6376/AB
vom 22.06.2021 zu 6440/J (XXVII. GP)

Bundeskanzleramt

bundeskanzleramt.gv.at

Sebastian Kurz
Bundeskanzler

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2021-0.295.767

Wien, am 22. Juni 2021

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Dr. Oberrauner, Kolleginnen und Kollegen haben am 22. April 2021 unter der Nr. **6440/J** eine schriftliche parlamentarische Anfrage betreffend „Auswirkungen der Sicherheitslücken bei Microsoft Exchange auf Österreichs Wirtschaft und Sicherheit“ an mich gerichtet.

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

Zu den Fragen 1 bis 3:

1. *Wie viele Server sind in Österreich von der Sicherheitslücke bei Microsoft Exchange betroffen?*
2. *Wie viele dieser Server sind bislang mit einem Patch versehen worden?*
3. *Wie viele Hintertüren (Webshells) sind bislang auf den betroffenen Servern aufgespürt worden?*

Als die Sicherheitslücke bei Microsoft Exchange im März 2021 in Österreich bekannt wurde sind durch das Government Computer Emergency Response Team für die öffentliche Verwaltung in Österreich (govCERT) bzw. nationale Computer Emergency Response Team (na-

tionale CERT) 4.196 Server als potentiell betroffen identifiziert worden. Mit Stand Mitte April 2021 wurden 190 Server als tatsächlich kompromittiert identifiziert, 283 Server galten weiterhin als potentiell kompromittiert.

Die Empfehlung zur weiteren Vorgehensweise wurde den potentiell Betroffenen mehrmals übermittelt und liegt nun in der Verantwortung der Systemeigner.

Patches werden durch die jeweiligen Systemeigner selbst eingespielt. Ein zentrales Führen aller Patchstände aller Systeme findet nicht statt und ist mit den dem govCERT / nationalen CERT zur Verfügung stehenden technischen und rechtlichen Mitteln nicht möglich.

Zu Frage 4:

4. *Bis wann sollen alle Server mit einem Patch versehen worden sein?*

Die Warnung des govCERT und des nationalen CERT empfahl bereits am 3. März 2021 allen potentiell Betroffenen, die Patches so schnell wie möglich einzuspielen. Die Warnungen und Informationen zu notwendigen Patches wurden in der Folge kontinuierlich aktualisiert. Die Annahme und Verarbeitung der Informationen bzw. Umsetzung der empfohlenen Maßnahmen liegt in der Verantwortung der Empfänger/Systemeigner.

Zu den Fragen 5 bis 8, 10, 14 und 18:

5. *Waren auch Server staatlicher Einrichtungen (Ministerien, Behörden, Parlamente, Gerichte, Krankenhäuser, Universitäten etc.) auf Bundes-, Landes- und kommunaler Ebene sowie Server weiterer kritischer Infrastrukturen und von Unternehmen der öffentlichen Daseinsvorsorge von der Sicherheitslücke betroffen? Wenn ja, wie viele und in welchen Bereichen?*
6. *Wurden bei diesen Servern auch Webshells gefunden?*
7. *Bis wann konnten bei diesen Servern die Lücken geschlossen und die Webshells entfernt werden?*
8. *Ist es aufgrund installierter Webshells zu Angriffen auf staatliche Einrichtungen, kritische Infrastrukturen und Unternehmen der öffentlichen Daseinsvorsorge gekommen? Wenn ja, zu welchen?*
10. *Welche finanziellen Kosten sind für diese Maßnahmen angefallen? Konnten diese aus dem hierfür vorgesehen Kostenstellen gedeckt werden oder wurden zusätzliche Mittel bereitgestellt?*

14. *Wann und in welcher Form haben Sie die Unternehmerinnen und Unternehmer und ihre Betriebe über die Sicherheitslücke bei Microsoft Exchange, vor Webshells und drohenden Cyberangriffen informiert?*
18. *Welche Kenntnisse besitzen Sie darüber, wer bzw. welche Gruppierung oder Organisation hinter der massenhaften Platzierung von Webshells steckt?*

Zur Betroffenheit von IT-Systemen staatlicher Einrichtungen kann grundsätzlich aus Gründen der Sicherheit keine Auskunft gegeben werden.

Mit den dem govCERT und dem nationalen CERT zur Verfügung stehenden technischen und rechtlichen Mitteln wurden Schwachstellenscans durchgeführt und betroffene Stellen direkt kontaktiert.

Zu Frage 9:

9. *Welche Maßnahmen wurden von Ihnen ergriffen, um die digitale Infrastruktur staatlicher Einrichtungen, kritischer Infrastrukturen und von Unternehmen der öffentlichen Daseinsvorsorge auf Sicherheitslücken und Webshells zu überprüfen und identifizierte Sicherheitslücken und Schadprogramme schnellstmöglich zu beseitigen?*

Die Server wurden mit den von MS zur Verfügung gestellten Tools geprüft und mit Software-Updates versorgt. Dadurch sind weder dem govCERT oder dem nationalen CERT noch dem BKA für diese Maßnahmen zusätzliche Kosten entstanden.

Zu den Fragen 11 und 12:

11. *Wie viele Unternehmen (wie viele davon Kleinst-, Klein- und Mittelständische Unternehmen) sind in Österreich von der Sicherheitslücke, der Platzierung von Webshells und darauf folgenden Angriffen mit Schad- und Spionagesoftware betroffen?*
12. *Ist es aufgrund der Sicherheitslücken und damit verbundener Cyberangriffe in Österreich zu Produktionsausfällen gekommen? Falls ja, in welchen Branchen?*

Ich darf auf meine Beantwortung zu Frage 1 verweisen. Ergänzend darf festgestellt werden, dass die Entgegennahme von Anzeigen und deren strafrechtliche Verfolgung nicht in den Verantwortungsbereich des BKA (govCERT) oder nationalen CERT fällt.

Die Aufgaben von Computernotfallteams (CSIRTs) ergeben sich aus dem § 14 Abs. 2 NISG – die Prozessverantwortlichkeit obliegt jedem CSIRTs selbst. Die Verteilung relevanter Informationen – wie zur vorliegenden Schwachstelle – erfolgt grundsätzlich mehrdimensional und proaktiv.

Zu den Fragen 13 und 15:

13. Auf welche Höhe beläuft sich bislang der volkswirtschaftliche Schaden?

15. Wann, in welcher Form und in welchem Zeitraum haben Sie betroffenen Unternehmen Ihre Hilfe bei der Sicherung ihrer digitalen Infrastruktur angeboten?

Ich ersuche um Verständnis, dass diese Fragen nach den Bestimmungen des Bundesministeriengesetzes 1986 in der nunmehr geltenden Fassung, BGBl. I Nr. 30/2021, nicht Gegenstand meines Vollzugsbereiches sind und somit nicht beantwortet werden können.

Zu Fragen 16:

16. Wie viele Personen sind damit in Ihrem Ministerium befasst und welche finanziellen Mittel wurden hierfür aus welcher Kostenstelle aufgewendet?

Es wurde mit den Ressourcen der internen IT-Abteilung, die für das zeitnahe Einspielen von Updates und Sicherheitspatches verantwortlich ist, das Auslangen gefunden und keine externe Unterstützung benötigt.

Zu Frage 17:

17. Gibt es von ihrem Ministerium finanzielle Unterstützung für Unternehmen in Österreich, die durch die Sicherheitslücken bei Microsoft Exchange und daraus resultierenden Cyberangriffen einen existenzbedrohenden finanziellen Schaden erlitten haben? Falls ja, in welcher Höhe?

Es gibt keine finanzielle Unterstützung aus dem Titel Koordination Cybersicherheit.

Zu Frage 19:

19. Was wollen Sie unternehmen, um die digitale Infrastruktur im staatlichen und nichtstaatlichen Bereich zukünftig besser vor den Risiken derartiger Sicherheitslücken und massenhafter Cyberattacken zu schützen?

Österreich hat bereits umfassende Strukturen zur Cybersicherheitsvorsorge und Vorfallsbehandlung eingerichtet, welche regulär zur Anwendung kommen. Diese basieren auf gesetzlichen und strategischen Grundlagen. Fortführende Maßnahmen und Prioritäten ergeben sich darüber hinaus aus dem laufenden Regierungsprogramm und der Strategie für die Cybersicherheit 2013, die derzeit aktualisiert wird.

Sebastian Kurz

REPUBLIK ÖSTERREICH BUNDESKANZLERAMT AMTSSIGNATUR	Unterzeichner	serialNumber=932783133,CN=Bundeskanzleramt,C=AT
	Datum/Zeit	2021-06-22T16:25:44+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	2021-06-22T16:31:56+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.	