Daten im Auge behalten

27 Den Schutz ausgelagerter Daten verbessern

29 Umfrage und Kontrolle bei der KESB

30 ISMS für die kantonale Verwaltung

31 Entschlüsselung von sicheren Verbindungen

32 Fachexpertise in den Gemeinden

Den Schutz ausgelagerter Daten verbessern

Der Schwerpunkt der Datenschutzreviews lag 2019 auf der Kontrolle von grösseren IT-Dienstleistern, die für Gemeinden, Spitäler und andere öffentliche Organe das Outsourcing des IT-Betriebs erbringen oder als Webprovider tätig sind.

Die aktuellen Bedrohungsszenarien und die zunehmend anspruchsvollere Technik erfordern einen IT-Betrieb auf hohem Sicherheitsniveau mit einer angemessenen Professionalisierung. Bei den Gemeinden ist deshalb eine Tendenz zur Auslagerung des IT-Betriebs festzustellen. Mit den Kontrollen von Auftragnehmern prüft der Datenschutzbeauftragte die Dienstleistungen dort, wo sie tatsächlich erbracht werden. Zudem erzielt er einen Skaleneffekt, weil das Prüfresultat auf alle angeschlossenen Dienstleistungsbezüger angewendet werden kann. Allfällige Verbesserungsmassnahmen entfalten so einen breiten Nutzen.

Bei den Dienstleistern wurde in der Regel eine professionelle Umgebung angetroffen, welche die hohen Anforderungen in den meisten Fällen erfüllen konnte. In einigen Fällen entsprachen die vertraglichen Regelungen nicht den kantonalen Vorgaben, die in den Allgemeinen Geschäftsbedingungen bei der Auslagerung von Informatikleistungen beinhaltet sind. Oft bestanden keine Service Level Agreements mit den Kunden, welche die zu erbringenden Dienstleistungen ausreichend genau und nachvollziehbar beschrieben.

Gemeinden tragen die Verantwortung

In den meisten Fällen fehlten den Gemeinden die Möglichkeiten, um die erbrachten Leistungen zu kontrollieren. Viele Gemeinden waren ungenügend informiert über die Umstände, wie ihr IT-Betrieb erbracht wird. Der Datenschutzbeauftragte rief in Erinnerung, dass auch bei einer Auslagerung das öffentliche Organ die Verantwortung für die Daten und ihre Sicherheit behält.

Der Datenschutzbeauftragte unterstützte Gemeinden und andere kleinere Organe während der Datenschutzreviews und danach bei der Umsetzung von Massnahmen. Er beurteilte Lösungsvorschläge, Konzepte oder Verträge und unterstützte damit die jeweiligen Verantwortlichen auf ihrem Weg zu mehr Informationssicherheit.

Im Zuge unserer Prüfungen und deren Nachkontrollen zeigte sich, dass bei Gemeinden ein grosser Bedarf für Beratungen durch den Datenschutzbeauftragten vorhanden ist. Massnahmen in Bezug auf Datenschutz und Informationssicherheit werden aufgrund von fehlendem IT-Know-how nicht angegangen.

Mängel bei zentralen Plattformen

Der Datenschutzbeauftragte kontrollierte auch zentrale IT-Plattformen der Kantonsverwaltung. Sie bergen ein hohes Risiko für Datenverluste. Zudem kommt ihnen durch ihre Eigenschaft als Datendrehscheibe oder Datenspeicher eine hohe Bedeutung in Sachen Verfügbarkeit zu. Die festgestellten Mängel in der Dokumentation sowie in Verwaltungs- und Kontrollprozessen sind angesichts des hohen Risikos nicht tragbar.

Mehr Informationssicherheit bei weniger Aufwand

Der Datenschutzbeauftragte arbeitete bei den Kontrollen der Gemeinden 2019 erstmals mit der Internen Revision des kantonalen Steueramts zusammen. Sie führt jedes Jahr bei einer hohen Zahl von Gemeinden Steuerprüfungen durch, die auch einzelne Aspekte der Informationssicherheit enthielten.

Um bei Gemeinden doppelte Prüfungen innerhalb kurzer Zeit zu verhindern, werden die Prüfungsplanungen der beiden Stellen neu aufeinander abgestimmt. Der Datenschutzbeauftragte erstellte ein speziell zugeschnittenes Prüfprogramm für die Mitarbeitenden der Steuerrevision und schulte sie, damit sie ihren Prüfauftrag im Bereich Informationssicherheit noch wirksamer ausführen können.

Dank der Zusammenarbeit können mehr Gemeinden kontrolliert und damit das Informationssicherheitsniveau erhöht werden, andererseits werden die Effizienz gesteigert und Synergien genutzt. Zudem werden die Anforderungen an die Gemeinden vereinheitlicht. Die Kontrollen der Internen Revision des Steueramts zeigten in vielen Fällen Verbesserungspotenzial, beispielsweise bei der Regelung der Zugriffs- und Zutrittsrechte.

Unterstützung der Gemeinden

Die Erfahrungen der letzten Jahre zeigten die Schwierigkeiten von Gemeinden, Massnahmen zur Stärkung des Datenschutzes und der Informationssicherheit umzusetzen. Es fehlt kleineren Gemeinden an Zeit, finanziellen Mitteln und dem nötigen Fachwissen, vor allem wenn konzeptionelle Aufbauarbeiten erforderlich sind. Der Datenschutzbeauftragte entwickelte ein Selbstdeklarationsmodell, das die Gemeinden bei der kontinuierlichen Verbesserung ihrer Informatik- und Kommunikationsstrukturen unterstützt.

Für das Selbstdeklarationsmodell stellt der Datenschutzbeauftragte ein Set von Vorgaben und Vorlagen zusammen, das die Mindestanforderungen im Hinblick auf Datenschutz und Informationssicherheit beschreibt und dabei Faktoren wie Grösse der Gemeinde, Anzahl der Mitarbeitenden, IT-Betriebsmodell und eingesetzte Technologien berücksichtigt. Die Dokumente sind so gestaltet, dass die Gemeinden die Massnahmen umsetzen können, ohne über vertiefte Kenntnisse verfügen oder zeitraubende konzeptionelle Arbeiten erbringen zu müssen.

Zu Beginn der Kontrolle nach dem neuen Modell wird die Gemeinde zum Vorgehen und zu den umzusetzenden Massnahmen beraten. In der nächsten Phase setzt die Gemeinde die vorgeschlagenen Massnahmen um. Der Datenschutzbeauftragte kontrolliert danach die Umsetzung und stellt eine Bestätigung aus, wenn die Gemeinde alle Vorgaben erfüllt. Das Selbstdeklarationsmodell baut darauf auf, dass die Gemeinde sich verpflichtet, die Massnahmen auch nach der Kontrolle periodisch zu prüfen und zu aktualisieren. Es wurde an der Versammlung der IG ICT der Gemeinden vorgestellt und stiess auf breite Zustimmung.

Umfrage und Kontrolle bei der KESB

Die Kindes- und Erwachsenenschutzbehörden (KESB) bearbeiten höchst sensitive Personendaten wie medizinische und psychiatrische Gutachten, Details aus dem familiären Umfeld, finanzielle Daten oder polizeiliche Akten.

Der Datenschutzbeauftragte hat im Jahr 2019 bei allen KESB eine Umfrage durchgeführt, um Informationen zu ihrer Grösse, Organisation und ihrem IT-Betrieb zu sammeln. Aufgrund dieser Angaben erfolgte eine Auswahl der KESB, deren IT-Betrieb nicht an eine Gemeinde oder Stadt angeschlossen ist. Der Datenschutzbeauftragte beginnt 2020 mit einer Kontrollreihe bei verschiedenen KESB, um sicherzustellen, dass die Massnahmen zum Datenschutz und zur Informationssicherheit der Bearbeitung der höchst vertraulichen Daten angemessen sind.

ISMS für die kantonale Verwaltung

Am 1. Januar 2020 trat die Verordnung über die Informationsverwaltung und -sicherheit (IVSV) in Kraft. Zusätzlich wurde eine Allgemeine Informationssicherheitsrichtlinie eingeführt, die durch Besondere Richtlinien und Basiskonfigurationen die Vorgaben detailliert regeln sollen. Mit der IVSV soll der Kanton Zürich ein modernes Informationssicherheits-Managementsystem (ISMS) und einheitliche Vorgaben für alle öffentlichen Organe des Kantons erhalten.

Der Datenschutzbeauftragte war in die Vernehmlassungen involviert, wurde jedoch nicht in die Erstellung miteinbezogen. Die Beanstandungen an den eingereichten Dokumenten waren deshalb entsprechend umfangreich.

Für die Erstellung der besonderen Richtlinien kam nun mit dem Amt für Informatik (AFI) eine Zusammenarbeit zustande, wodurch Informationssicherheitsspezialisten des Datenschutzbeauftragten bei der Ausarbeitung der Richtlinien mitarbeiten können. Der Datenschutzbeauftragte begrüsst die Möglichkeit, sich frühzeitig einbringen zu können. Somit fliesst neben seinem spezifischen Fachwissen auch die Erfahrung aus seiner umfassenden Kontrolltätigkeit in die Richtlinien ein.

Entschlüsselung von sicheren Verbindungen

Die Verschlüsselung der Webverbindungen mit dem https-Protokoll ist eine wesentliche Massnahme zum Schutz der Privatsphäre im Internet. Allerdings verwenden Malware-Websites verschlüsselte Verbindungen, um der Entdeckung durch Malwarescanner und ähnliche Systeme zu entgehen. Damit die öffentlichen Organe und ihre IT-Dienstleister gegen solche Angriffe gewappnet sind und Malware herausgefiltert werden kann, werden die Verschlüsselungen oft aufgebrochen. Die Entschlüsselung greift in die Privatsphäre der betroffenen Personen ein, tangiert aber auch die Integrität und Authentizität von Online-Transaktionen. Der Datenschutzbeauftragte hat in seinen Beratungen und Kontrollen festgestellt, dass die Entschlüsselung von Webverbindungen in den meisten Fällen nicht datenschutzkonform ist.

Die Checkliste Entschlüsselung von Webverbindungen auf der Website des Datenschutzbeauftragten zeigt, welche Voraussetzungen erfüllt sein müssen, damit eine Entschlüsselung erlaubt ist. Die folgenden Massnahmen sind dafür zu beurteilen:

- In einer Risikoanalyse und -beurteilung ist aufzuzeigen, dass die Massnahmen zur Risikominderung das Aufbrechen der Verbindung rechtfertigen.
- Die Nutzerinnen und Nutzer sind transparent über die Entschlüsselung zu informieren.
- Über einen definierten Prozess müssen bestimmte Websites von der Entschlüsselung ausgenommen werden können.
- Die Zertifikate für die verschlüsselten Webverbindungen müssen korrekt umgesetzt und behandelt werden.
- Die nötigen technischen Massnahmen für den Betrieb der Internetsurf-Proxy-Infrastruktur müssen sichergestellt sein.
- Die Anforderungen an die Auslagerung von Datenbearbeitungen sind einzuhalten, falls der Internetsurf-Proxy von einem Auftragnehmer betrieben wird.

Fachexpertise in den Gemeinden

Mit der Digitalisierung werden in der Verwaltung immer mehr Prozesse automatisiert oder mithilfe neuer Technologien optimiert. Das Resultat ist ein ständig wachsender Datenfluss. Oft ist es für Verantwortliche in Digitalisierungsprojekten schwierig, die rechtliche und technische Tragweite ihrer Entscheidungen abzuschätzen. Wie können die Informationssicherheit und der Datenschutz praktisch umgesetzt werden? Wie können die betroffenen Mitarbeitenden einbezogen werden? Mit diesen und anderen praxisorientierten Fragen beschäftigten sich 15 Teilnehmerinnen und Teilnehmer im Seminar Informationssicherheit für Gemeinden.

Zu den Lernzielen des Seminars gehörten die datenschutzrechtlichen Anforderungen an die Bearbeitung von Personendaten. Kleine und grosse Gemeinden haben die gleichen gesetzlichen Voraussetzungen an die Informationssicherheit zu erfüllen. Die Teilnehmenden lernten an praktischen Beispielen, die Vorlagen, Anleitungen und Checklisten des Datenschutzbeauftragten anzuwenden.

Gemeinden haben angemessene technische und organisatorische Massnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit und Integrität umzusetzen. So steht es im Gesetz über die Information und den Datenschutz (§ 7, IDG, LS 170.4). Werden Dienstleistungen durch einen Auftraggeber erbracht, sind die Verträge datenschutzkonform zu gestalten. Dazu gehören datenschutzkonforme Allgemeine Geschäftsbedingungen (AGB). Das Amt für Informatik (AFI) stellt auf seiner Website die AGB Auslagerung Informatikleistungen und die AGB Datenbearbeitung durch Dritte zur Verfügung.

Die Komplexität und Heftigkeit der Angriffe auf die IT-Struktur auch von Gemeinden und anderen öffentlichen Organen verlangt nach einem bewussten und strukturierten Umgang mit den Risiken und technisch-organisatorischen Massnahmen. Die Grundlage dafür bilden eine angemessene Organisation und Ziele zur Sicherstellung der Informationssicherheit. Die Vorlagen auf der Website des Datenschutzbeauftragten helfen bei der Umsetzung der nötigen Massnahmen zur Gewährleistung der Informationssicherheit und des Datenschutzes.

Das alltägliche Verhalten der Mitarbeitenden und der Vorgesetzten bestimmt das Sicherheitsniveau einer Organisation. Deshalb sind alle Beteiligten zu schulen und zu sensibilisieren, damit eine Sicherheitskultur entsteht. Dafür eignen sich Informationen in einem persönlichen Gespräch oder an einer Teamsitzung wie auch ein spezifischer Themenworkshop, beispielsweise zum Thema Sichere Passwörter. Weitere Anregungen und Möglichkeiten enthält die Anleitung Sensibilisierung der Mitarbeitenden für Informationssicherheit auf der Website des Datenschutzbeauftragten.

Bekanntgabe der Adressen von Beiständen an Einwohnerkontrolle

Die Weitergabe von Personendaten durch ein öffentliches Organ an ein anderes öffentliches Organ muss gesetzlich vorgesehen sein. Trotzdem kann unklar erscheinen, welche Informationen von einer vorhandenen Rechtsgrundlage umfasst sind. Ein Amt wandte sich an den Datenschutzbeauftragten und wollte wissen, ob die Einwohnerkontrolle einer Gemeinde von einem Kinder- und Jugendhilfezentrum (KJZ) Informationen über Kindesschutzmassnahmen erwarten darf. Die Einwohnerkontrolle wollte den Namen des Beistands im System erfassen und über Adressänderungen informiert werden. Der Datenschutzbeauftragte wies die Einwohnerkontrolle darauf hin, dass Kindes- und Erwachsenenschutzbehörden der Gemeinde Regelungen betreffend die elterliche Sorge über minderjährige Personen melden. Diese Meldung umfasst Namen und Adressen der sorgeberechtigten Personen. Darunter fallen auch Fälle, in denen die elterliche Sorge nur in gewissen wichtigen Bereichen beschränkt wurde und diese Bereiche einem Beistand übertragen worden sind. Besuchsbeistände sind davon allerdings nicht erfasst.