5343/AB
vom 15.04.2021 zu 5366/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: 2021-0.116.514

Die schriftliche parlamentarische Anfrage Nr. 5366/J-NR/2021 betreffend Einsatz von Solarwinds-Software, die die Abg. Mag. Selma Yildirim, Kolleginnen und Kollegen am 15. Februar 2021 an mich richteten, wird wie folgt beantwortet:

Zu Frage 1:

- *Sind Ihnen die Hackerangriffe auf den Softwareanbieter Solarwinds bekannt?*

Die Angriffe auf den Softwareanbieter Solarwinds, das operative Vorgehen der Angreifer, sowie die Folgewirkungen auf die Kunden des Softwareanbieters sind im Bundesministerium für Bildung, Wissenschaft und Forschung bekannt.

Zu Fragen 2 und 4:

- *Welche Konsequenzen haben Sie daraus für Ihr Ressort gezogen?*
- *Haben Sie sich bezüglich der Angriffe auf Solarwinds mit AmtskollegInnen in- und außerhalb der EU ausgetauscht und ein gemeinsames Vorgehen dagegen besprochen?*
  a) Wenn ja, mit welchen?
  b) Welche Maßnahmen waren die Folge?

Dazu wird auf die Beantwortung der Parlamentarischen Anfrage Nr. 5354/J-NR/2021 durch den Herrn Bundeskanzler verwiesen.

Zu Fragen 3 und 5 bis 7:

- *Haben Sie eine Schadensanalyse vorgenommen?*
  a) Wenn ja, mit welchem Ergebnis?
  b) Wenn nein, warum nicht?
- *Nutzte oder nutzt Ihr Ressort Produkte des Softwareanbieters Solarwinds?*
  a) Ist es dadurch zu unberechtigten Zugriffen auf Systeme des Ressorts gekommen?

- *Welche Ihrem Ressort zugeordneten Bundesbehörden nutzen oder nutzen Produkte des Softwareanbieters Solarwinds?*
  a) Ist es dadurch zu unberechtigten Zugriffen auf Systeme der Bundesbehörden gekommen?
- *Waren Ihr Ressort oder diesem zugeordnete Bundesbehörden [sic!] von dem Hackerangriff betroffen?*
  a) Wenn ja, welche?
  b) In welchem Ausmaß?

Im Bundesministerium für Bildung, Wissenschaft und Forschung wird keine Software des Anbieters Solarwinds eingesetzt. Das Bundesministerium für Bildung, Wissenschaft und Forschung war von dem Angriff auf die Firma Solarwinds nicht betroffen.

In Bezug auf den nachgeordneten Bereich einschließlich der in Trägerschaft des Bundes befindlichen mittleren und höheren Bundesschulen erfolgt die Beschaffung unter anderem von Software eigenverantwortlich im Zuständigkeitsbereich vor Ort. Die jeweils eingesetzte Software unterliegt keinen zentralen Vorgaben des Bundesministeriums für Bildung, Wissenschaft und Forschung. Eine Beantwortung der Fragestellungen nach eingesetzten bzw. eingesetzt gewesenen Produkten des genannten Softwareanbieters würde eine detaillierte Erhebung im nachgeordneten Bereich österreichweit erforderlich machen. Derartiges wäre mit einem erheblichen, unter anderem den mehr als 500 Bundesschulstandorten nicht zumutbaren Verwaltungsaufwand verbunden. Vor diesem Hintergrund wird um Verständnis ersucht, dass eine Beantwortung in diesem Teilbereich aus verwaltungsökonomischen Gründen nicht möglich ist. Jedenfalls liegen dem Bundesministerium für Bildung, Wissenschaft und Forschung mit Stichtag der Anfragestellung keine Informationen vor, dass sein nachgeordneter Bereich von gegenständlichem Angriff betroffen gewesen wäre.

Zu Fragen 8 und 9:

- *Wurden in Folge des Öffentlich-werdens des Hackerangriffs zusätzliche Sicherheitsmaßnahmen getroffen?*
  a) Wenn ja, welche?
  b) Wenn nein, warum nicht?
- *Wie stellen Sie den Schutz Ihres Ressorts und diesem zugeordneter Bundesbehörden [sic!] gegen Hackerangriffe sicher?*

IKT-Sicherheit wird als fortlaufender Prozess verstanden. Dementsprechend werden kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur vorgenommen und IKT-Sicherheitsprojekte zeitnahe abgewickelt. Dies betrifft sowohl die Beschaffung von IKT-Sicherheitsinfrastruktur, die State-of-the-Art ist, als auch die permanente Evaluierung und Anpassung der Prozesse. Darüber hinaus werden basierend auf den aktuellen Bedrohungslagen Maßnahmen zur Hebung der Awareness durchgeführt. Erkenntnisse aus

dem gesamtstaatlichen Lagebildprozess entlang den strategischen Handlungsempfehlungen des Bundeskanzleramts werden in Zusammenarbeit mit der Technik des Bundesministeriums 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), oder aber auch der Auflistung einzelner im Einsatz befindlicher Softwareprodukte im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden. Das Bundesministerium für Bildung, Wissenschaft und Forschung setzt strategische Handlungsempfehlungen des Bundeskanzleramts regelmäßig um.

Wien, 15. April 2021
Der Bundesminister:

Univ.-Prof. Dr. Heinz Faßmann eh.

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR BILDUNG, WISSENSCHAFT UND FORSCHUNG @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Bildung, Wissenschaft und Forschung
	Datum/Zeit	2021-04-15T12:31:41+02:00
	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	2021-04-15T12:37:44+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.	