildung, Wissenschaft und Forschung war nicht direkt von diesem Bericht des Rechnungshofes adressiert. Es darf daher auf die Beantwortung der Parlamentarischen Anfragen Nr. 12156/J-NR/2022, Nr. 12157/J-NR/2022, Nr. 12154/J-NR/2022 und Nr. 12148/J-NR/2022, jeweils vom 14. September 2022, durch die jeweiligen Mitglieder der Bundesregierung verwiesen werden (insbesondere auch hinsichtlich des Rapid Response Teams und des Cyberlagezentrums).

Zu Frage 9:

- *Zudem forderte der Rechnungshof ein regelmäßig zu erstellendes Cyber-Lagebild, um laufende Bedrohungen und potentielle Gefahrenquellen schneller und effektiver zu identifizieren. Wird ein solches Cyberlagebild in Ihrem Ressort zum Zeitpunkt der Beantwortung dieser Anfrage bereits regelmäßig erstellt?*
  a. Falls ja, seit wann wird ein solches Lagebild in Ihrem Ressort erstellt und in welchen Abständen findet das statt?
  b. Falls nein, warum wird bisher kein Cyber-Lagebild in Ihrem Ressort erstellt und ab wann planen Sie, ein solches regelmäßig zu erstellen?

Das Bundesministerium für Bildung, Wissenschaft und Forschung ist Empfänger des vom Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK) erstellten gesamtstaatlichen Cyberlagebildes und leitet dementsprechende Maßnahmensetzungen für den eigenen Verantwortungsbereich daraus ab.

Wien, 14. November 2022

Ao. Univ.-Prof. Dr. Martin Polaschek

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR BILDUNG, WISSENSCHAFT UND FORSCHUNG
@ AMTSSIGNATUR

Unterzeichner	Bundesministerium für Bildung, Wissenschaft und Forschung
Datum/Zeit	2022-11-14T09:15:48+01:00
Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
Serien-Nr.	285175223
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.bmbwf.gv.at/verifizierung.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-11-14T09:25:18+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.	