Check & Balance

Wirkung der Datenschutzreviews verstärken

Der Datenschutzbeauftragte überprüft mit Kontrollen, ob die öffentlichen Organe die Anforderungen des Datenschutzes in rechtlicher, organisatorischer und sicherheitstechnischer Hinsicht einhalten. Das Spektrum der zu kontrollierenden Organe umfasst alle Ämter der kantonalen Verwaltung und der über 160 Gemeinden, die Spitäler und Schulen sowie weitere Institutionen wie Alters- und Pflegeheime, Staatsanwaltschaften und Notariate.

Mit den vorhandenen Ressourcen kann der Datenschutzbeauftragte die ungefähr tausend Institutionen nicht regelmässig überprüfen. Er hat verschiedene Massnahmen ergriffen, um die Aufsichtspflicht trotzdem zu erfüllen und die Wirksamkeit der Kontrollen zu optimieren. Der Datenschutzreview wurde neu konzipiert, und es werden zunehmend Auftragnehmer kontrolliert, die für zahlreiche öffentliche Organe tätig sind.

Optimierter Datenschutzreview

Die Neukonzipierung der Datenschutzreviews verfolgt die folgenden Ziele:

- Erfassung aller zu prüfenden Institutionen und Objekte
- Einführung eines risikobasierten Ansatzes mit nachvollziehbarer Bewertung als Grundlage zur Jahresprüfplanung
- Einführung einer detaillierten Jahresprüfplanung
- Neugestaltung des Prüfprogramms für Datenschutzreviews in Anlehnung an die Empfehlungen des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) und die Normen ISO 27001/ISO 27002
- Detaillierte Darstellung der Massnahmen und der damit adressierten Risiken in den Berichten zur Verbesserung der Verständlichkeit bei den geprüften Organen sowie des Nachvollzugs
- Einführung von abgestuften Umsetzungsterminen je nach Risiko und Aufwand
- Einführung einer Stellungnahme zur Umsetzung der Massnahmen durch die geprüften Organe, um diese in den Lösungsprozess einzubeziehen und eine grössere Akzeptanz zu erreichen

Die neue Prüfmethodik und die neue Berichtsform werden seit Anfang 2017 angewendet.

Kontrolle von Outsourcingnehmern

Gemeinden und andere öffentliche Organe lagern ihre IT-Leistungen zunehmend aus. Deshalb entwickelte der Datenschutzbeauftragte ein Konzept zur Prüfung der Auftragnehmer mit den folgenden drei Zielen:

- Prüfung der Informationssicherheit dort, wo die Leistungen erbracht werden, bei Outsourcings also beim Auftragnehmer und nicht primär bei den Gemeinden
- Verbesserung der Effizienz und der Nutzung des Synergieeffekts, indem durch die Prüfung von Auftragnehmern Rückschlüsse auf alle angeschlossenen öffentlichen Organe gezogen werden können, so dass diese nicht umfassend geprüft werden müssen
- Erweiterung der Wissensbasis des Datenschutzbeauftragten über die bei den Auftragnehmern eingesetzten Technologien und Prozesse sowie Schaffung von Vergleichsmöglichkeiten

Der Prüfumfang wurde wie folgt festgelegt:

- Informationssicherheitsstrategie sowie Einsatz von Informationssicherheits-Managementsystemen (ISMS)
- Informationssicherheitskonzept (Risikoanalyse, Schutzbedarfsfeststellung, Modellierung, Massnahmenplanung, Umsetzung, Kontrolle der Umsetzung)
- Verfügbarkeit der IT-Systeme (Notfallvorsorge, Back-up und Restore)
- Sicherheits- und Betriebsorganisation (Zuweisung der Verantwortlichkeiten)
- Clients/Server (Grundkonfiguration und Verwaltung)
- Physische Schutzmassnahmen gegen Umwelteinflüsse sowie Zutrittsrechte
- Outsourcing (Verträge, Kontrollmittel, Betriebskonzept sowie -handbücher, insbesondere Back-up-Konzept, Incident-Management-Prozess, Sicherheitsmassnahmen, Verschlüsselung, Protokollierung und Auswertung bei besonderen Personendaten, Entsorgung von Datenträgern)
- Regelung des Passwortgebrauchs und technische Umsetzung
- Netzwerke (Übersicht Verbindungen, Provider, Anbindung, drahtlose Netzwerke)
- Rollen- und Berechtigungskonzept (Rolle des Datenverantwortlichen, Klassifizierung von Daten, administrative Prozesse für Zugriffe und Passwörter), Umsetzung, Aktualitätskontrolle
- Mobile Arbeitsplätze, Smartphones und mobile Datenträger (Bewilligung, Richtlinien, Schulung, Schutzmassnahmen wie Verschlüsselung, Passwort, Softwareupdates, Back-up)
- Weisungen für Benutzerinnen und Benutzer (PC/Client, Passwörter, E-Mail und Internet)
- Interne und externe Überprüfung der Informationssicherheit

Der Datenschutzbeauftragte erstellte eine Liste der Auftragnehmer, die IT-Dienstleistungen für öffentliche Organe erbringen, und priorisierte sie nach ihrer Verbreitung und ihrem Marktanteil. Darauf definierte er einen Fragenkatalog für Auftragnehmer und einen für die angeschlossenen öffentlichen Organe, mit dem die Resultate der Auftragnehmerprüfung verifiziert werden sollen. In der nächsten Phase überprüfte der Datenschutzbeauftragte einen öffentlich-rechtlichen und einen privatrechtlichen Outsourcingnehmer. Mit einer Kontrolle bei drei Gemeinden, die unterschiedliche Dienstleistungen vom privat-rechtlichen Outsourcingnehmer beziehen, wurden die Resultate verifiziert.

Die Umsetzung des Konzepts verlief erfolgreich, weshalb im Lauf der nächsten Jahre weitere Auftragnehmer geprüft werden.

Überprüfung eines öffentlich-rechtlichen Auftragnehmers

Ein öffentliches Organ, das sämtliche IT-Dienstleistungen von einer kantonalen Organisationseinheit bezieht, fragte den Datenschutzbeauftragten an, den Schutz der ausgelagerten Daten zu prüfen. Die kantonale Organisationseinheit erbringt Leistungen für 40 angeschlossene Institutionen und rund 1800 Arbeitsplätze in der kantonalen Verwaltung. Sie betreibt für verschiedene Amtsstellen eine Sicherheitsinfrastruktur. Die Risikoeinstufung der Organisationseinheit wurde anhand eines Bewertungsrasters als hoch eingestuft, da mehr als 1000 Systeme und mehr als 50 000 betroffene Personen festgestellt wurden.

Die Prüfung zeigte, dass die Organisationseinheit einen stabilen und gegen grössere Ausfälle abgesicherten Betrieb für ihre Kunden erbringt. Weiter ist ein Informationssicherheitsmanagement etabliert und wichtige Dokumente wie eine Strategie, ein IT-Sicherheitskonzept sowie ein Qualitätsmanagement sind vorhanden.

Mängel im organisatorisch-technischen Bereich bestehen etwa im Bereich von Weisungen, Vorgaben und bei der Umsetzung in Bezug auf verschiedene IT-sicherheitsrelevante Themen. Zudem sind besondere Personendaten auf Servern von Softwarelieferanten gespeichert. Der Datenschutzbeauftragte stellte weiter Schwachpunkte beim Netzwerk und Verbesserungspotenzial bei den Prozessen im Bereich der Zugriffsberechtigungen fest. Er erhielt bislang keine Rückmeldung bezüglich der Umsetzung der Massnahmen.

Datenschutzreview eines privaten Auftragnehmers

Der Outsourcingnehmer erbringt verschiedene IT-Dienstleistungen für private Unternehmen wie auch öffentliche Organe. Neben Softwarelösungen bietet er auch Systemlösungen wie eine Schweizer Cloud an. Rund 50 Zürcher Gemeinden und Städte beziehen Dienstleistungen dieses Outsourcingnehmers. Er ist nach der Norm für Informationssicherheits-Managementsysteme ISO 27001 zertifiziert. Das Risiko des Outsourcingnehmers wurde anhand eines Bewertungsrasters als hoch eingestuft.

Der Datenschutzbeauftragte prüfte beim Outsourcingnehmer neben den organisatorischen und technischen auch juristische Fragen wie die Gewährleistung des Datenschutzes und der Informationssicherheit in Verträgen mit Auftraggebern sowie die Aufbewahrungsdauer, Archivierung und Löschung von Personendaten.

Die Kontrolle zeigte, dass das Unternehmen über ein etabliertes Informationssicherheits-Managementsystem (ISMS) verfügt, das in der Organisation gut verankert ist. In den zentralen rechtlichen, organisatorischen und technischen Prüfbereichen setzt das Unternehmen die Anforderungen des Datenschutzes und der Informationssicherheit umfassend um.

In einzelnen Prüfbereichen sind Optimierungen möglich, beispielsweise kann die Rolle eines internen Datenschutzverantwortlichen geschaffen, sollten die Daten bei der Übermittlung und Speicherung verschlüsselt, ein umfassenden Protokollierungskonzepts erstellt und schliesslich die Verträge mit den Kunden der öffentlichen Verwaltung an die Vorgaben des Kantons Zürich angepasst werden.

Wie erwartet verringerte die Prüfung des Auftragnehmers den Prüfungsaufwand bei den angeschlossenen Gemeinden. Durch die Prüfung des Outsourcingnehmers konnten Rückschlüsse auf insgesamt 19 Gemeinden gezogen werden, die Kunden sind.

Nachkontrolle der Massnahmen-umsetzung

Im Jahr 2017 prüfte der Datenschutzbeauftragte die Umsetzung aller seit 2014 bei Kontrollen empfohlenen Massnahmen. Dafür wurden die geprüften Organe angeschrieben und um Rückmeldung über den Stand der Umsetzung gebeten.

Oft verliefen die Rückmeldungen schleppend oder erfolgten gar nicht. Zudem zeigten die Nachkontrollen, dass die Massnahmen ungenügend umgesetzt worden waren. Teilweise waren gar keine Verbesserungen festzustellen.

Der Datenschutzbeauftragte beschloss, die Nachkontrollen zu intensivieren, um die Wirkung und Nachhaltigkeit der Datenschutzreviews sicherzustellen. Er entwickelt deshalb 2017 ein Konzept zur ständigen Nachkontrolle aller Massnahmen. Damit wird gewährleistet, dass die angetroffenen Risiken und Sicherheitslücken zeitnah behoben werden und die Kontrollen die gewünschte Verbesserung der Informationssicherheit bewirken.