Eingegangen: 15.07.2022
GGR-Nr. 2022-257

Sitzung vom 12. Juli 2022

Beschl. Nr. **2022-221**

9.5.0 Allgemeines
Interpellation von Vera Buchmann-Bach (FDP) und Patrick Sager (FDP) vom 28. April 2022 betreffend «Wie schützt sich Adliswil vor Cyberangriffen?»; Beantwortung

Ausgangslage

Am 28. April 2022 wurde die Interpellation von Vera Buchmann-Bach (FDP) und Patrick Sager (FDP) mit dem Titel «Wie schützt sich Adliswil vor Cyberangriffen?» eingereicht.

Die Interpellanten führen folgenden Sachverhalt auf:
Cyberangriffe auf Unternehmen, private und öffentliche Organisationen mit ihren teilweise gravierenden Konsequenzen haben in den letzten Jahren massiv zugenommen. So wurden auch mehrere Schweizer Gemeinden Opfer solcher Angriffe, welche zum Teil auch erfolgreich waren. Die sensiblen persönlichen Daten der Einwohner von Adliswil sind besonders schützenswert. Mit den digitalen Angeboten der Stadt Adliswil gewinnt die Frage der Cyber-Sicherheit noch mehr an Bedeutung, zum Beispiel über die Dienstleistungen per Online-Schalter und das elektronische Steuerkonto.

Erwägungen

Die Bedrohungen durch Cyber-Attacken haben in den letzten Jahren spürbar zugenommen. Sie reichen von Angriffen auf die Verfügbarkeit von Webseiten oder anderen Internetdiensten, über Schadsoftware und Ransomware hin zu Phishing-Attacken.

Die Informationssicherheit und der Datenschutz sind für die Stadt Adliswil von grösster Wichtigkeit und haben deshalb auch den nötigen Stellenwert. Seit dem 1. Januar 2022 betreibt die OBT AG als Full-Outsourcing-Partnerin das Rechenzentrum und die Cloud-Lösungen (OBT Swiss Cloud) der Stadtverwaltung. Die georedundanten Datacenter der OBT AG entsprechen dem aktuellen Stand der Technik und besitzen die erforderlichen Zertifizierungen (SOC 1 (ISAE 3402 Type II), SOC 2 (ISAE 3000), ISO27001, ISO22301, PCI DSS, FINMA RS-18/3).

Die gesetzlichen Grundlagen für den Kanton Zürich als Basis für den OBT Swiss Cloud Vertrag sind:
- Gesetz über die Auslagerung von Informatikdienstleistungen vom 23.8.1999 (LS 172.71);
- Gesetz über die Information und den Datenschutz (IDG) vom 12.2.2007 (LS 170.4);
- Verordnung über die Information und den Datenschutz (IDV) vom 28.5.2008 (LS 170.41);
- Allgemeine Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen (AGB Auslagerung Informatikleistungen) vom 24. Juni 2015;
- Allgemeine datenschutzrechtliche Geschäftsbedingungen bei der Datenbearbeitung durch Dritte (AGB Datenbearbeitung durch Dritte) vom 24. Juni 2015.

Die OBT AG investiert viel in diesem Bereich sowohl in Betriebsprozesse, Software und Hardware als auch in die Sensibilisierung ihrer Mitarbeitenden, um die Betriebssicherheit für ihre Kunden jederzeit zu gewährleisten. Die OBT AG als Full-Outsourcing-Partnerin hat in ihrem Vertragswerk auch wichtige Informatiksicherheitsrichtlinien (Kundenrichtlinien für die Nutzung der OBT-Informatikmittel) definiert, die durch alle Mitarbeitenden der Stadt Adliswil, die über ein Zugangskonto zum Rechencenter haben, eingehalten werden müssen. Die Sensibilisierung aller User der Stadt Adliswil bezüglich Cyber-Risiken wie Phishing ist daher besonders wichtig.

Beantwortung der Fragen

1. **Welche technischen Abwehr- und Schutzmassnahmen existieren bei der Stadtverwaltung Adliswil zur Verbesserung der Cyber-Sicherheit?**

   Der Grundbaustein für die Abwehr von Cyberangriffen ist ein gut geschütztes System. Die OBT AG ist seit vielen Jahren ISO27001 zertifiziert und setzt über 100 Massnahmen im Bereich Informationssicherheit um. Dazu gehören namentlich folgende Sicherheitsvorkehrungen im Aufbau und Betrieb der Datacenter:

   - Schutzzonen im Netzwerk durch Segmentierung;
   - Härtung des Systems;
   - Zwei-Faktor-Authentisierung;
   - Zeitnahes Patchmanagement;
   - Wöchentliche Prüfung der Vulnerabilität (Vulnerability Management);
   - Regelmässige Systemscans um Schwachstellen von Software und Hardware zu finden;
   - Sicherheitsupdates in regelmässigen Abständen. Für kritische Sicherheitslücken existiert ein Notfallprozess;
   - Zentrales Virenschutz System;
   - Disaster Recovery;
   - Zwei georedundante Datacenter. Failover Test werden regelmässig durchgeführt;
   - Sensibilisierung des Personals und regelmässige Schulungen.

   Diese Massnahmen werden ergänzt durch technische Sicherheitsvorkehrungen und eine Backup Prozess in den beiden georedundanten Datacentern und in der OBT Swiss Cloud.

2. **Wer überprüft diese Massnahmen? Gibt es einen externen Anbieter, welche diese wiederkehrend auditiert und werden regelmässig Stresstests durchgeführt?**

   Die OBT AG beschäftigt einen Mitarbeiter in der Funktion des CISO (Corporate Information Security Officer). Der hochqualifizierte Mitarbeiter arbeitet daneben noch als freier Senior Lead Auditor IEC/ISO27001 PECB und ist im Schweizerischen Normen Verband (SNV) tätig. Die Haupttätigkeiten des CISO sind vor allem die Beratung der OBT bei sicherheitsrelevanten Themen, die Erstellung periodischer Berichte zur Informationssicherheit, die Pflege des Informations-Sicherheits-Managementsystem (ISMS), das Durchführen von Risikoanalysen, die Analyse und Behandlung von Sicherheitsvorfällen, die Beurteilung der Sicherheitsrelevanz von Changes, das Tracking der Massnahmen

Korrektur- und Präventivmassnahmen sowie die Schulung, Sensibilisierung und Beratung der Mitarbeitenden.

Periodisch wird das ISMS der OBT nach ISO/IEC 27001:2013 durch eine externe Auditierungsstelle rezertifiziert, letztmals im Dezember 2020.

Die OBT AG führt punktuell Penetrationstests durch. In der Regel wird dies nach erfolgtem Auf- und/oder Ausbau eines kritischen, wichtigen Systems in Auftrag gegeben. Die OBT AG arbeitet dazu regelmässig mit dem spezialisierten Unternehmen InfoGuard (www.infoguard.ch) zusammen.

3. Falls Nein, wieso nicht? Wäre die Stadt Adliswil zukünftig bereit, die Massnahmen extern prüfen zu lassen?

Siehe Antwort zu Frage 2.

4. Gibt es höhere Sicherheitsmassnahmen für das persönliche Steuerkonto oder andere Angebote mit sensiblen persönlichen Daten?

Für einen einfachen Zugang zu den eGovernment-Diensten der Stadt Adliswil steht unseren Kundinnen und Kunden ein zentrales Benutzerkonto zur Verfügung. Hier finden die Verwaltungskunden all ihre laufenden und abgeschlossenen Geschäfte. Sie können den Bearbeitungsstand abfragen und Dokumente und Rückfragen empfangen.

Das „eSteuerkonto" ermöglicht es, direkt aus dem Benutzerkonto den Steuerkontostand abzufragen, einen Einzahlungsschein oder Zahlungen per E-Banking zu erzeugen oder das Auszahlungskonto zu ändern. Der Service wird durch Schnittstellen zwischen dem Benutzerkonto und dem Steuersystem ermöglicht. Dabei kommt ein Webservice zum Einsatz, der die Anfrage der Steuerpflichtigen über zwei hintereinander geschaltete verschlüsselte Verbindungen vom Benutzerkonto an das Steuersystem übergibt. Die Steuerapplikation schickt die angefragten Daten SSL-verschlüsselt an das Benutzerkonto.

Um den Steuerservice zu nutzen, müssen sich Steuerpflichtige zuerst via Benutzerkonto bei der Verwaltung registrieren lassen. Danach erhalten sie per Post einen Aktivierungscode. Durch die Zustellung per Post wird verhindert, dass eine Person das Steuerkonto einer Drittperson abfragt. Für Anfragen werden den Benutzerinnen und Benutzern zwei Sicherheits-Standards zur Verfügung gestellt. Im einfachen Fall kann die Anmeldung mit Benutzername und Passwort erfolgen. Die Steuerpflichtigen können ihr Konto noch zusätzlich schützen, indem sie die Multi-Faktor-Authentisierung aktivieren. Mit einer Authenticator-App wird ein zusätzlicher Zugangscode generiert. Dieser Service bietet eine zusätzliche Sicherheitsebene für das Benutzerkonto. Er verhindert den Zugriff Dritter im Fall eines Passwortdiebstahls.

5. Existiert ein Krisen- und Kommunikationskonzept im Fall eines gravierenden Cyber-Angriffs mit Verschlüsselung und/oder Veröffentlichung sensibler Daten?

Ja, es existiert bei der OBT AG ein Krisenkonzept im Fall eines Cyber-Angriffs. Die stetig aktualisierte Notfallplanung ist Bestandteil des ISMS (Information Security Management System) und tritt im Falle eines Cyber-Angriffs sofort in Kraft. Bei Bedarf werden von der OBT AG zusätzlich Cyber Security Experten hinzugezogen.

Die städtische Krisenkommunikation basiert auf dem Kommunikationskonzept der Stadt Adliswil. Die Grundsätze des Kommunikationskonzepts gelten auch in Krisenlagen oder Notfallsituationen. Die Zuständigkeit liegt grundsätzlich beim Stadtrat. Er kann dafür bei Bedarf auf das Gemeindeführungsorgan und weitere Spezialistinnen und Spezialisten abstellen.

Auf Antrag des Stadtpräsidenten fasst der Stadtrat, gestützt auf Art. 89 der Geschäftsordnung des Grossen Gemeinderates, folgenden

Beschluss:

1 Die Interpellation vom 28. April 2022 betr. «Wie schützt sich Adliswil vor Cyberangriffen?» von Vera Buchmann-Bach und Patrick Sager wird gemäss den Erwägungen beantwortet.

2 Dieser Beschluss ist öffentlich.

3 Mitteilung an:

- 3.1 Grosser Gemeinderat
- 3.2 Stadtrat
- 3.3 Ressortleitende
- 3.4 Informatik

Stadt Adliswil
Stadtrat

Farid Zeroual
Stadtpräsident

Thomas Winkelmann
Stadtschreiber

Stadt Adliswil