Datenschutzbeauftragter Kanton Zürich: Tätigkeitsbericht 2019 – Der Datenschutz ist krisentauglich

Mittwoch, 29 April 2020

https://www.datenschutz.de/datenschutzbeauftragter-kanton-zuerich-taetigkeitsbericht-2019-der-datenschutz-ist-krisentauglich/

Medienmitteilung des Datenschutzbeauftragten des Kantons Zürich vom 28.04.2020.

Die Corona-Krise verleiht der Digitalisierung der Verwaltung einen ungeahnten Schub. „Gerade in solchen Zeiten, auch wenn Notrecht angewendet wird, sind die Grundrechte zu wahren, auch dasjenige auf Schutz der Privatsphäre“, betonte Bruno Baeriswyl, der seinen 25. und letzten Tätigkeitsbericht als Datenschutzbeauftragter präsentierte. Die gute Zusammenarbeit des Datenschutzbeauftragten mit den Digitalisierungsgremien und der wirkungsorientierte Einsatz seines Teams in den Bereichen Cloud Computing und Informationssicherheit haben dazu beigetragen, dass die öffentlichen Organe sicher in diese neue Zeit der digitalen Zusammenarbeit übergehen können.

Die Schliessung der Schulen und die Verlagerung der Verwaltungsarbeiten ins Homeoffice verdeutlichten die Herausforderungen für den Schutz und die Sicherheit der Personendaten. Cloud-Lösungen, die sich als Standardprodukte an private Kunden richten, werden oft den datenschutzrechtlichen Anforderungen für öffentliche Organe nicht gerecht. Sie tragen auch beim Cloud Computing die Verantwortung. Deshalb muss die Rechtsdurchsetzung gewährleistet sein. Dafür sind bei der Nutzung von Cloud-Produkten zwingend die Bestimmungen des Gesetzes über die Information und den Datenschutz (IDG) zu beachten und ein Schweizer Gerichtsstand zu vereinbaren.

Abhängigkeit von ausländischen Strukturen

Die Cloud-Verträge für die Verwaltung, Spitäler und andere öffentliche Organe müssen separat verhandelt werden. Es stellen sich Fragen zu den Daten, die unter dem Berufsgeheimnis im Gesundheitsbereich oder einem Spezialgeheimnis stehen, beispielsweise dem Steuergeheimnis oder dem Sozialhilfegeheimnis. Mit organisatorischen und technischen Massnahmen könnte hier ein angemessener Schutz der Daten erreicht werden. Beim Berufsgeheimnis wäre dies durch eine Verschlüsselung und dem Schlüsselmanagement beim öffentlichen Organ möglich.

In diesem Zusammenhang ist auch zu berücksichtigen, wie weit ausländische Behörden auf Daten in der Cloud zugreifen können, ohne ein Rechtshilfeverfahren einzuleiten. Dies ist heute zum Beispiel bei US-Firmen der Fall, die dem CLOUD Act unterliegen. Sie sind verpflichtet, US-amerikanischen Behörden Daten zu liefern, auch wenn diese beispielsweise in der Schweiz gespeichert sind.

Die Fragen rund um den Datenschutz und die Datensicherheit in der Cloud zeigen einen Handlungsbedarf, der in einer Cloud-Strategie der öffentlichen Organe aufgenommen werden und konkret reguliert werden sollte. Dabei wären auch weitere Risiken wie die Abhängigkeit von ausländischen Infrastrukturen zu berücksichtigen.

Gemeinden müssen Verantwortung tragen können

Durch die Digitalisierung wird auch die Informationstechnologie in den Gemeinden immer komplexer. Die gesetzlichen Anforderungen an die Datensicherheit sind für kleine wie grosse Gemeinden gleich. Besonders für kleinere Einheiten ist es schwierig, das nötige Fachwissen in der eigenen Verwaltung zu gewährleisten. Die Auslagerung grosser Bereiche der Datenbearbeitungsaufgaben kann hier zu mehr Sicherheit führen. Der Datenschutzbeauftragte kontrollierte mehrere solcher Dienstleister für die Gemeinden und traf meist eine professionelle Umgebung an. Oft kannten die Gemeinden die vertraglichen Abmachungen der ausgelagerten Datenbearbeitungen nicht genügend. Die Gemeinden sind jedoch immer für ihre Daten verantwortlich. Diese Verantwortung können sie nur wahrnehmen, wenn sie genau wissen, welche Leistungen von den externen Dienstleistern unter welchen Umständen erbracht werden.

Homeoffice lockt Cyberkriminelle

Die ausserordentliche Lage verlagert grosse Teile der Verwaltung ins Homeoffice. Oft müssen die Mitarbeitenden auf ihren privaten Geräten arbeiten. In vielen Fällen war ein gesicherter Zugang zum Geschäftssystem, ein Remote Access, nicht vorgesehen. Dem Datenschutzbeauftragte war wichtig, in dieser Situation schnelle und praxisorientierte Unterstützung zu bieten, damit der Kanton und die Gemeinden ihre Dienste sicher und effizient leisten konnten und die Mitarbeitenden in ihren Herausforderungen zu unterstützen. Dazu evaluierte sein Team Produkte und Dienste für die digitale Zusammenarbeit und veröffentlichte eine Liste der empfohlenen Instrumente auf seiner Website. Sie wurde auch über die Landesgrenzen hinaus rege genutzt.

Eine Krisensituation mit solch grundlegenden und abrupten Veränderungen in der Arbeitsweise stellt für Cyberkriminelle ein wahres Eldorado dar. Plötzlich werden Personendaten, auch besonders schützenswerte, ausserhalb des gesicherten Geschäftsumfeldes gespeichert und als unverschlüsselte Emails verschickt. Das Abgreifen dieser Daten durch Unberechtigte wird so um ein Vielfaches einfacher. Daten, die einmal in falsche Hände geraten sind, sind für immer verloren und können missbraucht werden.

Wer auf seinem privaten Gerät bisher nur gelegentlich Updates aufgespielt hat, der muss dies jetzt zwingend regelmässig tun. Ein Gerät ohne Passwortschutz darf nicht eingesetzt werden. Für jeden Dienst ist ein eigenes starkes Passwort zu verwenden. Neben den technischen Grundregeln müssen auch persönliche Verhaltensregeln eingehalten werden. Daten unter dem Amtsgeheimnis müssen auch gegenüber Familienmitgliedern unter Verschluss gehalten werden, elektronisch und physisch. Daten müssen etwa auf USB-Sticks verschlüsselt gespeichert werden. Nicht mehr benötigte geschäftliche Dokumente sind nach Ablage im Geschäftssystem zu vernichten. Wer physische Dokumente zu Hause nicht schreddern kann, muss diese unter Verschluss aufbewahren, bis sie im Büro sicher vernichtet werden können. Der Datenschutzbeauftragte fasste die wichtigsten Verhaltensregeln für die Arbeit im Homeoffice in einem Leitfaden zusammen. Die Einhaltung dieser Regeln gewährleistet einen Grundschutz beim Bearbeiten von Daten unter dem Amtsgeheimnis in der privaten Umgebung.

25 wirkungsvolle Jahre für den Datenschutz

„Ich bin froh, dass der Datenschutz im Kanton Zürich so gut aufgestellt ist und in Politik und Verwaltung

Gehör findet“, sagte Bruno Baeriswyl an seiner letzten Medienkonferenz als Datenschutzbeauftragter. Auf Ende April geht er nach 25 Jahren im Amt in Pension. Das Grundanliegen des Datenschutzes sei nie infrage gestellt, aber oft herausgefordert worden. So wurden dem Datenschutzbeauftragten Kontrollen verweigert, obwohl dies im Gesetz vorgesehen ist, oder gesetzliche Bestimmungen wurden entgegen der Empfehlung des Datenschutzbeauftragten so erlassen, dass sensitive Gesundheitsdaten bei der Abrechnung bei den Gemeindeverwaltungen landeten.

Vor 25 Jahren musste für einen Internetzugang beim Kanton noch ein begründetes Gesuch eingereicht werden. Vor 12 Jahren kam das Smartphone und führte alle Datenströme zusammen. Jetzt hat die Corona-Krise die Mitarbeitenden der öffentlichen Organe ohne Vorwarnung aus der gesicherten Umgebung der betrieblichen Informationstechnologiestruktur hinauskatapultiert. Die Bevölkerung verlangt nach einem guten Schutz der Privatsphäre beim Staat, auch wenn sie zusehends resigniert gegenüber dem Druck auf ihre Privatsphäre bei Anwendungen von grossen Unternehmen und angesichts der verlockenden Möglichkeiten, die scheinbar kostenlos zur Verfügung gestellt werden. Bruno Baeriswyl wies darauf hin, dass der Datenschutz die notwendigen Rahmenbedingungen für die Datenbearbeitungen in einer liberalen Rechts- und Wirtschaftsordnung setzt. Nicht in der Technologie, aber in ihrer Anwendung muss sich die Demokratie von anderen Systemen unterscheiden, jetzt während der Corona-Krise wie auch in der Zukunft.

Blick in den Tätigkeitsbericht 2019 (PDF, 94 kB)
Tätigkeitsbericht 2019 (PDF, 56 Seiten, 1 MB)

Die Medienmitteilungen des Datenschutzbeauftragten des Kantons Zürich können hier abgerufen werden.
