REPORT

Defizite beim Datenschutz

[21.06.2010] Die aktuellen Tätigkeitsberichte der Datenschutzbeauftragten der Länder Brandenburg und Thüringen stellen Kommunen ein schlechtes Zeugnis in Sachen Datenschutz aus. Die Defizite können nicht alleine mit fehlender Sachkenntnis begründet werden. Vielmehr mangelt es häufig an den notwendigen finanziellen und personellen Ressourcen.

Das Thema Datenschutz ist für die öffentliche Verwaltung heute aktueller denn je, werden doch unter anderem im Zuge von E-Government-Services immer mehr personenbezogene Daten erfasst und verarbeitet. Die Umsetzung datenschutzrechtlicher Vorgaben bereitet vielen Kommunen jedoch noch Probleme.

Olfen: Vertrauliche Daten im Web

Jüngstes Beispiel ist die Stadt Olfen in Nordrhein-Westfalen. Wie der WDR berichtet hatte, waren hier vertrauliche Daten aus dem städtischen Ratsinformationssystem (RIS) möglicherweise jahrelang öffentlich im Internet zugänglich gewesen. Die Panne war zufällig ans Licht gekommen, als ein WDR-Zuschauer im Internet nach einer Politikerin gesucht hatte. Gleich der erste Treffer der Suchmaschine war ein vertrauliches Dokument. Bei Recherchen des Senders tauchten dann weitere nicht öffentliche Dokumente mit hochsensiblen Daten auf. In der Stadt Olfen war das Problem nach Angaben von Bürgermeister Josef Himmelmann zu diesem Zeitpunkt seit über einer Woche bekannt. Die Stadt hatte den Zugriff auf das Ratsinformationssystem bereits gesperrt und überprüft, ob weiterhin nicht öffentliche Dokumente im Netz recherchiert werden konnten. Da dies nicht möglich gewesen sei, sei man davon ausgegangen, das Problem gelöst zu haben, so Bürgermeister Himmelmann gegenüber dem WDR.
Professor Thomas Hoeren von der Universität Münster zeigte sich in einem Bericht des Senders erstaunt über das Verhalten der Stadt, das er als in mehrfacher Hinsicht grob fahrlässig bezeichnete. „Erstmal versteht man nicht, wie die Unterlagen überhaupt ins Netz kommen konnten. Noch schlimmer ist aber, dass die Stadt Tage braucht, um die Unterlagen wieder aus dem Netz zu entfernen“, so Hoeren. Seiner Einschätzung nach könnten auf die Stadt nun Beschwerden der Betroffenen, Schadensersatzklagen oder gar ein Gerichtsverfahren zukommen. Im Gespräch mit dem WDR übernahm der Bürgermeister der Stadt Olfen die volle Verantwortung. Er hoffe, dass die Datenschutzpanne glimpflich ausgehe.
Und die Ursache für die Datenschutzpanne? Nach Angaben von Bernd Thiem, Geschäftsführer der Firma Somacos, deren Rats- und Bürgerinformationssystem SessionNet in Olfen zum Einsatz kommt, hatte die Kommune bei der Bereitstellung von Informationen aus dem Sitzungsdienst auf einem externen Webserver erforderliche Schutzmaßnahmen nicht getroffen. Somacos habe seine Kunden bereits im August 2008 auf mögliche Sicherheitslücken bei Webservern hingewiesen. Thiem: „Leider haben nicht alle Anwender die Sicherheitshinweise, konkreten Installationsanleitungen, Schulungsunterlagen, Hilfe-Dokumente und Testsysteme beachtet. Bildlich gesprochen, wurden im Haus alle Türen zweifach verschlossen und die Fenster auf der Rückseite weit geöffnet.“
Dass sich die Anwendung SessionNet sicher betreiben lässt, wenn Sicherheitshinweise des Herstellers beachtet und der Netzzugang entsprechend abgesichert wird, bekräftigt der kommunale IT-Dienstleister der Stadt Münster, citeq. Das Unternehmen rät Verwaltungen beim Betrieb eines RIS generell zu besonderer Sorgfalt bei der Wahl von Datei- und Ordnernamen sowie des Ortes der Datenablage und empfiehlt – wie es bei der Stadt Münster erfolgreich praktiziert werde – den Online-Zugang zu

vertraulichen Informationen zusätzlich durch einen VPN-Tunnel und eine Nutzeridentifizierung per Token abzusichern. Lothar Lechtenberg von citeq: „Aus unserer Sicht lohnen sich diese Investitionen in eine höhere Sicherheit. Auch kleinere Unbequemlichkeiten bei der Handhabung der sichereren Zugänge sollten in Kauf genommen werden: Denn das Mehr an Sicherheit schafft Vertrauen und bietet eine Chance, die Akzeptanz der Bürger für die Online-Services zu erhöhen."
Die Datenschutzpanne und ihre genauen Ursachen werden die Stadt Olfen jedenfalls noch eine Weile beschäftigen: Da nach Angaben der Firma Somacos der Verdacht auf mögliche strafbare Handlungen besteht, hat die Kommune jetzt die zuständige Aufsichtsbehörde im Kreis Coesfeld sowie den Datenschutzbeauftragten des Landes Nordrhein-Westfalen eingeschaltet.

Mehr Sensibilität gefordert

Dass sich die Kommunen offensichtlich noch nicht hinreichend darüber im Klaren sind, was mit personenbezogenen Dokumenten geschieht, die ins Internet gestellt werden, und welche negativen Konsequenzen dies für die Betroffenen haben kann, hat das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) in seinem aktuellen Tätigkeitsbericht angemerkt. Immer öfter würden beispielsweise in nicht zulässiger Weise vertrauliche Daten aus Sitzungsunterlagen kommunaler Gremien auf den gemeindlichen Web-Auftritten veröffentlicht, da die einzustellenden Dokumente nur unzureichend kontrolliert würden. In Schleswig-Holstein etwa hatten Bürger mehrfach persönliche Daten im Internet gefunden, verbunden mit Details über ihre Einwendungen gegen Bauleitplanungen ihrer Kommune. Laut ULD sollte bei der Einstellung von Dokumenten ins Web daher in jedem Fall das Vier-Augen-Prinzip gelten. Im konkreten Fall hätten die Einwendungen der Bürger gegen die Bauleitplanung zumindest pseudonymisiert und zum Beispiel unter einer Nummer anstelle des Namens im Sitzungsprotokoll veröffentlicht werden müssen.
Und noch ein Umstand ist wohl vielen Kommunen nicht bewusst: Das Internet vergisst nichts. Auch wenn beanstandete Seiten schnell von der Homepage entfernt werden, bleiben sie dennoch im Cache der Suchmaschinen erhalten und damit für jeden Nutzer weiterhin einsehbar. Um Daten tatsächlich dauerhaft aus dem Web zu entfernen, müssen die Speicherinhalte gelöscht werden, was für die Kommunen im Einzelfall einen nicht unbeträchtlichen Aufwand bedeuten kann.

Brandenburg: Schlechte Noten für Kommunen

Aber auch im Umgang mit physischen Daten lassen es die Verwaltungen manchmal an der notwendigen Sensibilität mangeln, wie ein Beispiel aus dem aktuellen Tätigkeitsbericht der brandenburgischen Landesdatenschutzbeauftragten zeigt: So waren im Grundsicherungsamt einer Kommune offene Posteingänge, ausgefüllte Überweisungsträger und komplette Leistungsakten ungesichert auf dem Flur gelagert worden, sodass jeder Besucher Einsicht in die Unterlagen nehmen konnte.
Insgesamt hat in Brandenburg in den Jahren 2008 und 2009 die Mehrheit der Kommunen gegen datenschutzrechtliche Bestimmungen verstoßen. Als geradezu niederschmetternd hatte die Datenschutzbeauftragte des Landes, Dagmar Hartge, laut der Berliner Morgenpost das Ergebnis ihres Tätigkeitsberichts bezeichnet. Unter anderem bei E-Government-Anwendungen und der Umsetzung der EU-Dienstleistungsrichtlinie würden technische und rechtliche Anforderungen zum Schutz der verarbeiteten personenbezogenen Daten noch nicht in vollem Umfang erfüllt. So sei etwa die Authentisierung der Nutzer nicht immer ausreichend sichergestellt und einzelne Anwendungen nicht lückenlos verschlüsselt. Auch existiere in lediglich zwölf Prozent der Kommunen ein IT-Sicherheitskonzept. „Die Kommunen sind sich zwar in vielen Bereichen ihrer Verantwortung hinsichtlich der Gewährleistung des Datenschutzes bewusst. Es fehlt aber in großen Teilen – insbesondere auf dem Gebiet der IT-Sicherheit – an der notwendigen Fachkompetenz sowie an Ressourcen, um die obliegenden Aufgaben

vollständig umzusetzen“, so Dagmar Hartge gegenüber Kommune21.
Über einen behördlichen Datenschutzbeauftragten verfügen inzwischen zwar 80 Prozent der brandenburgischen Kommunen, jedoch können diese ihre Aufgaben kaum erfüllen, da sie in der überwiegenden Mehrzahl weniger als zehn Prozent der regelmäßigen Arbeitszeit dafür aufwenden können. Dagmar Hartge: „Zudem ist häufig selbst der behördliche Datenschutzbeauftragte nicht ausreichend geschult. Es stellt sich die Frage, wie ein Datenschutzbeauftragter ohne ausreichendes Fachwissen auf die Einhaltung des Datenschutzes hinwirken soll.“ Fehlendes Bewusstsein für den Datenschutz will die brandenburgische Landesdatenschutzbeauftragte den Kommunen aber nicht unterstellen. Insbesondere die in der Vergangenheit bekannt gewordenen Datenschutzskandale im nicht öffentlichen Bereich hätten dazu beigetragen, die Kommunalverwaltung weiter für den Datenschutz zu sensibilisieren.

Thüringen: Im negativen Sinne überrascht

Dies alleine nützt jedoch nichts, wenn es Kommunen an Grundlegendem mangelt, um die Anforderungen an Datenschutz und IT-Sicherheit vollumfänglich umzusetzen: genügend qualifiziertes Personal sowie die erforderlichen zeitlichen und finanziellen Ressourcen. Harald Stauch, Thüringer Landesbeauftragter für den Datenschutz (TLfD): „Die Schlussfolgerung kann natürlich nicht lauten, dass die gesetzlich festgelegten Datenschutzanforderungen gesenkt werden. Allerdings müssen Wege gefunden werden, dass es auch kleineren Gemeinden gelingt, einen Grunddatenschutz zu gewährleisten.“
Im Freistaat hatte der aktuelle Tätigkeitsbericht des TLfD, bei dem erstmals auch eine repräsentative Kontrolle von 40 Kommunen unterschiedlichster Größe durchgeführt worden war, ein ähnliches Bild wie in Brandenburg ergeben. „16 der 40 überprüften Kommunen mussten formell beanstandet werden, was einem Anteil von 40 Prozent entspricht“, so Harald Stauch. Und das, obwohl die Hürden für eine Beanstandung nach eigenen Angaben recht hoch angesetzt wurden. Häufigste Mängel seien nicht vorhandene Datenschutzbeauftragte, fehlende oder mangelhafte Sicherheitskonzepte sowie unzureichende oder fehlende Datenschutzvereinbarungen beim Outsourcing der Datenverarbeitung an Privatunternehmen. „Die Quantität und Qualität der Datenschutzmängel hat im negativen Sinne überrascht“, heißt es in dem Bericht. Datenschutzverstöße würden mit abnehmender Größe der Kommune zunehmen.
Die Gründe für den schlechten Datenschutzstandard vor allem in kleineren Verwaltungen sind dem Thüringer Landesdatenschutzbeauftragten zufolge vielfältig: So müsste das Thema stärker in den Fokus der kommunalen Leitungsebene rücken. Auch die relativ schwache rechtliche Stellung des behördlichen Datenschutzbeauftragten und dessen Überlastung mit anderen Aufgaben sowie die unzureichende Personal- und Finanzausstattung der Kommunen sei ein Problem. Im Gegensatz zur brandenburgischen Landesdatenschutzbeauftragten macht Harald Stauch aber auch mangelndes Problembewusstsein der Kommunen sowie fehlende (Rechts-)Kenntnisse und eine wenig ausgeprägte Motivation, die vorhandenen Wissenslücken zu schließen, als Ursachen für die Defizite beim Datenschutz aus. „Auch wenn sich bei vielen Behörden des Landes das Datenschutzbewusstsein verbessert hat, haben die vergangenen zwei Jahre gezeigt, dass es in der Fläche noch zum Teil gravierende Defizite gibt. Das dürfte auch an der ständig fortschreitenden Digitalisierung sämtlicher Arbeitsbereiche der Verwaltung liegen. Um diese begleiten zu können, muss jedoch auch die Datenschutzkontrollbehörde angemessen ausgestattet sein“, so Harald Stauch. Gemeinsam mit dem Gemeinde- und Städtebund Thüringen will der TLfD nun über Lösungsansätze diskutieren, wie die Position des behördlichen Datenschutzbeauftragten gestärkt und die Erstellung von IT-Sicherheitskonzepten vorangebracht werden kann.

Amt Viöl setzt Standards

Dass es auch kleinen Kommunen gelingen kann, Standards in Sachen IT-Sicherheit und Datenschutz zu setzen, zeigt das Amt Viöl (etwa 9.000 Einwohner) im Kreis Nordfriesland: Die Amtsverwaltung hat ein Datenschutz-Management zur Absicherung der internen IT-Systeme und für den Anschluss des internen Verwaltungsnetzes an das Internet etabliert. Für die vorbildliche Verarbeitung personenbezogener Daten auf IT-Systemen wurde die Kommune im Jahr 2009 mit einem Datenschutzaudit-Zertifikat des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) belohnt.

(bs)

Bericht des WDR zur Panne in Olfen Teil 1
Bericht des WDR zur Panne in Olfen Teil 2

Stichwörter: IT-Sicherheit, Datenschutz, Olfen, Somacos, citeq, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Brandenburg, Thüringen, Amt Viöl