Stadt Zürich
Stadtrat

Beschluss des Stadtrats

vom 7. Februar 2024

GR Nr. 2023/397

Nr. 390/2024
Interpellation von Sven Sobernheim und Sanija Ameti betreffend Datenschutzproblem mit der Software für Sportabos, Hintergründe zur Beschaffung der Software, Behebung der Probleme nach Mitteilung an das Sportamt, Kosten für die Anpassungen, Information der Datenschutzstelle und Zeitplan für die Aufarbeitung des Vorfalls sowie genereller Umgang mit sensiblen Personendaten

Am 23. August 2023 reichten die Mitglieder des Gemeinderats Sven Sobernheim und Sanija Ameti (beide GLP) folgende Interpellation, GR Nr. 2023/397, ein:

Am 12. August 2023 machte der Tages-Anzeiger publik, dass das Sportamt ein Datenschutzproblem mit der Software für Sportabos hatte. Gleichzeitig wurde bekannt, dass das Sportamt den Fehler lange Zeit nicht behob und auch den städtischen Datenschutzbeauftragen nicht informiert hatte.

Das Nonchalance Vorgehen weist grosse parallelen zur illegalen Videoüberwachung des Sportamts im Jahr 2018 auf. Auch dort sah das Sportamt keine Probleme.

In diesem Zusammenhang bitten wir den Stadtrat um die Beantwortung der folgenden Fragen:

1. Wann wurde die entsprechende Software beschafft? Wer hat die Ausschreibung durchgeführt und wie wurde das Thema Datenschutz in der Ausschreibung gefordert?
2. Warum ist das Sportamt und nicht OIZ für eine solche Software zuständig?
3. Laut Medienberichterstattung fand die Meldung ans Sportamt am 14.06 statt. Kann dies bestätigt werden? Und was wurde, wann zwischen der Meldung und der Anpassung am 14.07 vorgenommen?
4. Wie hoch waren die Kosten für die Anpassung und wer hat diese auf Grundlage von welchem Vertrag getragen?
5. Wann wurde die Datenschutzstelle durch wen informiert?
6. Mit Medienmitteilung vom 14.08.23 hat das Sportamt verkündet, dass es keine Hinweise auf unbefugten Datenzugriff gab. Auf welcher Grundlage wurde diese Aussage getroffen? Welche Auswertungen und Tests wurden durch wen durchgeführt?
7. Gemäss dieser Meldung wird der Vorfall nun gemeinsam aufgearbeitet. Wie sieht der Zeitplan aus? Wer bzw. welche Stellen sind involviert und wird der Abschlussbericht veröffentlicht werden?
8. Nimmt der Stadtrat den Vorfall zum Anlass, den generellen Umgang mit sensiblen Personendaten zu thematisieren? Welche Massnahmen sind geplant um zum Beispiel ähnliche Vorfälle im Bereich Schülerdaten, ebenfalls im Schul- und Sportdepartement, zu verhindern?

Der Stadtrat beantwortet die Anfrage wie folgt:

Frage 1
Wann wurde die entsprechende Software beschafft? Wer hat die Ausschreibung durchgeführt und wie wurde das Thema Datenschutz in der Ausschreibung gefordert?

Die Ausschreibung zur Beschaffung eines neuen Zutritts- und Kassensystems inklusive Onlineshop für die Bade- und Eisanlagen der Stadt Zürich wurde am 16. März 2021 vom Sportamt

(SPA) auf simap.ch publiziert. Die Offertöffnung erfolgte am 26. Mai 2021. Der am 15. Oktober 2021 kommunizierte Zuschlag erfolgte an die Firma n-tree solutions schweiz GmbH (nachfolgend «n-tree» oder «die Lieferantin»).

Die Ausschreibung erfolgte formell durch das SPA und wurde inhaltlich in Zusammenarbeit mit der Organisation und Informatik (OIZ) erarbeitet, der stadtintern die Projektleitung übertragen war.

Im Pflichtenheft der Ausschreibung ist unter dem Titel «Sicherheit und Datenschutz» folgende Anforderung aufgeführt: «Es wird vorausgesetzt, dass Anbietende die allgemeingültigen Regeln und Gesetze bezüglich Informationssicherheit und Datenschutz einhalten. Die durch öffentliche Organe bearbeiteten Informationen sind gemäss dem «Gesetz über die Information und den Datenschutz («IDG»)» (LS 170.4) durch angemessene organisatorische und technische Massnahmen zu schützen (§ 7)».

Frage 2
Warum ist das Sportamt und nicht OIZ für eine solche Software zuständig?

Beim Zutritts- und Kassensystem handelt sich um eine Fachapplikation, die in der Stadtverwaltung ausschliesslich vom SPA genutzt wird. Das Schul- und Sportdepartement (SSD) verfügt im Departementssekretariat über eine zentrale IT-Abteilung, weshalb die Verantwortung für die Beschaffung und den technischen Betrieb der Software für Fachapplikationen beim SSD liegt. Das SSD beauftragte stadtintern jedoch OIZ mit der Projektleitung und Koordination der Ausschreibung.

Frage 3
Laut Medienberichterstattung fand die Meldung ans Sportamt am 14.06 statt. Kann dies bestätigt werden? Und was wurde, wann zwischen der Meldung und der Anpassung am 14.07 vorgenommen?

Es ist zutreffend, dass die Meldung an das SPA am 14. Juni 2023 erfolgt ist. Untenstehend folgt die Chronologie der Ereignisse zwischen dem 14. Juni 2023 und dem 14. Juli 2023.

14. Juni 2023

Eingang der Meldung per E-Mail des Kunden beim SPA auf die allgemeine E-Mail-Adresse des SPA (sportamt@zuerich.ch), in der darauf hingewiesen wird, dass eine Sicherheitslücke besteht.

15. Juni 2023

E-Mail SPA (Leiter Zentrale Dienste der Abteilung Badeanlagen) an OIZ (Projektleiter) und n-tree (Geschäftsführung/Projektleitung).

15. Juni 2023

Telefonische Besprechung der Meldung des Kunden durch OIZ (Projektleiter) und n-tree (Geschäftsführung/Projektleitung).

15. Juni 2023

Start Erarbeitung einer Lösung zur Behebung der Sicherheitslücke durch n-tree.

15. Juni 2023

Mitteilung Leiter Zentrale Dienste der Abteilung Badeanlagen, SPA, an Abteilungsleitung Sportamt Badeanlagen, SPA, inklusive der technischen Einschätzung durch n-tree (Geschäftsführung/Projektleitung).

15. Juni 2023

Entscheid Abteilungsleitung Badeanlagen, SPA, aufgrund der technischen Einschätzung durch n-tree (Geschäftsführung/Projektleitung), den Onlineshop nicht zu schliessen.

20. Juni 2023

Eingangsbestätigung per E-Mail durch SPA (Leitung Zentrale Dienste) an Kunden.

22. Juni 2023

Rückmeldung SPA (Leiter Zentrale Dienste Badeanlagen) an Kunden mit Hinweis, dass Kontakt mit Lieferanten des Onlineshops aufgenommen wurde, um Massnahmen umzusetzen.

6. Juli 2023

Telefonische Nachfrage durch OIZ (Projektleiter) bei n-tree (Geschäftsführung/Projektleitung).

6. Juli 2023

Antwort n-tree (Geschäftsführung/Projektleitung), dass Behebung der Sicherheitslücke auf den 17. Juli 2023 geplant sei.

14. Juli 2023

Meldung durch Kunden an Datenschutzstelle der Stadt Zürich (DAS).

14. Juli 2023

Meldung DAS (Mitarbeiterin DAS) an SPA (DC SPA).

14. Juli 2023

Offlineschaltung der betroffenen Funktion («Kartenverwaltung» / «Meine Daten») im Onlineshop.

14. Juli 2023

Schliessen der Sicherheitslücke (Update betreffend Registrierung Chipkarte: neu Kartennummer in Kombination mit Namen und Vornamen der Karteninhaberin oder des Karteninhabers notwendig).

Frage 4
Wie hoch waren die Kosten für die Anpassung und wer hat diese auf Grundlage von welchem Vertrag getragen?

Für die Stadt entstanden keine Kosten. Die Lieferantin n-tree hat Mängel gestützt auf die vertragliche Gewährleistungspflicht behoben und trägt dafür die Kosten.

Frage 5
Wann wurde die Datenschutzstelle durch wen informiert?

Die DAS wurde am 14. Juli 2023 durch den Kunden, der sich als «White-Hat-Hacker» bezeichnet, über den Datenschutzvorfall informiert. Zur Meldung des SPA an die DAS siehe die Antwort auf Frage 7.

Frage 6

Mit Medienmitteilung vom 14.08.23 hat das Sportamt verkündet, dass es keine Hinweise auf unbefugten Datenzugriff gab. Auf welcher Grundlage wurde diese Aussage getroffen? Welche Auswertungen und Tests wurden durch wen durchgeführt?

Die Lieferantin n-tree hat Auswertungen in den Log-Files des Kassen- und Zutrittssystems vorgenommen. Neben den fünfhundert Datensätzen, die durch den Kunden, der sich als «White-Hat-Hacker» bezeichnet, abgezogen wurden, gibt es keinerlei Hinweise auf unbefugte Zugriffe auf Daten von Drittpersonen. Aufgrund der grossen Datenmenge kann nicht mit Sicherheit ausgeschlossen werden, dass weitere unbefugte Zugriffe auf Daten erfolgt sind.

Frage 7

Gemäss dieser Meldung wird der Vorfall nun gemeinsam aufgearbeitet. Wie sieht der Zeitplan aus? Wer bzw. welche Stellen sind involviert und wird der Abschlussbericht veröffentlicht werden?

Der Vorfall wurde im Rahmen der Erarbeitung der Meldung gemäss § 12a IDG vom SPA unter Mitwirkung der Beraterin für Datenschutz des SSD, der OIZ, der Lieferantin n-tree und der DAS aufgearbeitet. Gestützt auf die Erkenntnisse der Aufarbeitung wurden Massnahmen zur Vermeidung von Datenschutzvorfällen und zur korrekten Bearbeitung von Datenschutzvorfällen definiert und initiiert. Die finale Meldung gemäss § 12a IDG des SPA an die DAS erfolgte am 13. November 2023. Die Meldung kann gestützt auf das IDG herausverlangt werden.

Frage 8

Nimmt der Stadtrat den Vorfall zum Anlass, den generellen Umgang mit sensiblen Personendaten zu thematisieren? Welche Massnahmen sind geplant um zum Beispiel ähnliche Vorfälle im Bereich Schülerdaten, ebenfalls im Schul- und Sportdepartement, zu verhindern?

Der korrekte Umgang mit Personendaten hat in allen städtischen Informatikprojekten, somit auch in denjenigen des SSD, einen hohen Stellenwert. Alle Vorhaben werden zu Projektbeginn in Bezug auf den Datenschutz und die Informatiksicherheit geprüft. Dabei werden die Fachstellen der OIZ und die DAS gemäss den Vorgaben im Handbuch für Informationssicherheit (HISi) beigezogen. Der Einbezug der IT Security (OIZ) und der DAS ist stadtweit einheitlich geregelt und für alle Departemente verbindlich. Zusätzlich werden die Anwendenden über die notwendigen Vorsichtsmassnahmen bei der Bearbeitung von Personendaten instruiert. Der Stadtrat erachtet diese Massnahmen als ausreichend. Er wird den korrekten Umgang mit sensiblen Personendaten weiterhin als wichtiges Thema beim Betrieb von Fachapplikationen behandeln.

Im Namen des Stadtrats
Die Stadtschreiberin
Dr. Claudia Cuche-Curti