Blick in den Tätigkeitsbericht 2019

Mit klarem Kopf in der Cloud

Das Cloud Computing entwickelt sich zu einem Kernthema für die Verwaltung. Viele neue Anwendungen nutzen die Cloud mindestens teilweise und so wandern Daten und Datenbearbeitungen immer weiter weg vom verantwortlichen öffentlichen Organ.

Das Cloud Computing beinhaltet besondere Risiken für den Datenschutz und die Datensicherheit. Viele cloudbasierte Anwendungen sind Standardprodukte. Die rechtlichen Rahmenbedingungen werden durch Allgemeine Geschäftsbedingungen des Anbieters definiert. Oft ist die Grundlage ausländisches Recht und der Gerichtsstand liegt im Ausland. Für das öffentliche Organ erschwert dies die korrekte Rechtsanwendung und -durchsetzung. Es hat deshalb zu vereinbaren, dass die Vorgaben des kantonalen Informations- und Datenschutzgesetzes (IDG) eingehalten werden und ein Gerichtsstand in der Schweiz vorliegt. Für den Bildungsbereich konnte dies mit den grossen Anbietern vereinbart werden.

Weitere Fragen stellen sich bei Daten, die unter dem Berufsgeheimnis im Gesundheitsbereich oder unter einem Spezialgeheimnis stehen, beispielsweise dem Steuergeheimnis oder dem Sozialhilfegeheimnis. Hier lässt sich ein verlässlicher Schutz der Daten nur mit organisatorischen und technischen Massnahmen erreichen. Beim Berufsgeheimnis ist dies durch eine Verschlüsselung und ein Schlüsselmanagement beim öffentlichen Organ möglich. Weiter ist zu berücksichtigen, wie weit ausländische Behörden auf Daten in der Cloud zugreifen können, ohne ein Rechtshilfeverfahren einzuleiten. Dies trifft heute auf US-Firmen zu, die dem CLOUD Act unterliegen.

Die Fragen zum Datenschutz und zur Datensicherheit in der Cloud zeigen Handlungsbedarf auf. Sie sollten in einer Cloud-Strategie der öffentlichen Organe berücksichtigt werden. Zu bedenken wäre eine Regulierung, die die spezifischen Anforderungen des Geheimnisschutzes in der Verwaltung und insbesondere im Gesundheitsbereich aufnehmen würde. Bis es soweit ist, berät der Datenschutzbeauftragte die öffentlichen Organe im Einzelfall. Die allgemeinen Fragen zur Auslagerung der Datenbearbeitungen werden in Merkblättern und Checklisten festgehalten.

International ausgezeichnet
Lehrmittel macht Privatsphäre erfahrbar. **Seite 3**

Vorsicht mit mobilen Geräten
Schulen dürfen Randdaten nicht auswerten. **Seite 2**

Kontrolle behalten bei Auslagerungen
Gemeinden müssen Bedingungen besser kennen. **Seite 3**

Dr. Bruno Baeriswyl
Der Datenschutzbeauftragte
des Kantons Zürich

Dieser Tätigkeitsbericht ist der 25. und letzte in meiner Amtszeit. Ich danke allen, die zur Entwicklung des Datenschutzes und der Informationssicherheit im Kanton Zürich beigetragen haben. Dank dieser Unterstützung kommt der persönlichen Freiheit der Bürgerinnen und Bürger auch bei der Digitalisierung der Verwaltung ein hoher Stellenwert zu. Ich wünsche meiner Nachfolgerin, Dr. Dominika Blonski, und allen Mitarbeitenden, dass ihnen die öffentlichen Organe weiterhin ihr Wohlwollen entgegenbringen.
Sie finden den Tätigkeitsbericht unter www.datenschutz.ch/tb2019.

Mobile Geräte machen alles einfacher?

Schulen rüsten ihre Schülerinnen und Schüler mit Tablets aus. Andere erlauben die Benutzung von privaten mobilen Geräten. Alles easy?

So oder so vermischen sich private und schulische Daten. Was die Schülerin oder der Schüler mit dem mobilen Gerät in der Freizeit tut, darf die Schule nicht interessieren. Wenn etwas online abgelegt wird, wird automatisch ein Zeitstempel zugefügt. Aus diesem Randdatum kann die Lehrperson ableiten, zu welcher Tages- oder Nachtzeit die Hausaufgaben gemacht wurden. Diese Auswertung der vorhandenen Daten ist nicht erlaubt. Solche Randdaten sind zu unterdrücken oder sofort zu löschen. Die Schule darf nur Daten bearbeiten, die zur Erfüllung ihrer Aufgaben nötig sind. Andererseits bleibt sie für die Daten auch verantwortlich, wenn sie auf einem privaten Gerät bearbeitet werden. Sie muss deshalb minimale Sicherheitsstandards auf den privaten Geräten verlangen: ein aktuelles Virenschutzprogramme und eine Firewall sind ebenso Voraussetzung wie die Verschlüsselung von sensitiven Daten bei der Übermittlung und Speicherung.

Eindeutig identifiziert im Bildungsraum Schweiz

Digitale Lernmittel, Cloud-Anwendungen für Schulen – und für jedes Angebot ein eigenes Login mit Passwort. Damit soll Schluss sein. Mit Edulog bekommt jede Person im Bildungsraum Schweiz eine eindeutige Identität – von der Schülerin zur Lehrperson und zur Schulleiterin. Bei solchen Vorhaben sind viele Organisationen mit unterschiedlichen gesetzlichen Auflagen beteiligt: die Schule, die Softwarefirma wie bei Office 365 und die educa.ch, die die Plattform anbietet. Nach der Vorabkontrolle durch den Datenschutzbeauftragten im Auftrag der Bildungsdirektion wurde das System datenschutzfreundlicher gestaltet.

Neue Leitplanken beim Datenschutz

Zürcherinnen und Zürcher bekommen einen besseren Datenschutz. Der Kantonsrat passte das Gesetz über die Information und den Datenschutz (IDG) an die Anforderungen aus der Schengen-Zusammenarbeit und der revidierten Konvention 108+ des Europarats an. Bei neuen Datenbearbeitungen müssen öffentliche Organe die Risiken für die persönliche Freiheit der Betroffenen abschätzen. Datenlecks müssen dem Datenschutzbeauftragten gemeldet werden. Dieser kann die Verwaltung, Gemeinden, Schulen und Spitäler verpflichten, Bestimmungen für einen besseren Datenschutz umzusetzen. Das neue IDG tritt am 1. Juni 2020 in Kraft.

Knowhow bei Gemeinden stärken

Die Komplexität der IT-Strukturen wächst. Von Gemeinden erfordert dies ein solides Wissen über den Umgang mit Risiken und die Schutzmöglichkeiten. Im Seminar Informationssicherheit für Gemeinden lernen die Teilnehmenden, welche Anforderungen bestehen und wie sie die Anleitungen und Checklisten des Datenschutzbeauftragten nutzen können. Letztendlich ist die Sensibilisierung der einzelnen Mitarbeitenden ein Faktor, der über die Sicherheit des Systems entscheidet.

Zürcher Datenschutz international ausgezeichnet

«Weltneuheit aus Zürich» titelte die NZZ, als das Lehrmittel «Geheimnisse sind erlaubt» im Januar 2019 vorgestellt wurde. Zum ersten Mal wird Privatsphäre für Kindergartenkinder erfahrbar. Im Herbst des Jahres wurden die Unterrichtsmaterialien mit dem Global Privacy and Data Protection Award ausgezeichnet, der wichtigsten internationalen Fachauszeichnung. Der Datenschutzbeauftragte entwickelte das Lehrmittel zusammen mit der Pädagogischen Hochschule (PHZH). Sie setzt es in der Lehrpersonenausbildung ein.

Einbürgerungsdaten im Internet aufräumen

Angaben zu Einbürgerungsentscheiden müssen im Internet nach Abschluss des Verfahrens gelöscht werden. So steht es in der Bürgerrechtsverordnung. Sie ist neu, die Löschpflicht jedoch nicht. Sie ergibt sich aus dem datenschutzrechtlichen Grundsatz der Verhältnismässigkeit. Einbürgerungsdaten werden publiziert, um die Bevölkerung zu informieren. Nach Abschluss des Verfahrens ist das Informationsbedürfnis befriedigt. Die Informationen sind in allen online publizierten Protokollen zu löschen.

Kontrolle behalten – auch bei Auslagerung

Angriffe auf IT-Infrastrukturen häufen sich und sie werden immer heftiger. Verschlüsselungstrojaner waren mehrmals bei verschiedenen Institutionen im Kanton aktiv. Dem kann nur mit verstärkter Professionalisierung begegnet werden. Gerade kleinere Gemeinden können die Informationssicherheit durch die Auslagerung der IT-Infrastruktur verbessern. Die Kontrollen des Datenschutzbeauftragten bei Dienstleistern bestätigen dies. Meist traf er eine professionelle Umgebung an.

Doch aufgepasst! Viele Gemeinden haben den IT-Betrieb zwar ausgelagert, kennen aber die Umstände der Auslagerung zu wenig. So können sie die Leistungen eines Rechenzentrums nicht kontrollieren. Gemeinden bleiben jedoch immer verantwortlich für ihre Daten, wie alle anderen öffentlichen Organe auch. Es heisst also: Immer die Kontrolle behalten – erst recht bei Auslagerungen.

Ab 2020 können Gemeinden ihre Informationssicherheit eigenständig und kontinuierlich verbessern, dank dem Modell Selbstdeklaration des Datenschutzbeauftragten. Mit selbsterklärenden Unterlagen werden die Gemeinden Schritt für Schritt bei der Verantwortung für ihre Daten unterstützt. Mit weniger Aufwand erhalten sie den Überblick und eine nachhaltig verbesserte Kontrolle über ihren IT-Betrieb.

Sichere Verbindung entschlüsselt

Das https in der Browseradresse zeigt an, dass die Daten im Internet verschlüsselt übermittelt werden. An sich eine gute Sache im Namen der Informationssicherheit, nur nutzen Kriminelle genau diese Sicherung, um Malware an den Schutzmechanismen vorbei zu schmuggeln. Deshalb kann eine Organisation zum Schutz ihrer Sicherheit an der Entschlüsselung der Daten interessiert sein. Damit greift sie in die Privatsphäre ihrer Mitarbeitenden ein. Der Datenschutzbeauftragte veröffentlichte eine Checkliste, die zeigt, wann eine Entschlüsselung der Daten erlaubt ist.

Mehr Privatsphäre, mehr Sicherheit, selbstgemacht

Auf Smartphones kommt alles zusammen. Telefoniert wird kaum mehr, dafür fotografiert, kommuniziert, organisiert, gespielt, bezahlt, identifiziert, das Auto entriegelt, ein E-Trotti freigeschaltet und die Heizung im Smart Home reguliert. Unter die privaten Daten mischt sich immer mehr Geschäftliches, wenn Mails synchronisiert und Projekte auf Chatplattformen diskutiert werden. Der Handy Boxenstopp ist die Roadshow des Datenschutzbeauftragten, die Mitarbeitende öffentlicher Organe auf ihre Möglichkeiten zur Verbesserung der Informationssicherheit für sich und den Arbeitgeber aufmerksam macht. Direkt am eigenen Smartphone lernen die Interessentinnen und Interessenten in den Ämtern, Schulen und Gemeinden, mit welchen einfachen Vorkehrungen sie ihren Schutz erhöhen können. Der Schutz durch ein Passwort oder einen Fingerabdruck sollte auf keinem Gerät mehr fehlen. Bei Apps sollte immer wieder geprüft werden, welche Berechtigungen warum freigegeben sind.

In 60 Veranstaltungen konnten 2019 über 1200 Mitarbeitende des Kantons und der Gemeinden von spezifisch geschulten Studierenden individuell beraten werden. Der Handy Boxenstopp ist eine Erfolgsgeschichte, die 2020 weitergeführt wird.

Sicherheit mit QR Codes

Der QR Code, dieses Quadrat mit unregelmässigen Punkten, überwindet den Medienbruch von Print zu Digital.

Zwei Sicherheitshinweise:

1. **Eine sichere Scan-App benutzen**
   iOS: Kamera-App zum Scannen verwenden (ab Systemversion 11)
   Android: QR Scanner der Secuso Research Group installieren

2. **Angezeigte Webadresse kontrollieren**

Download
Hier können Sie den Tätigkeitsbericht 2019 herunterladen.

Kontakt
Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

www.datenschutz.ch
twitter.com/dsb_zh
+ 41 43 259 39 99