5346/AB
vom 15.04.2021 zu 5365/J (XXVII. GP)

Bundesministerium
Inneres

Karl Nehammer, MSc
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2021-0.196.608

Wien, am 7. April 2021

Sehr geehrter Herr Präsident!

Die Abgeordnete zum Nationalrat Mag.ª Selma Yildirim, Genossinnen und Genossen haben am 15. Februar 2021 unter der Nr. **5365/J** 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 der Folgewirkungen auf die Kunden des Softwareanbieters sind bekannt.

Zur Frage 2:

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

Mit Bekanntwerden der Angriffe Mitte Dezember wurde durch den IKDOK (Innerer Kreis der operativen Koordinierungsstruktur) im Wege des Lagebildprozesses eine gesamtstaatliche Risikoanalyse durchgeführt. Als direkte Konsequenz wurde ein Sonderlagebild inklusive Auflistung risikomitigierender 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, 6 und 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 von dem Hackerangriff betroffen?*
  a. *Wenn ja, welche?*
  b. *In welchem Ausmaß?*

Aus Gründen der Sicherheit können zu im IT -Security Bereich eingesetzten Produkten grundsätzlich keine Angaben gemacht werden. Zu keinem Zeitpunkt bestand jedoch eine der angesprochenen Gefährdungslagen.

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?*

Im Wege des IKDOK Lagebildprozesses fand ein Austausch mit einer Vielzahl nationaler und internationaler Experten statt. Exemplarisch kann hier das CSIRT-Netzwerk (https://csirtsnetwork.eu/), die European Government CERTs group (http://www.egc-group.org/), das Cyber Crisis Liaison Organisation Network (CyCLONE) der EU, sowie das US Federal Bureau of Investigation genannt werden.

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

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 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.

Karl Nehammer, MSc

REPUBLIK ÖSTERREICH AMTSSIGNATUR	Datum/Zeit	2021-04-15T12:42:16+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	148769640
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2021-04-15T12:43:55+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.	