Deutscher Bundestag Drucksache 19/27994
19. Wahlperiode 26.03.2021

Schriftliche Fragen

mit den in der Woche vom 22. März 2021 eingegangenen Antworten der Bundesregierung

19. Abgeordnete Petra Pau (DIE LINKE.)

Welche sechs anderen Behörden und sonstigen Stellen im Verantwortungsbereich der Bundesregierung außer dem bereits öffentlich bekannten Paul-Ehrlich-Institut (PEI), dem Umweltbundesamt (UBA) und der Bundesanstalt für Verwaltungsdienstleistungen (Microsoft-Schwachstelle: Impfstoff-Experten vom Paul-Ehrlich-Institut betroffen – DER SPIEGEL vom 15. März 2021)troffen – DER SPIEGEL vom 15. März 2021) sind inwiefern von dem Cyberangriff über die Schwachstelle im E-Mail-System Exchange von Microsoft betroffen?

Antwort des Parlamentarischen Staatssekretärs Dr. Günter Krings vom 25. März 2021

Vorbemerkung der Bundesregierung:

Sicherheitslücken in Software sind relativ häufig. Die großen Softwarehersteller liefern daher teilweise im Monatsrhythmus Patches aus, um Sicherheitslücken zu schließen. Ein technisches Verfahren, um Sicherheitslücken in Software von vornherein auszuschließen, ist nicht bekannt. Aus Sicht der Bundesregierung liegt die Identifikation und Bereinigung von Sicherheitslücken daher zunächst im Verhältnis zwischen Hersteller und seinen Kunden.

Erst wenn durch Sicherheitslücken eine erhebliche Beeinträchtigung der öffentlichen Sicherheit und Ordnung, der Versorgungssicherheit oder anderer hochrangiger Rechtsgüter erfolgen könnte, ist eine staatliche Regulierung oder eine Meldepflicht von Unternehmen angezeigt und verhältnismäßig.

Vor diesem Hintergrund definieren sowohl die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) als auch das zur Umsetzung dienende IT-Sicherheitsgesetz und die darauf aufbauenden Verordnungen Melde- und Vorsorgepflichten erst ab bestimmten Gefahren-schwellen. Dies wird auch im IT-Sicherheitsgesetz 2.0, das derzeit in den parlamentarischen Beratungen ist, beibehalten. Selbst Betreiber so genannter kritischer Infrastrukturen müssen daher nicht die bloße Existenz einer Sicherheitslücke in ihren IT-Systemen gegenüber staatlichen Stellen offenlegen. Erst wenn die Ausnutzung einer Sicherheitslücke derart erfolgt, dass erhebliche Auswirkungen auf die Versorgungssicherheit zu erwarten sind, ist eine Meldung an das Bundesamt für Sicherheit in der Informationstechnik (BSI) und ggf. an die Aufsichtsbehörden gesetzlich festgelegt und verhältnismäßig.

Im Rahmen der Untersuchungen von möglichen Verdachtsfällen in der Bundesverwaltung konnten diese Verdachtsfälle nicht bestätigt werden. Derzeit sind der Bundesregierung zwei Bundesbehörden bekannt, in denen eine Kompromittierung der IT-Systeme durch das Ausnutzen der Sicherheitslücke und die Installation einer Web-Shell bestätigt werden kann. Ein

zwischenzeitlich „False-Positive“ (positives Ergebnis der Detektion ohne tatsächliche Betroffenheit) erkannter Sachverhalt wurde entsprechend korrigiert. Es bleibt daher bei den zwei betroffenen Behörden.

20. Abgeordnete Petra Pau (DIE LINKE.)

Bei welcher dieser betroffenen Behörden und sonstigen Stellen im Verantwortungsbereich der Bundesregierung wurde ein mutmaßlich über diese Schwachstelle hinterlegter Schadcode detektiert, der als Hintertür insbesondere dazu genutzt werden könnte, zu einem späteren Zeitpunkt unberechtigt Daten dieser Stellen abzusaugen bzw. zu verschlüsseln, um ggf. Lösegeldforderungen zu stellen?

Antwort des Parlamentarischen Staatssekretärs Dr. Günter Krings vom 25. März 2021

Bei zwei Behörden konnte das Vorhandensein der Web-Shells als mögliche Hintertür bestätigt werden. Die Web-Shells wurden von Angreifern nach Bekanntwerden der Schwachstellen automatisiert verteilt. Die Existenz der Web-Shell bedeutet jedoch noch nicht, dass es zu Datenabflüssen oder weiteren Aktionen der Angreifer auf den betroffenen Systemen gekommen ist.

21. Abgeordnete Petra Pau (DIE LINKE.)

Weshalb kann – wie medial berichtet wurde (Microsoft-Schwachstelle: Impfstoff-Experten vom Paul-Ehrlich-Institut betroffen – DER SPIEGEL vom 15. März 2021) – inzwischen als gesichert gelten, dass es bislang bei keiner dieser oder anderer Behörden und sonstiger Stellen im Verantwortungsbereich der Bundesregierung infolge der Schwachstelle im E-Mail-System Exchange zu Datenabflüssen gekommen ist?

Antwort des Parlamentarischen Staatssekretärs Dr. Günter Krings vom 25. März 2021

Das BSI hat Einrichtungen der Bundesverwaltung, die eine Meldung zu diesem Sachverhalt abgegeben haben, bei der Bewältigung des Vorfalls mit Incident-Response-Maßnahmen unterstützt. Bei den durchgeführten forensischen Untersuchungen im Rahmen der Exchange Sicherheitslücke konnte nach aktuellem Stand eine Ausnutzung der Exchange Schwachstelle nur in Form der Installation einer Web-Shell bei den zwei betroffenen Behörden festgestellt werden.

Nach aktuellem Stand der laufenden forensischen Analysen gibt es bislang keine Hinweise, dass dabei ein Datenabfluss über Web-Shells oder auf anderem Weg erfolgte. Die Analysen werden weiter mit Nachdruck durchgeführt.

22. Abgeordnete Petra Pau (DIE LINKE.)

Inwiefern kann die Bundesregierung nach derzeitigem Kenntnisstand ausschließen, dass außer der nach Darstellung der Firma Microsoft für die Schwachstellen in den eigenen Systemen verantwortlichen, vom Konzern als „Hafnium“ bezeichneten, „aus China operierenden, professionell vorgehenden und offenbar staatlich gesteuerten Gruppierung“ (Microsoft-Schwachstelle: Impfstoff-Experten vom Paul-Ehrlich-Institut betroffen – DER SPIEGEL vom 15. März 2021) andere staatliche oder nichtstaatliche Akteure die Schwachstellen aktiv ausgenutzt haben?

Antwort des Parlamentarischen Staatssekretärs Dr. Günter Krings vom 25. März 2021

Die Sicherheitsbehörden sind derzeit u. a. in der Prüfung, ob sich ein Anfangsverdacht einer geheimdienstlichen Agententätigkeit gegen die Bundesrepublik Deutschland (§ 99 des Strafgesetzbuches) erhärtet. Vor dem Hintergrund des laufenden Verfahrens können zum gegenwärtigen Zeitpunkt keine weiteren Details öffentlich gemacht werden.