11. April 2012 13:28; *Akt: 12.04.2012 14:25*

Datenschützer: «Dumm gelaufen»

Im Rahmen der Ermittlungen um das Datenleck beim Service Médico-Sportif zeigt sich immer deutlicher, dass es um den Datenschutz in Luxemburg schlecht bestellt ist.

Hat die nationale Datenschutzkommission in Luxemburg überhaupt die Mittel, ihre vom Gesetzgeber vorgesehene Rolle bei der Überwachung des elektronischen Datenschutzes zu erfüllen? (Bild: Screenshot/www.cnpd.public.lu)

Nicht nur die Piratenpartei bemängelt seit der Hausdurchsuchung bei ihrem Vorsitzenden im Rahmen der «Medicoleak»-Affäre die Krisen- und Datenschutzpolitik der Regierung. Auch Déi Gréng und der Chaos Computer Club Luxemburg meldeten sich am Dienstag zu Wort. Die Kritik richtet sich vorwiegend an die Regierung.

Das Luxemburger Datenschutzgesetz, das in seiner aktuellen Fassung seit 2011 in Kraft ist, gilt auf dem Papier als eines der umfassendsten und strengsten Europas. Doch durch die Tatsache, dass ein Unbekannter vor knapp fünf Monaten durch das Fehlverhalten eines Benutzers Zugriff auf rund 49 000 Patientenakten bekommen konnte, steht nun die Frage im Raum, wie es tatsächlich um die Sicherheit «sensibler» Datenbanken im Großherzogtum bestellt ist.

Passwortsicherung als Stand der Technik?

Zuerst die Fakten. Der Zugriff auf die betreffende Datenbank war lediglich durch einen Benutzernamen und ein Passwort gesichert, sowie direkt via Internet möglich. Auch ohne «Diebstahl» eines Passworts entspricht dies kaum dem erforderlichen Sicherheitsniveau, welches der Gesetzgeber beim Verfassen des Datenschutzgesetzes im Sinn hatte: Nach den Artikeln 22 und 23 sind die Betreiber von Datenbanken mit sensiblem, personenbezogenen Inhalt verpflichtet, «sämtliche technische und organisatorische Maßnahmen» zu ergreifen, um unbefugten den Zugriff auf die Daten zu verwehren.

Das Gesetz geht noch weiter und schreibt außerdem vor, dass die Sicherheitsmaßnahmen «gemäß dem Risiko einer Verletzung der Privatsphäre, dem Stand der Technik und der Kosten für eine Umsetzung» zu sichern sind.

Strukturelles Problem oder nicht?

Ob dies bei der Datenbank des «Service Médico Sportif» der Fall war, ist zu bezweifeln. Sie enthielt personenbezogene Informationen der gemeldeten Sportler sowie ihrer Familienangehörigen - unter anderem Angaben über chronische Krankheiten, Arzneimittelgebrauch und ethnische Herkunft.

Eine Anmeldung über Benutzername und Passwort über ein offen zugängliches Web-Interface entsprach schon 2005, als die nationale Datenschutzkommission CNPD die

Regierung bleibt stur auf Kurs

In einer Pressemitteilung reagierten die Minister François Biltgen und Romain Schneider am Mittwochnachmittag auf die Vorwürfe, die Regierung wolle in der «Medicoleak»-Affäre vom eigenen Versagen in Sachen Datenschutz ablenken und verfolge jene, die lediglich auf Missstände hinweisen würden.

Viel Neues hatten die zuständigen Minister allerdings nicht mitzuteilen. Einzige Ausnahme: Der Hinweis, die Regierung sei laut Strafgesetz verpflichtet, mutmaßliche Verbrechen zur Anzeige zu bringen und der illegale Zugriff auf personenbezogene Daten sei «kein Kavaliersdelikt».

Zudem wird auf die Unabhängigkeit der Staatsanwaltschaft sowie die Unschuldsvermutung hingewiesen, sowie auf die bereits bekannten Maßnahmen, die zur Schadensbegrenzung und Vorbeugung in Sachen Informationssicherheit in die Wege geleitet worden seien (siehe Artikel).

Erlaubnis für die Datenbank erteilte, längst nicht mehr dem «Stand der Technik». Da klingt es wie blanker Hohn, wenn der für die staatlichen Datenverarbeitungsinfrastrukturen zuständige Kommunikationsminister François Biltgen nach dem Leak am 17. Februar in der Abgeordnetenkammer erklärt, «nicht ein Systemfehler habe den Datendiebstahl möglich gemacht, sondern dieser sei auf die Nachlässigkeit einer Person zurückzuführen».

CNPD als Papiertiger?

Zudem stellt sich die Frage, inwiefern die CNPD ihrer Aufgabe, die Sicherheit «sensibler» Datenbanken zu garantieren, überhaupt gerecht werden kann, angesichts von Personalengpässen und gesetzlichen Ausnahmeregelungen.

Die betroffene Datenbank des Service Médico-Sportif wurde 2005 zwar vorschriftsmäßig bei der CNPD gemeldet, wie Pierre Weimerskirch von der Luxemburger Datenschutzkommission gegenüber «L'essentiel Online» bestätigt. Allerdings sei sie zu diesem Zeitpunkt noch gar nicht in Betrieb gewesen: «Die Struktur und der Inhalt der Datenbank wurden zu einem späteren Zeitpunkt erweitert, was uns jedoch nicht mitgeteilt wurde», so der Datenschützer.

«Lästige Vorsichtsmaßnahme»

Die Sicherung des betreffenden Systems sei nach dem Datenleck erneut in Augenschein genommen worden: «Diese wurde für unzureichend befunden und wir sorgten dafür, dass der Zugang in Zukunft nur mittels Luxtrust-Chipkarte möglich ist, obwohl manche dies als lästige Vorsichtsmaßnahme empfanden».

Die Umstellung laufe derzeit, so Weimerskirch: «Man kann natürlich sagen, es ist dumm gelaufen, dass es so weit kommen musste».

Aus den Augen, aus dem Sinn?

Wie viele Datenbanken mit sensiblen personenbezogenen Daten es derzeit in Luxemburg gibt, kann die Datenschutzkommission nicht sagen. Denn das Datenschutzgesetz wurde 2007 dahingehend geändert, dass eine ganze Reihe Betreiber diese Datenbanken nicht mehr bei der CNPD melden müssen – gerade im öffentlichen und medizinischen Sektor. Insgesamt könnten etwa 50 bis 60 weitere Datenbanken in Luxemburg von ähnlichen Problemen wie denen im Service Médico-Sportif betroffen sein.

Ein Rückschritt, der offiziell im Rahmen der Verwaltungsreform unternommen wurde. Er weist jedoch auch auf die Probleme hin, die bei der praktischen Umsetzung der strengen, legalen Auflagen bestanden. Laut Pierre Weimerskirch fiel die Zahl der Anmeldungen bei seiner Behörde nach der Gesetzesänderung «um 80 bis 90 Prozent».

Volle Kraft zurück

Am 16. März befasste sich der Regierungsrat mit einer Empfehlung des «Cyber Security Board», einem Gremium, das im Juli 2011 nach den weltweit vermehrt auftretenden Angriffen auf Industrierechner ins Leben gerufen wurde, um eine umfassende staatliche Sicherheitsstrategie im IT-Bereich auszuarbeiten. Daraufhin wurde eine Bestandsaufnahme sämtlicher Datenbanken im öffentlichen, parastaatlichen oder kommunalen Bereich beschlossen, sowie eine systematische Sicherung mit Hilfe starker Authentifizierungsmethoden wie etwa der elektronischen Luxtrust-PKI.

Zudem sollen die Benutzer dieser Datenbanken eine Unterweisung in Sachen Informationssicherheit erhalten – ein sinnvoller Ansatz, der jedoch angesichts tausender Beamter und Angestellter einige Zeit in Anspruch nehmen dürfte. Die Regierung rudert also seit dem Datenleck beim sportmedizinischen Dienst mit voller Kraft zurück, was die Vereinfachung beim Zugang von personenbezogenen Datenbanken betrifft.

Das Vorgehen der Regierung läßt eine - leider späte - Einsicht vermuten, dass der Datenschutz in der Vergangenheit zu sehr auf die leichte Schulter genommen wurde.

Datenschutz de facto unwirksam?

Was bleibt, ist ein strenges, aber unwirksames Datenschutzgesetz, das schlussendlich nur auf Repression setzt, wie die Vorgehensweise von Regierung und Justiz in der «Medicoleak»-Affäre zeigt. Sowie eine Datenschutzkommission, der in der Realität nur wenig Möglichkeiten zum Eingreifen bleiben – schon allein aufgrund von Personalengpässen.

Die Datenschutzkommission beschäftigt derzeit neun Mitarbeiter: «Es gibt in Luxemburg heute über 50 000 Datenbankanwendungen mit Netzzugang. Wir haben in den vergangenen zehn Jahren versucht, unsere Aufgabe zu erfüllen. Man muss dazu sagen, dass uns erst dieses Jahr ein Informatiker zugeteilt wurde, um bei der Umsetzung des Datenschutzes zu helfen», erklärt Pierre Weimerskirch.

(Michel Thiel/*L'essentiel Online*)