Der Bayerische Landesbeauftragte
für den Datenschutz

Hinweise zu einer Sicherheitslücke der Stay Informed App

Aktuelle Sonderinformation

Stichwörter: Benachrichtigungspflicht – Datenpanne – Meldepflicht – Risikobewertung – Stay Informed App– Unterschriftsgrafiken | **Stand:** 8. April 2024

Infolge der Fehlkonfiguration eines Webservers kam es beim Anbieter der unter anderem von Kindertagesstätten bayerischer Kommunen genutzten Stay Informed App zu einer Datenpanne, bei der personenbezogene Daten frühestens seit dem 20. Oktober 2021 und spätestens seit dem 18. August 2023 über das Internet frei abrufbar waren. Dieses „Datenleck" wurde mittlerweile geschlossen; dennoch ist die Aufarbeitung des Vorfalls noch nicht beendet. Der Anbieter der Stay Informed App hat unter dem folgenden Link ausführliche Informationen zu dem Vorfall bereitgestellt. 1

https://www.stayinformed.de/information-sicherheit

Der Bayerische Landesbeauftragte für den Datenschutz begrüßt, dass ihm zahlreiche bayerische öffentliche Stellen nach Art. 33 Datenschutz-Grundverordnung (DSGVO) Meldung erstattet und oftmals auch bereits die betroffenen Personen informiert haben. Da viele Meldungen und Informationen auf Grund der gesetzlichen Vorgaben alsbald nach Bekanntwerden des Datenlecks auf den Weg gebracht wurden, konnten darin noch nicht alle Fragen beantwortet werden. 2

Vor diesem Hintergrund gibt der Landesbeauftragte die folgenden Hinweise für Kommunen, in deren Einrichtungen die Stay Informed App genutzt wird (1.), sowie für betroffene Personen, insbesondere Kinder und ihre Personensorgeberechtigten (2.). 3

1. Hinweise für betroffene Kommunen

Wie in den Meldungen angegeben, bestehen Auftragsverarbeitungsvereinbarungen zwischen dem Anbieter der Stay Informed App als Auftragsverarbeiter und der jeweiligen Kommune als Verantwortlichem. Diese Rollenverteilung zugrunde gelegt, sind die Kommunen unter anderem verpflichtet, Datenpannen an die zuständige Datenschutz-Aufsichtsbehörde zu melden und bei ihrem Auftragsverarbeiter auf eine angemessene Aufarbeitung sowie auf die Umsetzung der gebotenen technisch-organisatorischen Maßnahmen hinzuwirken. Auftragsverarbeitung bedeutet für den Verantwortlichen also nicht „Problementsorgung". Vorläufig gemachte Meldungen müssen alsbald ergänzt werden; dies gilt namentlich für eine zunächst noch nicht abschließend mögliche Risikobewertung. 4

Entscheidend ist dabei, ob und welche personenbezogenen Daten aus dem eigenen kommunalen Verantwortungsbereich von der Datenpanne betroffen sind. Das Risikoprofil fällt also von Kommune zu Kommune unterschiedlich aus – daher muss es jeweils auch von der 5

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

Kommune selbst gezeichnet werden. Eine Hilfestellung bietet die einschlägige Orientierungshilfe des Landesbeauftragten, die unter dem nachstehenden Link abrufbar ist.

https://www.datenschutz-bayern.de/datenschutzreform2018/OH_Meldepflichten.pdf

6 Die folgenden Punkte sollte bei der Risikobewertung in jedem Fall bedacht werden:

7 – **Konkreter Inhalt der auf dem betroffenen Webserver gespeicherten PDF-Anhänge:** Insofern sollte geprüft werden, ob Inhalte wie Fotos oder weitere Daten von Kindern hochgeladen wurden, die einen besonderen Schutzbedarf auslösen und deren Zugänglichkeit für Nichtberechtigte zu einem hohen Risiko führen könnte.

8 – **Konkreter Inhalt der auf dem betroffenen Webserver gespeicherten exportierten CSV-Dateien:** Den bisherigen Meldungen ist zu entnehmen, dass die von den öffentlichen Stellen bereitgestellten Daten unterschiedlich detailliert sind. Soweit es sich nur um Namen und Zugehörigkeiten zu Betreuungsgruppen handelt („Lisa aus der Käfergruppe“), wird eher ein nur geringes Risiko angenommen werden können als bei Verfügbarkeit vollständiger E-Mail- oder Analogpost-Adressen. Besonders kritisch sind medizinische Informationen (etwa über gesundheitliche Beeinträchtigungen, die bei der Betreuung zu berücksichtigen sind, oder einen Impfstatus). Auch tatsächliche Wohnanschriften können im Einzelfall besonders risikoträchtig sein; dies gilt insbesondere, wenn für die betroffene Person eine melderechtliche Auskunftssperre besteht.

9 – **Konkrete Abbildungen Avatare/Profilbilder:** Hier ist zu prüfen, ob sich in dem relevanten Datenbestand nur „Platzhalter“ oder aber echte Lichtbilder von Kindern, Eltern oder sonstigen Bezugspersonen befinden; in solchen Fällen ist besonders kritisch zu prüfen, ob bereits ein hohes Risiko vorliegt.

10 – **Nutzung der Unterschriftenfunktion:** Die Option der Stay Informed App, Unterschriftsgrafiken zu speichern und damit Dokumente zu „unterschreiben“, wird erfreulicherweise nicht von allen meldenden Stellen verwendet. Werden Unterschriftsfaksimiles öffentlich, kommt grundsätzlich ein hohes Risiko in Betracht.

11 Hier sollte stets auch geprüft werden, ob diese Option wirklich genutzt werden soll. Dies gilt insbesondere vor dem Hintergrund, dass die wohl bezweckte Art der Unterschriftsleistung weder die Anforderungen an die Schriftform (§ 126 Abs. 1 Bürgerliches Gesetzbuch – BGB) noch an die elektronische Form (§ 126a Abs. 1 BGB) erfüllt. Auch wenn diese Daten nur in verschlüsselter Form „abgegriffen“ worden sein sollten, bleibt es bei dem grundsätzlichen Problem, dass kryptographische Verfahren veralten und die Unterschriftsdaten womöglich schon in einigen Jahren von Unbefugten entschlüsselt und dann missbräuchlich genutzt werden könnten. Dieser Aspekt ist bei der Risikobewertung ebenfalls zu berücksichtigen.

12 – **Korrekte Ermittlung der Anzahl der betroffenen Personen:** Nicht alle Stellen konnten zum Meldezeitpunkt bereits abschließend eine Anzahl der betroffenen Personen angeben. Das ist nach entsprechender Auswertung nachzuholen.

13 – **Langer Zeitraum bis zur Feststellung des Datenlecks:** Solange nicht zweifelsfrei das Gegenteil nachgewiesen werden kann, ist anzunehmen, dass im Zeitraum des Datenlecks tatsächlich unbekannte Dritte Zugriff auf zugängliche Daten genommen haben können.

Das muss zum einen bei der Risikoanalyse berücksichtigt werden; zum anderen sollten bayerische Kommunen bei ihrem Vertragspartner auch auf Maßnahmen gegen eine Weiterverwertung heruntergeladener Daten hinwirken (etwa durch Darknet-Monitoring).

– **Kurze Aufbewahrungsdauer für Protokollierungen:** In den Meldungen wurde zwar angeführt, dass der Anbieter der Stay Informed App das fragliche Datenleck mittlerweile geschlossen habe und zukünftig Penetrationstests sowie Audits durchführen wolle. Nicht beantwortet wurde allerdings die Frage, ob zukünftig auch eine längerfristige Protokollierung von Zugriffen und eine systematische Auswertung vorgesehen ist. Soweit Protokollierungen bislang nur für zwei Wochen vorgehalten wurden, lassen sich ältere unbefugte Zugriffe kaum noch nachweisen; auch dies ist bei der Risikobewertung zu verarbeiten. 14

Soweit eine Benachrichtigungspflicht nach Art. 34 DSGVO eingreift, sollte konkret erläutert werden, welche Daten betroffen sind und mit welchen Risiken zu rechnen ist. Auch auf geeignete Abhilfemaßnahmen (Selbstdatenschutz) sollte hingewiesen werden. 15

Sollte eine Meldung nach Art. 33 DSGVO bisher unterblieben, ein Risiko jedoch verwirklicht sein, ist sie umgehend nachzuholen. 16

2. Hinweise für betroffene Personen

Nach dem aktuellen Sachstand (Datum oben) kann nicht ausgeschlossen werden, dass etwa Profibilder, PDF-Anhänge, Adressdaten oder verschlüsselte Unterschriftsgrafiken in falsche Hände gelangt sind. 17

Betroffene Personen – für Kinder die Personensorgeberechtigten – sollten daher eine erhöhte Aufmerksamkeit auf den Umgang mit E-Mails, Telefonanrufen und Zusendungen per Analogpost richten. Aus Datenlecks abgegriffene Daten werden häufig für Phishing- oder Schadcode-Kampagnen verwendet. Eine Übersicht zum Umgang mit gehackten E-Mail-Konten hat das Bundesamt für Sicherheit in der Informationstechnik unter dem nachstehenden Link veröffentlicht. 18

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Identitaetsdiebstahl/Hilfe-fuer-Betroffene/hilfe-fuer-betroffene.html

Bei der Verwendung von echten Fotos als Profilbildern ist in einer Zeit, zu der Künstliche Intelligenz und automatisierte Bilderkennung in den Alltag eingezogen sind, ohnehin Vorsicht angebracht. Im Internet zugängliche Bilder können zunehmend leichter missbraucht werden, nicht nur für Identitätsdiebstahl, sondern auch etwa für Erpressungsversuche. 19

Gespeicherte Unterschriftsgrafiken stehen für Urkundenfälschungen zur Verfügung, sobald es gelingt, die vom Anbieter der Stay Informed App eingesetzte Verschlüsselung zu „knacken“. Wenn dies heute noch nicht möglich ist, kann dies schon in einem überschaubaren Zeitrahmen anders sein. Auch insofern ist Wachsamkeit zu empfehlen. 20