5357/J
vom 15.02.2021 (XXVII. GP)

Anfrage

der Abgeordneten Mag.a Selma Yildirim, Genossinnen und Genossen

an die Bundesministerin für Justiz

betreffend Einsatz von Solarwinds-Software

Rund um den Jahreswechsel 2020-2021 sorgte die Cyberattacke betreffend den Softwareanbieter Solarwinds für Schlagzeilen. Die Frankfurter Allgemeine Zeitung bezeichnete den Angriff aufgrund seiner Dimension gar als „historisch".[1] Der Standard schreibt von einem „Sicherheitsdebakel".[2]

Die Hacker haben sich dadurch Zugriff auf mehr als 250 US-amerikanische Behörden und große Unternehmen wie z.B. Microsoft verschafft und blieben über Monate hinweg unentdeckt.[3]

In Deutschland zeigte sich Anfang des Jahres 2021, dass zahlreiche Behörden, unter anderem das Bundeskriminalamt, das Verkehrsministerium, das Robert Koch-Institut oder der zentrale IT-Dienstleister des Bundes die manipulierte Software genutzt haben.[4]

Wie angreifbar und verletzlich diese Systeme sind, wurde uns dadurch einmal mehr eindrücklich vor Augen geführt.

Die unterzeichneten Abgeordneten richten daher an die Bundesministerin für Justiz nachstehende:

Anfrage

---

[1] Vgl.: https://www.faz.net/aktuell/wirtschaft/digitec/solarwinds-hack-massiver-cyberangriff-gefaehrdet-deutsche-behoerden-17134477.html

[2] Vgl : https://www.derstandard.at/story/2000122586991/solarwinds-passwort-fuer-gehackten-update-server-lautete-solarwinds123

[3] Vgl.: https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html

[4] Vgl.: https://www-spiegel-de.cdn.ampproject.org/c/s/www.spiegel.de/netzwelt/netzpolitik/solarwinds-hack-kompromittierte-software-auch-in-vielen-deutschen-behoerden-im-einsatz-a-2890f2fb-4422-40d2-b9eb-a1dcfe30e64d-amp

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

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

3. Haben Sie eine Schadensanalyse vorgenommen?

a) Wenn ja, mit welchem Ergebnis?

b) Wenn nein, warum nicht?

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?

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?

7. Waren Ihr Ressort oder diesem zugeordnete Bundesbehörden von dem Hackerangriff betroffen?

a) Wenn ja, welche?

b) In welchem Ausmaß?

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?

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2021-02-15T13:10:08+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.	