dsb
datenschutzbeauftragte
des kantons zürich

Fernwartung von Systemen der Informations- und Kommunikationstechnologie (IKT-Systeme)

Nach § 7 IDG muss das öffentliche Organ Personendaten durch angemessene organisatorische und technische Massnahmen schützen. Die gilt auch bei der Fernwartung von IKT-Systemen.

Fernwartung mit Zugriff auf Personendaten
Fernwartungen werden oft von Mitarbeitenden externer Firmen durchgeführt. Diese haben in den Arbeitsverträgen meist einen Datenschutz-Vermerk. Haben sie Zugriff auf heikle Daten, so genügt dieser Vermerk nicht. Vielmehr ist bereits die Kenntnisnahme der Daten durch diese Mitarbeitenden auszuschliessen. Als Hilfestellung kann der Baustein «OPS.1.2.5 Fernwartung» des Deutschen Bundesamtes für Sicherheit in der Informationstechnik genutzt werden.

Fernwartung mit Zugriff auf besondere Personendaten
Die Fernwartung von IKT-Systemen mit besonderen Personendaten ist nur unter folgenden Voraussetzungen zulässig (§ 3 IDG, LS 170.4):

- Die Verbindung darf ausschliesslich durch die Verantwortlichen des zu wartenden Computers aufgebaut werden können. Der Verbindungsaufbau sollte über eine festgelegte Adresse erfolgen, die im System hinterlegt sind.
- Die Wartungsfachperson muss sich bei jedem Wartungsvorgang mit einer starken Authentisierung (z.B. Chipkarte mit PIN, Token und Passwort etc.) und einer Multi-Faktor-Authentisierung anmelden.
- Es müssen sichere Kommunikationsprotokolle mit starker Verschlüsselung verwendet werden.
- Die Fernwartung muss auch im Notfall verfügbar sein. Eine entsprechende Notfallplanung ist zu erstellen.
- Die Fernwartungsaktivitäten sollen lokal mitverfolgt und unterbrochen werden können. Dafür muss beim verantwortlichen Organ eine fachkundige Person vor Ort anwesend sein.
- Die Fernwartungsaktivitäten sind revisionssicher aufzuzeichnen. Die Protokolle müssen automatisiert ausgewertet werden können und vor Manipulationen geschützt sein.
- Mit der Fernwartungsfirma ist eine vertragliche Vereinbarung abzuschliessen, die einen Hinweis auf die Strafbestimmung von § 40 IDG enthält.
- Es sind vertragliche Regelungen über die Geheimhaltung von Daten zu treffen. Werden Daten im Rahmen der Wartung extern gespeichert, so müssen sie nach Abschluss der Arbeiten sicher gelöscht werden. Die Pflichten und Kompetenzen des externen Wartungspersonals sind sorgfältig festzulegen.

V 2.5 / September 2024

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch