Bedrohte Personendaten

Mangelnder Schutz der Personendaten

Ein durchgängiger Mindeststandard bei der Informationssicherheit ist Voraussetzung für das Gelingen der Vorhaben der Digitalisierungsstrategie. Nur so kann den zunehmenden Risiken von immer ausgedehnteren Datenbearbeitungen und komplexeren Vernetzungen begegnet werden. Eine mangelnde Berücksichtigung des Datenschutzes bei der Umsetzung der Strategie Digitale Verwaltung gefährdet das aktuell ausgeprägte Vertrauen der Bürgerinnen und Bürger in den Staat.

Weiterhin Mängel in der Informationssicherheit

Der Datenschutzbeauftragte führte 2018 verschiedene Datenschutzreviews durch bei Gemeinden, Spitälern und IT-Dienstleistern sowie Checks von Websites, um die Einhaltung der Anforderungen beim Datenschutz in rechtlicher, organisatorischer und sicherheitstechnischer Hinsicht zu beurteilen. Diese Kontrollen zeigten, dass bei allen geprüften Organen weiterhin Mängel in der Informationssicherheit bestanden und im Kanton noch kein einheitliches und ausreichendes Sicherheitsniveau besteht.

Neu wurde 2018 ein Nachkontrollprozess eingeführt, womit die Wirkung der durchgeführten Kontrollen zeitnah und vertieft evaluiert werden kann. Dafür wird die Umsetzung monatlich kontrolliert, indem die geprüften Organe mit einem Schreiben auf die fälligen Massnahmen hingewiesen werden.

Damit reagierte der Datenschutzbeauftragte auf die Erkenntnis, dass bislang der Umsetzungsgrad bei Massnahmen, die bei früheren Kontrollen empfohlen worden waren, bei etwa 50 Prozent lag. Viele Organe hatten Schwierigkeiten, die Massnahmen inhaltlich und terminlich zufriedenstellend umzusetzen. Darunter befanden sich überraschend viele grössere Institutionen wie Spitäler, die über eigene und grössere IT-Abteilungen verfügen. Massnahmen, die grössere konzeptionelle Arbeiten und Änderungen bedingen, wurden während Jahren nicht in Angriff genommen und können jetzt nur schwer nachgeholt werden.

Vielfalt der Institutionen verlangt individuelle Vorgehensweisen

Der Datenschutzbeauftragte hat Massnahmen ergriffen, um die Wirkung seiner Kontrolltätigkeit zu verstärken. Trotzdem reichen die zur Verfügung stehenden Ressourcen im juristischen wie im technischen Bereich nicht zur Erfüllung des gesetzlichen Prüfauftrags. Der Datenschutzbeauftragte erbringt als einzige Instanz die Aufgaben von Prüfungen oder Revisionen der allgemeinen Informationssicherheit innerhalb der kantonalen Verwaltung und vor allem auch bei den Gemeinden. Zwar führen auch die Finanzkontrolle und das Steueramt Revisionstätigkeiten im Bereich der Informationssicherheit durch, sie beschränken sich jedoch auf die entsprechenden Spezialbereiche und Organe.

Insgesamt fallen über 1000 Organe unter den Kontrollauftrag des Datenschutzbeauftragten. Dazu gehören neben den rund 165 Gemeinden alle kantonalen Direktionen und Ämter, die Spitäler, Alters- und Pflegeheime, Schulen aller Stufen, die KESB, Gerichte, selbstständige und unselbstständige Anstalten, RAV, Fachstellen und Auftragnehmer aus der Privatwirtschaft. Die Vielfalt der Institutionen bedeutet eine zusätzliche Beanspruchung der Ressourcen. Die unterschiedlichen Organisationsformen und die sehr breit gefächerten Aufgaben verlangen eine individuelle Einarbeitung und Vorgehensweise.

Nachhaltige Stärkung der Informationssicherheit

Aufgrund von Erkenntnissen aus Kontrollen in Schulen erstellte das Mittelschul- und Berufsbildungsamt (MBA) zusammen mit dem Datenschutzbeauftragten eine Sammlung von Dokumenten zur nachhaltigen Stärkung der Informationssicherheit, um einen allgemeinen Standard für den Datenschutz und die Informationssicherheit zu schaffen (siehe Tätigkeitsbericht 2016, S. 42). Die Unterlagen wurden 2016 und 2017 in verschiedenen Workshops zusammen mit drei Pilotschulen erarbeitet. In einem zweiten Schritt testeten die Pilotschulen 2018 die Praxistauglichkeit der Vorlagen und Dokumente und verbesserten sie. So entstanden Unterlagen, welche die Schulleitungen und die Informationssicherheitsverantwortlichen im Sinne des Management-Kreislaufs bei der Planung, Umsetzung, Überprüfung und Verbesserung der nötigen Massnahmen unterstützen.

Der Regierungsrat beschloss Anfang 2019, die Informatik der Mittel- und Berufsfachschulen gemäss der kantonalen Strategie zu zentralisieren. Dadurch sind die Verantwortlichkeiten für die Umsetzung einzelner Massnahmen neu zu klären. Danach können die vom Datenschutzbeauftragten mit dem MBA erarbeiteten Grundlagen und Vorgaben für die Informationssicherheit an allen Schulen umgesetzt werden.

Systematischer Schutz von bedrohten Personendaten

Der Datenschutzbeauftragte wurde eingeladen, Stellung zu nehmen zur Allgemeinen Informationssicherheitsrichtlinie des Kantons. Sie ist der erste Schritt für den Aufbau eines Informationssicherheits-Managementsystems (ISMS).

Die zunehmende Bedrohung etwa durch Cyberangriffe verlangt nach effizienten, flexiblen und effektiven Mitteln für den Schutz von Informationen, besonders von Personendaten. Ein ISMS stellt dafür universelle Methoden und Werkzeuge bereit. Die Norm ISO / IEC 27001 beschreibt das ISMS und definiert die nötigen Massnahmen anhand des Management-Kreislaufes Planung, Umsetzung, Überprüfung und Verbesserung.

Die wichtigsten Ziele eines ISMS sind:

- Festlegen der Informationssicherheitspolitik und der Sicherheitsorganisation durch die oberste Leitung eines öffentlichen Organs oder Unternehmens (Planung)
- Definieren der Prozesse zur Beurteilung und Behandlung von Informationssicherheitsrisiken (Planung)
- Umsetzen der definierten Massnahmen zur Reduktion der Informationssicherheitsrisiken (Umsetzung)
- Bewerten der Wirksamkeit der Massnahmen zur Risikoreduktion (Überprüfung)
- Sicherstellen einer kontinuierlichen Verbesserung der Informationssicherheit (Verbesserung)

Ein ISMS würde die Informationssicherheit im Kanton nachhaltig unterstützen und stärken. Der Datenschutzbeauftragte begrüsst das Vorhaben. Die Allgemeine Informationssicherheitsrichtlinie und das ISMS wurden noch nicht definitiv verabschiedet.

Elektronische Dokumentation medizinischer Untersuchungen

Ein öffentliches Organ gelangte an den Datenschutzbeauftragten mit einem Projekt, das zum Ziel hat, medizinische Untersuchungen in Zukunft nicht mehr auf Papier, sondern digitalisiert zu dokumentieren. Für dieses Projekt sind die datenschutzrechtlichen Grundlagen für die Verantwortlichkeiten beim Datenaustausch der involvierten Stellen zu berücksichtigen. Die Wahrung des Berufsgeheimnisses der involvierten Ärzte und der Informationssicherheit sind besonders zu beachten.

Der Betrieb der Lösung, die Wartung der Applikation und der Betrieb eines Statistikmoduls sollten an Dritte ausgelagert werden. Die vertragliche Regelung der Auftragsdatenbearbeitung wurde geprüft. Daten, die dem Berufsgeheimnis unterliegen, müssen bei einer Auslagerung verschlüsselt gespeichert und das Schlüsselmanagement muss vertraglich festgelegt werden.

Der Datenschutzbeauftragte hielt fest, dass bei der Auswertung der Daten die Anonymität der betroffenen Personen bei jedem Bearbeitungsschritt zu gewährleisten ist. Die Hinweise des Datenschutzbeauftragten flossen in die Umsetzung des Projekts ein.

Sicherheit von Patientendaten gewährleisten

Der Datenschutzbeauftragte führte während der letzten drei Jahre zehn Kontrollen von Klinikinformationssystemen (KIS) durch bei Spitälern, deren Grösse, Fachbereiche und Organisationsformen unterschiedlich waren. Bei jeder Kontrolle wurden rechtliche Aspekte und Fragen zu Organisation und Technik geprüft.

Medizinische Daten sind sensitiv und als besondere Personendaten eingestuft. Die Anforderungen an den Schutz der Daten und die Informationssicherheit sind erhöht.

Spitäler sehen sich nicht nur mit den üblichen Themen der Informationssicherheit konfrontiert. Weitere Herausforderungen sind:

- die grosse Anzahl Patientinnen und Patienten
- die vielen Mitarbeitenden mit unterschiedlichen Zugriffsbedürfnissen
- eine weitgehend öffentlich zugängliche Infrastruktur
- die Einbindung von Drittanbietern und Lieferanten

Die Prüfungen zeigten Bereiche mit besonderem Verbesserungspotenzial:

- Einhaltung rechtlicher Vorgaben zur Datenbeschaffung und Datenbearbeitung, wie Prozesse zur Gewährung des Auskunftsrechts, die Nachvollziehbarkeit von Datenbearbeitungen und der Schulung der Mitarbeitenden
- Aufbewahrung von Informationen sowie Löschung der Daten nach Ablauf der gesetzlichen Aufbewahrungsfrist
- Definition und Einforderung der vertraglichen Grundlagen, wie Gerichtsstand oder AGBs
- fehlende, lückenhafte oder nicht aktuelle Dokumentationen und Frameworks
- nicht der heutigen Bedrohungslage angepasste Passwortrichtlinien
- keine oder nur geringe Unterscheidungen von Zugriffsrechten der Mitarbeitenden auf Patientendaten
- keine systematischen und umfassenden Schulungsmassnahmen, um die Mitarbeitenden für Risiken und Schutzmassnahmen zu sensibilisieren
- Verwendung von produktiven Daten auf Testsystemen, ohne dass dabei die gleichen Schutzmassnahmen wie auf produktiven Systemen umgesetzt werden
- fehlende Verschlüsselung von gespeicherten oder über interne und externe Netzwerke übertragenen Daten
- fehlende Konzeption und Umsetzung einer Protokollierung von Datentransaktionen

Persönliche Daten im Internet frei einsehbar

Ein unsachgemässer Aufbau oder Betrieb einer Website kann zu Verletzungen von Datenschutz- oder Geheimhaltungsvorschriften führen. Sicherheitsmassnahmen müssen umgesetzt und periodisch kontrolliert werden.

Ein öffentliches Organ machte einschlägige Erfahrungen mit den Risiken des Betriebs einer Website. In der betroffenen Webapplikation waren persönliche Daten während rund dreier Wochen im Internet frei einsehbar. Die Lücke wurde von der Entwicklerin der Webapplikation nach Bekanntwerden umgehend geschlossen. Die betroffenen Personen wurden über den Vorfall nicht informiert. Der Datenschutzbeauftragte wurde durch die Medien auf die Datenpanne aufmerksam gemacht und führte eine Kontrolle durch.

Die Kontrolle zeigte Optimierungspotenzial sowohl ihm rechtlichen wie auch im organisatorisch-technischen Bereich. Der Datenschutzbeauftragte verlangte vom verantwortlichen Organ die Umsetzung von Massnahmen in folgenden Bereichen:

- Einbindung der AGB Auslagerung Informatikleistungen des Kantons Zürich in den Vertrag mit der Entwicklerin der Webapplikation respektive Ergänzung des Vertrags im Rahmen einer Vertragsverlängerung oder -erneuerung gemäss dem Leitfaden Bearbeiten im Auftrag des Datenschutzbeauftragten
- Überprüfung von kritischen Funktionen, bevor eine neue Version der Webapplikation aufgeschaltet wird
- Protokollierung von kritischen Applikations- und Systemereignissen, um die Nachvollziehbarkeit zu gewährleisten
- Überprüfung und Anpassung der Architektur der Webanwendung

Cookie-Warnungen aufgrund der DSGVO

Der Datenschutzbeauftragte stellte fest, dass mit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union auch öffentliche Organe des Kantons Zürich auf ihren Websites Banner mit Informationen über die Verwendung von Cookies und Analysetools platzierten und die Einwilligung der Seitenbesucherinnen und -besucher einholten. Die DSGVO ist auf öffentliche Organe des Kantons Zürich, die ihre Dienstleistungen in der Schweiz erbringen, nicht anwendbar. Der Datenschutzbeauftragte informierte die betroffenen Organe, dass die Cookie-Warnungen nicht nötig seien.

Sorge um Passwörter

Sichere Passwörter schützen Daten. Eine Person bat den Datenschutzbeauftragten, zur Passwortrichtlinie eines kantonalen Internetportals Stellung zu nehmen. Der Datenschutzbeauftragte informierte das Organ über die Thematik.

Bei der Festlegung von Passwortrichtlinien sind der Stand der Technik sowie die Vorgaben von international anerkannten Institutionen wie dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) oder dem US-amerikanischen National Institute of Standards and Technology (NIST) zu berücksichtigen.

Folgende technischen Massnahmen führen zu besseren Passwörtern:

- Lange Passwörter und ganze Sätze ermöglichen
- Mit einer Passworthistorie verhindern, dass bei der Passwortänderung das aktuelle Passwort als neues Passwort gewählt wird
- Die Benutzerinnen und Benutzer bei der Wahl eines Passworts unterstützen: beispielsweise die Passwortstärke grafisch darstellen
- Prüfen, ob das Passwort oder Teile davon in einem Wörterbuch vorkommen
- Zwei-Faktor-Authentifizierung anbieten

Der Datenschutzbeauftragte bietet einen Passwortcheck an, mit dem die Qualität der eigenen Passwörter überprüft werden kann.

Kritische Sicherheitsrisiken in Webanwendungen

Immer mehr Dienstleistungen werden ins Internet verlagert. Neben den Vorteilen ergeben sich daraus auch Sicherheitsrisiken. Der Datenschutzbeauftragte führte 2018 seine Strategie weiter, Auftragnehmende zu kontrollieren. Er entwickelte ein Kontrollprogramm zur Überprüfung von Unternehmen, die Dienstleistungen wie die Bereitstellung und das Hosting von Websites, den Betrieb eines Content-Management-Systems (CMS) und Onlinedienste im Bereich E-Government anbieten. Das Prüfprogramm umfasst Fragen in den Bereichen Recht, Organisation und Technik und kombiniert international anerkannte Standards mit spezifischen Fragen des Datenschutzbeauftragten.

Der Datenschutzbeauftragte erstellte aufgrund der Erkenntnisse aus einer ersten Kontrolle folgenden Massnahmenkatalog:

- Die Verantwortung für den Datenschutz und die Informationssicherheit definieren
- Die AGB Auslagerung Informatikleistungen in den Rahmenvertrag einbinden
- Einen Entwicklungsprozess anwenden, der die Informationssicherheit unterstützt, wie der Secure Development Life Cycle
- Die zehn häufigsten Sicherheitsrisiken für Webanwendungen des Open Web Application Project beachten (OWASP Top 10)
- Regelmässiger Code Review sowie Vier-Augen-Prinzip bei der Freigabe von kritischen Programmteilen anwenden
- Die Passwortsicherheit gewährleisten

Der Datenschutzbeauftragte wird die Kontrolle von Webhosting-Unternehmen fortführen. Von den Kontrollen und den darauf folgenden Verbesserungen bei Auftragnehmern profitieren alle Organe, die Kunden der geprüften Unternehmen sind.

Meldung einer Datenpanne

Bei einem öffentlichen Organ war nach der Migration eines Servers ein Verzeichnis von Bewerberdaten für kurze Zeit im Internet zugänglich. Der Konfigurationsfehler wurde nach der Feststellung sofort behoben.

Das öffentliche Organ meldete die Datenpanne dem Datenschutzbeauftragten mit Datum und Art des Vorfalls, Kategorien der Daten, Anzahl betroffener Personen und eingeleiteten Sofortmassnahmen. Kurz danach folgte ein ausführlicher Bericht über die Ereignisse, die Feststellungen und die getroffenen Massnahmen. Der Datenschutzbeauftragte nahm zur Kenntnis, dass die notwendigen Massnahmen getroffen worden waren und kein weiterer Handlungsbedarf bestand. Die Meldung und die Problembehebung durch das betreffende öffentliche Organ waren vorbildlich.

Das zukünftige IDG sieht für solche Vorfälle neu eine Meldepflicht an den Datenschutzbeauftragten und unter Umständen die betroffenen Personen vor (Vorlage 5471, § 12a revIDG).

SwissID für die Verwaltung

Die SwissID der Firma SwissSign löst die SuisseID der Post ab. Der kostenlose Identifikationsdienst soll zukünftig in allen Bereichen als digitale Identität genutzt werden. Die SwissID soll zur Authentisierung bei Onlinediensten, Banken und Versicherungen wie auch bei Behörden dienen. Die gesetzliche Grundlage ergibt sich aus der Gleichstellung der elektronischen Signatur mit der handschriftlichen Unterschrift nach Art. 14 Abs. 2bis OR.

Aktuell kann die SwissID nur bei der Post genutzt werden. Die anderen Provider und Dienste arbeiten an der Implementation der Lösung. Auch die kantonale Verwaltung möchte in Zukunft zahlreiche Dienste digital anbieten, um so den Gang auf die jeweilige Behörde entfallen lassen zu können. Dabei wird die SwissID eine wichtige Rolle spielen, wenn es um die eindeutige Identifizierung über das Internet geht. Um verschiedene, nicht kompatible Insellösungen zu vermeiden, soll die Nutzung der SwissID zentral organisiert werden.

Der Datenschutzbeauftragte verfolgt und bewertet die Projekte und Initiativen zur digitalen Verwaltung und zu den digitalen Identitätsdiensten. Er wird wenn nötig Massnahmen vorschlagen.

Weitere Themen

Ein öffentliches Organ fragt, ob die Rolle des Chief Information Security Officer (CISO) zwingend geschaffen werden muss: Eine gesetzliche Pflicht besteht nicht. Je nach Grösse des Organs ist es sinnvoll, dass seine oberste Leitung ihre Verantwortung für die Einhaltung des Datenschutzes und der Informationssicherheit an eine Person in der CISO-Rolle delegiert.

Diebstahl von Nutzerdaten bei einem grossen Telekommunikationsdienstleister, der für den Kanton Zürich tätig ist: Der Kanton erstellte in Zusammenarbeit mit dem Datenschutzbeauftragten ein Schreiben, in dem er die stark verspätete Information über den Vorfall kritisierte und unter anderem einen Zeitplan für die Umsetzung verbesserter Sicherheitsmassnahmen verlangte.

Private verlangen von kantonalen Stellen, eine Vertraulichkeitserklärung zu unterzeichnen, bevor sie Einsicht in Personendaten erteilen: Das Vorgehen ist unter privaten Stellen üblich. Für öffentliche Organe ist es nicht anwendbar, da ihre Mitarbeitenden dem Amtsgeheimnis unterstehen.

Beurteilung des Nutzungsreglements einer Schule für die Verwendung von Facebook: Die Regeln für die Nutzung sozialer Medien an Schulen sind im privatim-Merkblatt Datenschutzkonforme Nutzung sozialer Medien durch öffentliche Organe beschrieben. Die Schülerinnen und Schüler sind für die Risiken der Nutzung von sozialen Medien zu sensibilisieren.