

Dr.ⁱⁿ Alma Zadić, LL.M.
Bundesministerin für Justiz

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2021-0.120.388

Ihr Zeichen: BKA - PDion (PDion)5357/J-NR/2021

Wien, am 15. April 2021

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Mag.a Selma Yildirim, Kolleginnen und Kollegen haben am 15. Februar 2021 unter der Nr. **5357/J-NR/2021** an mich eine schriftliche parlamentarische Anfrage betreffend „Einsatz von Solarwinds-Software“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zur Frage 1:

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

Ja. Die Angriffe auf den Softwareanbieter Solarwinds, das operative Vorgehen der Angreifer, sowie die Folgewirkungen auf die Kunden des Softwareanbieters sind bekannt.

Zur Frage 2:

- *Welche Konsequenzen haben Sie daraus für Ihr Ressort gezogen?*

Auf Basis der durch den IKDOK (Innerer Kreis der operativen Koordinierungsstruktur § 3 Z 4 Netz- und Informationssystemssicherheitsgesetz BGBl. I Nr. 111/2018 – NISG) bereitgestellten Informationen wurde die aktuelle IT-Sicherheitsstruktur einer Routineüberprüfung unterzogen, woraus sich keine weiteren Folgeaktivitäten für das Justizressort als notwendig herausgestellt haben.

Zu den Fragen 3, 5 und 6:

- *3. Haben Sie eine Schadensanalyse vorgenommen?
a) Wenn ja, mit welchem Ergebnis?
b) Wenn nein, warum nicht?*
- *5. Nutzte oder nutzt Ihr Ressort Produkte des Softwareanbieters Solarwinds?
a) Ist es dadurch zu unberechtigten Zugriffen auf Systeme des Ressorts gekommen?*
- *6. Welche Ihrem Ressort zugeordneten Bundesbehörden nutzen oder nutzen Produkte des Softwareanbieters Solarwinds?
a) Ist es dadurch zu unberechtigten Zugriffen auf Systeme der Bundesbehörden gekommen?*

Im Verantwortungsbereich des Bundesministeriums für Justiz ist das Produkt Solarwinds Orion Business Software nicht in Verwendung.

Zur Frage 4:

- *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?*

Der Austausch in- und außerhalb der EU erfolgt zentral über den IKDOK, die entsprechenden Erkenntnisse wurden dem BMJ zur Kenntnis gebracht (siehe Antwort zu Frage 2).

Zur Frage 7:

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

Nein, das BMJ oder in dessen Verantwortungsbereich liegende Behörden und Dienststellen waren von dem Hackerangriff auf die Firma Solarwinds nicht betroffen.

Zu den Fragen 8 und 9:

- *8. Wurden in Folge des Öffentlich-werdens des Hackerangriffs zusätzliche Sicherheitsmaßnahmen getroffen?
a) Wenn ja, welche?
b) Wenn nein, warum nicht?*

- *9. Wie stellen Sie den Schutz Ihres Ressorts und diesem zugeordneter Bundesbehörden gegen Hackerangriffe sicher?*

IKT-Sicherheit wird als fortlaufender Prozess verstanden. Dementsprechend werden gemeinsam mit dem BRZ, dem zentralen IKT-Dienstleister der Justiz, kontinuierlich Anpassungen an der IKT -Sicherheitsstruktur vorgenommen.

Dies betrifft sowohl die Beschaffung von IKT- Sicherheitsinfrastruktur, die State-of-the-Art ist, als auch die permanente Evaluierung und Anpassung der Prozesse.

Von einer detaillierten Auflistung der Maßnahmen zur Erhöhung bzw. dem Erhalt eines hohen IKT- Sicherheitsniveaus gemäß NISG sowie einer Auflistung einzelner im Einsatz befindlicher Softwareprodukte muss zur Sicherung der weiteren Effektivität der Schutzmaßnahmen Abstand genommen werden.

Dr.ⁱⁿ Alma Zadić, LL.M.

