

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB

Der Beauftragte

POST CH AG CH-3003 Bern EDÖB; EDÖB-A-1E8D3401/3

Einschreiben (R)MLL Meyerlustenberger Lachenal Froriep AG
Schiffbaustrasse 2

Postfach 8031 Zürich

Ihr Zeichen: Unser Zeichen: EDÖB-A-1E8D3401/3 Sachbearbeiter/in: Katja Gysin Bern, 17. März 2023

Mitto AG, möglicher Missbrauch des Zugangs zum Mobilfunknetz, Abschluss Vorabklärung

Sehr geehrte Damen und Herren

Im Dezember 2021 wurde der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) aufgrund von Medienberichten auf eine mögliche unrechtmässige Datenbearbeitung durch einen Mitarbeiter der Mitto AG aufmerksam. Es wurde der Vorwurf erhoben, dass ein Mitarbeiter der Mitto AG über das Firmennetzwerk die unerlaubte Überwachung von Personen, möglicherweise durch Drittfirmen, ermöglicht habe.

Im Rahmen einer Vorabklärung wurden vom EDÖB dazu folgende Untersuchungshandlungen vorgenommen:

Abklärungen

1.

In einer ersten Aufforderung wurde die Mitto AG am 8. Dezember 2021 gebeten, zum fraglichen Sachverhalt generell Stellung zu nehmen. Die entsprechende Antwort erfolgte durch die Rechtsvertretung der Mitto AG innerhalb der erstreckten Frist am 7. Januar 2022. Darin wurde ausgeführt, dass die Mitto AG über keine Kenntnisse eines derartigen Missbrauchs verfügte, und dass die Mitto AG organisatorische und technische Datenschutzmassnahmen zum Schutz vor einer unbefugten Bearbeitung getroffen hätte. Begleitet wurde diese Eingabe von einer umfangreichen Dokumentation der anwendbaren Prozesse und Richtlinien.

Parallel zur Stellungnahme der Mitto AG hat der EDÖB die drei schweizerischen Mobilfunkbetreiber um Beantwortung eines Fragenkatalogs gebeten. Der Fokus lag bei einer allfälligen geschäftlichen Verbindung zur Mitto AG sowie der technischen Einschätzung der mutmasslich ausgenutzten Schwachstelle durch die Mitto AG. Die Mobilfunkanbieter bestätigten vertragliche Verbindungen zur

Feldeggweg 1 3003 Bern Tel. +41 58 463 74 84, Fax +41 58 465 99 96 www.edoeb.admin.ch



Mitto AG, aber schlossen – unter Verweis auf technische und organisatorische Massnahmen zur Gewährleistung der Datensicherheit – aus, dass es zu effektiven Missbräuchen über die jeweiligen Mobilnetze gekommen war.

2.

In einem zweiten Schriftenwechsel forderte der EDÖB die Mitto AG am 4. April 2022 auf, ihm Unterlagen zuzustellen, aus denen hervorgeht, welche Prüfungen von der Mitto AG oder von ihr Beauftragten konkret durchgeführt wurden, um festzustellen, dass – gemäss ihren Aussagen – kein Missbrauch vorgelegen hat.

Die Mitto AG nahm dazu innerhalb der erstreckten Frist am 1. Juni 2022 Stellung. In den Ausführungen wurde auf die ISO-Zertifizierungen der Mitto AG verwiesen und darüber hinaus geltend gemacht, dass eine interne Prüfung der Service-Plattform keine Kompromittierung des Systems gezeigt habe. Es seien keine Anhaltspunkte für einen Missbrauch gefunden und die in den Medienberichten erwähnten Personen hätten keinen Zugriff auf Code-Repositories, und konnten somit keine unrechtmässigen Änderungen vornehmen. Es seien auch keine Änderungen oder unerwünschte Aktivitäten im Bereich der Software festgestellt worden. Eine externe Prüfung im Rahmen eines Sicherheits-Audits der Service Delivery Plattform und der Telekommunikationssysteme der Mitto AG hätten ebenfalls keine Auffälligkeiten zu Tage gefördert.

3.

Mit Schreiben vom 19. August 2022 forderte der EDÖB die Mitto AG auf, zusätzliche Ausführungen zu möglichen unberechtigten Zugriffen auf die Systeme zu machen. Er stellte die Frage, ob eine oder mehrere Personen ihren Zugriff auf die Systeme der Mitto AG ausgenutzt hatten, um nicht berechtigten Dritten Zugang zu Informationen zu verschaffen oder direkten Zugang zum System selber zu ermöglichen. Der EDÖB erwartete eine Auswertung von Protokollierungsdaten, um nachzuweisen, dass alle Systemzugriffe gerechtfertigt waren.

Die Mitto AG nahm mit Schreiben vom 28. Oktober 2022 zu diesem Themenbereich ausführlich Stellung und stellte einen Untersuchungsbericht zu den durchgeführten Prüfschritten zur Verfügung. Der Bericht wertete die Active Directory-Protokolle, Fernzugriffs-VPN Protokolle, Multifaktor-Authentifizierungsprotokolle, Anwendungsprotokolle und alle Serverprotokolle (einschliesslich Server- und Dienstprotokolle, die mit den Netzen der Mobilfunkbetreiber und -anbieter verbunden sind) für verschiedene Zeiträume aus.

Darüber hinaus wurden alle Identitätszugriffskontrollsysteme geprüft, um sicherzustellen, dass der Zugriff entsprechend der Rollen und Berechtigungen erfolgte. Zudem machte der Bericht Angaben zum Software Development Lifecycle, der seit 2015 Standard war und nach Einschätzung der Mitto AG eine unzulässige Installation von Software für die Lokalisierung von Mobilfunkteilnehmern verhindert bzw. aufgezeigt hätte. Der Bericht enthielt auch Erläuterungen zum Identity and Access Management für interne und externe User bei der Mitto AG. Auch hier wurden keine Auffälligkeiten festgestellt.

4.

In einer virtuellen Besprechung am 13. Dezember 2022 zwischen Vertreterinnen des EDÖB, der Mitto AG und ihrer Rechtsvertretung wurden gewisse zusätzliche Erläuterungen zum Bericht abgegeben.

Würdigung

Gemäss dem Bundesgesetz über den Datenschutz (DSG, SR 235.1) dürfen Datenbearbeiter Personendaten nur rechtmässig und unter Einhaltung der allgemeinen Bearbeitungsgrundsätze bearbeiten (Art. 4 DSG). Sie haben dabei die Pflicht, die Daten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten, beispielsweise unberechtigte Zugriffe, zu schützen. Der EDÖB hat angesichts der geschilderten Vorkommnisse in einer Vorabklärung geprüft, ob es diesbezüglich zu Versäumnissen gekommen ist. Die Mitto AG ist dabei den Begehren des EDÖB in allen Belangen nachgekommen.

So hat sie im Rahmen des Schriftenwechsels Nachweise zu den organisatorischen Rahmenbedingungen des Systembetriebs erbracht. Sie hat im Weiteren erläutert, mit welchen Massnahmen sie unerwünschte bzw. unerlaubte Änderungen an der Software ihrer Systeme verhindert bzw. aufdecken kann. Die Auswertung der vorhandenen Protokollierungsdaten erlaubte Aussagen zu Zugriffen auf die Systeme.

Sowohl die Prüfung der Regeln für Software-Änderungen als auch die Auswertung der Zugriffe auf die Systeme haben gemäss den Angaben der Mitto AG keine Hinweise ergeben, die eine missbräuchliche Verwendung der Systeme in der vorgeworfenen Weise nahelegen würden.

Die Mitto AG hat zudem mehrfach ausgeführt, dass es Mitarbeitenden gar nicht möglich sei – ohne eine Veränderung der Systeme bzw. der Software – einen Zugriff auf Lokalisierungsdaten von SMS-Empfängerinnen und Empfängern zu erlangen. Diese Aussage wird von den Erläuterungen der angefragten Mobilfunkanbietern gestützt. Eine unentdeckte bzw. unerlaubte Veränderung der Software schloss die Mitto AG, gestützt auf den seit 2015 eingeführte Software Development Cycle, aus.

Der EDÖB hat im Rahmen seiner ihm zur Verfügung stehenden Mittel die notwendigen und möglichen Prüfungen veranlasst. Anhand der dem EDÖB zur Verfügung stehenden Angaben ergeben sich keine Hinweise, die den Verdacht, dass es zu einer Verletzung von Datenschutzbestimmungen gekommen ist, bestätigen würden. Da es sich bei den Vorwürfen zum Fehlverhalten der Mitto AG um technisch wenig spezifische Anschuldigungen handelt, hat der EDÖB seine Mittel vorderhand ausgeschöpft, ohne dass sich der Verdacht auf eine Verletzung von Datenschutzbestimmungen erhärtet hätte.

Unter diesen Gesichtspunkten schliesst der EDÖB die Vorabklärung in Sachen Mitto AG ab und verzichtet auf allfällige Empfehlungen.

Freundliche Grüsse

Adrian Lobsiger Der Beauftragte

Beilage: Englische Übersetzung des deutschen Originalberichts