5153/AB
vom 26.03.2021 zu 5360/J (XXVII. GP)

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

bmk.gv.at

Leonore Gewessler, BA
Bundesministerin

leonore.gewessler@bmk.gv.at
+43 1 711 62-658000
Radetzkystraße 2, 1030 Wien
Österreich

An den
Präsident des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 W i e n

Geschäftszahl: 2021-0.119.416

26 . März 2021

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Mag.[a] Yildirim, Genossinnen und Genossen haben am 15. Februar 2021 unter der **Nr. 5360/J** an mich eine schriftliche parlamentarische Anfrage betreffend Einsatz von Solarwinds-Software gerichtet.

Diese Anfrage beantworte ich wie folgt:

Zu Frage 1:

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

Ja. Die Angriffe auf den Softwareanbieter Solarwinds sind bekannt.

Zu den 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?*

Es wurde geprüft, in welchem Ausmaß das Ressort (Zentralstelle) betroffen ist. Die Überprüfung ergab, dass die Software des Anbieters Solarwinds nicht produktiv eingesetzt wird und es wurden diesbezüglich auch keine unberechtigten Zugriffe festgestellt.

Weiters wurde mit Bekanntwerden der Angriffe durch den IKDOK (Innerer Kreis der operativen Koordinierungsstruktur § 3 Z 4 Netz- und Informationssystemsicherheitsgesetz BGBl. I Nr. 111/2018 – NISG) eine gesamtstaatliche Risikoanalyse durchgeführt. Im Wege des IKDOK-Lagebildprozesses fand auch ein Austausch mit einer Vielzahl nationaler und internationaler Expert_innen statt.

Seitens des Österreichischen Patentamtes wurde mitgeteilt, dass nach einer Schadensanalyse mit Solarwind direkt Kontakt aufgenommen wurde. Es wurden präventive Maßnahmen von Solarwinds zur Vermeidung von Sicherheitsrisiken und Lücken in der Zukunft besprochen. Zudem wurden Consultingleistungen durch auf Monitoring & Security spezialisierte Unternehmen in Anspruch genommen. Daraus resultierend soll eine Entscheidungsgrundlage für den fortbestehenden Einsatz dieser Software in Zukunft getroffen werden.

Zu den Fragen 3, 5 und 6:

- *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 nutzten oder nutzen Produkte des Softwareanbieters Solarwinds?*
    a) *Ist es dadurch zu unberechtigten Zugriffen auf Systeme der Bundesbehörden gekommen?*

Seitens der für die Zentralstelle des BMK zuständigen ho. IKT-Abteilung wird und wurde produktiv keine Software des Anbieters Solarwinds genutzt.
Es wurde für Testzwecke eine Demo-Version einer Software von Solarwinds getestet, um sich ein Bild von der Funktionalität zu machen. Ein Produktiveinsatz dieser Demo-Version hat aber nicht stattgefunden.
Eine Überprüfung der Systeme ergab, dass im Zusammenhang mit dem Angriff auf die Firma Solarwinds kein unberechtigter Zugriff festgestellt wurde und dem BMK daher kein Schaden entstand.

Seitens des Österreichischen Patentamtes wurde mitgeteilt, dass die betroffenen Softwareversionen (2019.4 bis 2020.2.1.) do. nicht im Einsatz waren.
Bei der derzeit im Einsatz befindlichen Softwareversion 2016.1.5300 wurde mithilfe des Solarwinds Support Teams eine Analyse durchgeführt. Da es sich hierbei jedoch um eine ältere Softwareversion handelte, war diese nicht betroffen.

Zu Frage 7:

- *Waren Ihr Ressort oder diesem zugeordnete Bundesbehörden von dem Hackerangriff betroffen?*
    a) *Wenn ja, welche?*
    b) *In welchem Ausmaß?*

Nein.

Zu den 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 gegen Hackerangriffe sicher?*

IKT-Sicherheit wird als fortlaufender Prozess verstanden. Dementsprechend werden im risikobasierten Ansatz kontinuierlich Anpassungen an der IKT -Sicherheitsstruktur vorgenommen. Dies betrifft sowohl die Beschaffung von IKT- Sicherheitsinfrastruktur als auch die permanente Evaluierung und Anpassung der Prozesse. Außerdem werden basierend auf den aktuellen Bedrohungslagen Maßnahmen zur Hebung der Awareness durchgeführt. Erkenntnisse aus dem gesamtstaatlichen Lagebildprozess werden in Zusammenarbeit mit den Techniker_innen des Ressorts zeitnahe umgesetzt.

Darüber hinaus muss von der detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus oder auch von der Auflistung einzelner im Einsatz befindlicher Softwareprodukte im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Leonore Gewessler, BA

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR KLIMASCHUTZ, UMWELT, ENERGIE, MOBILITÄT, INNOVATION UND TECHNOLOGIE @ AMTSSIGNATUR	Hinweis	Dieses Dokument wurde amtssigniert.
	Datum	2021-03-26T16:18:14+01:00
	Seriennummer	1871969199
	Aussteller-Zertifikat	CN=a-sign-corporate-05,OU=a-sign-corporate-05,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at/

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2021-03-26T16:21:13+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.	