6441/J XXVII. GP

Eingelangt am 22.04.2021

Anfrage

der Abgeordneten Dr.in Petra Oberrauner, Genossinnen und Genossen

an die Bundesministerin für Digitalisierung und Wirtschaftsstandort

betreffend **Auswirkungen der Sicherheitslücken bei Microsoft Exchange auf Österreichs Wirtschaft und Sicherheit**

Am 2. März 2021 warnte Microsoft vor einer Sicherheitslücke auf der weltweit meistgenutzten E-Mail-Plattform Microsoft Exchange und rief seine Kunden dazu auf, die Software so schnell wie möglich mit einem Sicherheitsupdate zu aktualisieren. Zuvor war bekannt geworden, dass kriminelle Hackerorganisationen die Sicherheitslücke bereits ausgenutzt hatten, um weltweit mehr als 100.000 Server mit Hintertüren (so genannte Webshells) auszustatten, die nun Cyberkriminellen für Straftaten offenstehen. So können diese Hintertüren – wenn sie nicht rechtzeitig entdeckt werden – dafür genutzt werden, um sensible Daten von Firmen und ihren MitarbeiterInnen abzugreifen oder Schadsoftware wie Ransomware einzuschleusen. Um die Gefahr zu bannen, ist es daher wichtig sowohl die Sicherheitslücke zu schließen, als auch zu überprüfen, ob bereits eine Hintertür installiert worden ist. [1] Eine Umfassende Analyse der IT-Systeme ist jedoch sehr kostenintensiv und gerade kleinen und mittleren Unternehmen könnten hierfür die notwendigen IT-Ressourcen fehlen.[2]

Der österreichische IT-Spezialist ACP warnte am 19.03.2021, dass in Österreich über 1500 Organisationen von der Sicherheitslücke betroffen seien und die Lücke auch zwei Wochen nach der Warnung durch Microsoft noch nicht geschlossen hätten. Betroffen seien Wirtschaftsbetriebe aus unterschiedlichen Branchen, Gemeinden und auch kritische Infrastruktur. [3]

In Deutschland hat das Bundesamt für Sicherheit in der Informationstechnologie (BSI) aufgrund der großen Verbreitung der Sicherheitslücke die Alarmstufe Rot ausgerufen.[4] Der Präsident des BSI, Arne Schönbohm warnte am 12. März auf Twitter vor einer Welle krimineller Cyberangriffe und erklärte, er würde sich besonders um kleine und mittlere Betriebe sorgen.[5]

---

[1] https://www.derstandard.at/story/2000124994425/exchange-desaster-viele-offene-fragen-und-schwere-entscheidungen-nach-dem

[2] https://www.derstandard.at/story/2000124762096/exchange-die-microsoft-luecken-sind-ein-sicherheitsdesaster-fuer-zehntausende-unternehmen

[3] https://www.acp.at/news-und-events/microsoft-exchange-hacks-ueber-1500-betriebe-in-oesterreich-betroffen

[4] https://www.heise.de/news/Exchange-Luecken-BSI-ruft-IT-Bedrohungslage-rot-aus-5075457.html

[5] https://twitter.com/ArneSchoenbohm/status/1370380206658162689?s=19

Die unterfertigten Abgeordneten stellen daher folgende

ANFRAGE

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?
4. Bis wann –geht ihr Ministerium aus - sollen alle Server mit einem Patch versehen worden sein?
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?
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?
10. Welche finanziellen Kosten sind für diese Maßnahmen angefallen? Konnten diese aus dem hierfür vorgesehen Kostenstellen gedeckt werden oder wurden zusätzliche Mittel bereitgestellt?
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?
13. Auf welche Höhe beläuft sich bislang der volkswirtschaftliche Schaden?
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?
15. Wann, in welcher Form und in welchem Zeitraum haben Sie betroffenen Unternehmen Ihre Hilfe bei der Sicherung ihrer digitalen Infrastruktur angeboten?
16. Wie viele Personen sind damit in Ihrem Ministerium befasst und welche finanziellen Mittel wurden hierfür aus welcher Kostenstelle aufgewendet?
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?
18. Welche Kenntnisse besitzen Sie darüber, wer bzw. welche Gruppierung oder Organisation hinter der massenhaften Platzierung von Webshells steckt?
19. Was wollen Sie unternehmen, um die digitale Infrastruktur im staatlichen und nicht-staatlichen Bereich zukünftig besser vor den Risiken derartiger Sicherheitslücken und massenhafter Cyberattacken zu schützen?