5366/AB
vom 15.04.2021 zu 5354/J (XXVII. GP)

Bundeskanzleramt

bundeskanzleramt.gv.at

Sebastian Kurz
Bundeskanzler

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2021-0.116.640

Wien, am 15. April 2021

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Mag. Yildrim, Kolleginnen und Kollegen haben am 15. Februar 2021 unter der Nr. **5354/J** eine schriftliche parlamentarische Anfrage betreffend „Einsatz von Solarwinds-Software“ an mich gerichtet.

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

Zu Frage 1:

1. *Sind Ihnen die Hackerangriffe auf den Softwareanbieter Solarwinds bekannt?*

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

Zu Frage 2:

2. *Welche Konsequenzen haben Sie daraus für Ihr Ressort gezogen?*

Mit Bekanntwerden der Angriffe Mitte Dezember 2020 wurde durch den IKDOK (Innerer Kreis der operativen Koordinierungsstruktur nach § 3 Z 4 Netz- und Informationssystemsi-

cherheitsgesetz BGBl. I Nr. 111/2018 – NISG) im Wege des Lagebildprozesses eine gesamtstaatliche Risikoanalyse durchgeführt. Als direkte Konsequenz wurde ein Sonderlagebild inklusive Auflistung risikominimierender Maßnahmen erstellt. Dieses wurde sowohl an die Ressorts, die Einrichtungen der öffentlichen Verwaltung als auch an die Betreiber kritischer Infrastruktur verteilt.

Darüber hinaus wurde die Thematik der Supply Chain Attacken als Themenschwerpunkt für Awarenessinformationen identifiziert.

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 Bundeskanzleramts ist das Produkt Solarwinds Orion Business Software nicht in Verwendung. Eine von der gleichnamigen Firma erstellte Software für den Betrieb von FTP Servern kommt im Bunkeskanzleramt zum Einsatz – diese ist nach vorliegenden Informationen nicht vom Angriff betroffen.

Eine Überprüfung der Systeme ergab, dass im Zusammenhang mit dem Angriff auf die Firma Solarwinds kein unberechtigter Zugriff festgestellt wurde. Dem Bundeskanzleramt entstand daher kein Schaden.

Basierend auf den Risikoanalysen des IKDOK wurden die eigenen Systeme entsprechend der empfohlenen Maßnahmen angepasst.

Zu Frage 4:

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?

Im Wege des IKDOK Lagebildprozesses fand ein Austausch mit einer Vielzahl nationaler und internationaler Experten statt. Exemplarisch kann hier das CSIRT-Netzwerk (https://csirts-network.eu/), die European Government CERTs group (http://www.egc-group.org/) sowie das US Federal Bureau of Investigation genannt werden. Darüber hinaus wurden von der für die Entdeckung des Angriffs zuständigen Firma FireEye direkt Informationen eingeholt.

Als Folge konnten zeitnah das Lagebild verdichtet und risikominierende Maßnahmen aggregiert und kommuniziert werden.

Zu Frage 7:

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

Nein, das Bundeskanzleramt oder in dessen Verantwortungsbereich liegende Behörden und Dienststellen waren vom 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 im risikobasierten Ansatz 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. Darüber hinaus werden basierend auf den aktuellen Bedrohungslagen Maßnahmen zur Hebung der Awareness durchgeführt. 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 NISG oder aber auch der Auflistung einzelner im Einsatz befindlicher Softwareprodukte im Hinblick auf die Sicherung der Effektivität der Schutzmaßnahmen Abstand genommen werden.

Sebastian Kurz

REPUBLIK ÖSTERREICH BUNDESKANZLERAMT AMTSSIGNATUR	Unterzeichner	serialNumber=932783133,CN=Bundeskanzleramt,C=AT
	Datum/Zeit	2021-04-15T16:05:11+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bundeskanzleramt.gv.at/verifizierung
	Hinweis	Dieses Dokument wurde amtssigniert.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2021-04-15T16:07:52+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.	