

Liechtensteiner Verhältnisse in der Kanzlei?

von Volker Andreae, Lecare GmbH

Rechtsanwälte und Mitarbeiter sind zur Berufsverschwiegenheit nach § 202 Strafgesetzbuch (StGB) verpflichtet. Zur Verschwiegenheit gehören sämtliche Informationen, die der Mandant der Kanzlei im Rahmen des Mandatsverhältnisses mitteilt. Nach dem Bundesdatenschutzgesetz sind die mit der Datenverarbeitung beschäftigten Mitarbeiter darauf zu verpflichten, geschützte personenbezogene Daten nicht zu einem anderen als dem zur rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu nutzen.

Aber reicht diese Verpflichtung der Mitarbeiter aus? Ist die Kanzlei nicht verpflichtet, weitere vorbeugende Maßnahmen zu treffen, um einen möglichen, umfassenden Datenklau durch Mitarbeiter oder Internet Eindringlinge zu verhindern oder zumindest den Nachweis führen zu können, nicht fahrlässig gehandelt zu haben? Es soll hier nicht die juristische, sondern die technische Seite betrachtet werden.

Viele Anwälte wiegen sich in trügerischer Sicherheit, durch das tägliche Einwählen aller Mitarbeiter in eine Kanzleisoftware zumindest die technische Seite der Datenschutzverpflichtungen zu erfüllen, denn schließlich wurde für alle User ein Passwort vergeben. Sie vertrauen darauf, dass somit nur Zugriff auf vertrauliche Mandantendaten erhält, wer im Besitz eines gültigen Passwortes ist. Genau diese Annahme ist aber sehr oft falsch und nur sehr wenigen Kanzleien ist dieses Problem überhaupt bekannt.

Viele Anwaltsprogramme schützen zwar die Personen- und Buchhaltungsdaten; auch Fristen, Termine oder Aktendetails werden einem Berechtigungssystem unterworfen. Verbreitet ist aber immer noch Software im Einsatz, deren Daten im Klartext mit jedem Textverarbeitungsprogramm gelesen und manipuliert werden können, ohne dass man sich hierfür in die Kanzleisoftware einloggen müsste.

Abseits dieser softwaretechnischen Dinosaurier besteht aber auch für modernere Programme der große Schwachpunkt in der Speicherung der Dokumente zu der jeweiligen Akte. Auch wenn hier gerne von einer Datenbanksoftware gesprochen wird, heißt dies noch lange nicht, dass die Dokumente etwa in einer Datenbank selbst gespeichert werden. Vielmehr erfolgt die Ablage des Schriftgutes gerne unverschlüsselt auf einem Verzeichnis des Netzwerkserverns und wird so mit der Akte verknüpft, dass das Dokument dieser zugeordnet erscheint und aufgerufen werden kann. Nur in seltenen Fällen wird das Netzwerkverzeichnis hingegen so geschützt, dass die Zugriffsrechte auf Betriebssystemebene mit den Rechten der einzelnen Mitarbeiter in der Anwaltssoftware übereinstimmen. Denn wenn die Betriebssystem-Verzeichnisse nur für einzelne

Mitarbeiter freigeschaltet wären, wäre ein Zugriff über die Akte auch nur für diesen Mitarbeiter und nicht für alle möglich.

Vielmehr ist es durchaus üblich, dass diese Dokumenten-Netzwerkverzeichnisse für jeden frei erreichbar sind, der sich im Netzwerk anmeldet und Dokumente zur Akte erzeugen kann. Die Rechte für Anwaltsprogramm und Dokumentenspeicherung fallen plötzlich auseinander. Nicht selten wird für die Dokumentenspeicherung ein System verwendet, welches seitens der Anwaltssoftware auf dem Server Unterverzeichnisse für die Dokumente automatisch erzeugt, beispielsweise entsprechend der Anlagejahre und der Aktennummern-Endziffern. In diesem Falle ist es bei Kenntnis der Aktennummer besonders leicht, an die Dokumente der Akte zu gelangen, ohne selbst in der Anwaltssoftware Zugriffsrechte auf diese Akte zu haben. Ebenso einfach ist es meist für eine Person mit böswilliger Absicht, das gesamte Dokumentenverzeichnis auf eine CD zu kopieren und – nach dem Liechtensteiner Vorbild – meistbietend interessierten Diensten zu verkaufen.

Das Bekanntwerden eines derartigen Falls wäre für die Anwaltschaft fatal, denn aus Mandantensicht schützenswert sind nicht so sehr die eigene Adresse, das Fremdgeld oder das Aktenrubrum, sondern der Inhalt des Vertragsentwurfes oder eines internen Mandantenmemos.

Abhilfe schaffen könnte hier ein professionelles Dokumentenmanagementsystem, welches dann aber über eine Schnittstelle mit der Kanzleisoftware verbunden sein müsste und eine entsprechende Rechtesynchronisation ermöglicht. Die Alternative besteht in der Integration eines Dokumentenmanagementsystems in die Anwaltssoftware selbst. In diesem Falle werden die Dokumente nicht auf einem Netzwerkserver, sondern in der Datenbank selbst zur Akte gespeichert. Man kann sich die Akte hier wie einen Schrank vorstellen, in dem die Dokumente verwahrt werden und von außen nicht zugänglich sind. Es gibt entsprechend nur ein Berechtigungssystem für Akten und Dokumente, der einheitliche Zugriff ist ausschließlich über das Login in die Datenbank möglich. Nachteil: Es bedarf besonderer Schnittstellen, um beispielsweise einen in der Datenbank gespeicherten Vertragsentwurf per E-Mail an den Mandanten zu versenden.

Der große Vorteil der Speicherung von Dokumenten in einer Datenbank besteht aber – neben dem Zugriffsschutz und der Tatsache, dass Serververzeichnisse mit zehntausenden von Einträgen vermieden werden – in einer umfangreichen Indizierung, die im Dateisystem auf einem Server nicht möglich ist. Das Dokument wird in einem Datensatz gespeichert, der mit beliebig vielen weiteren Informationen ausgestattet sein kann.



rechtsanwalt .com
Besser beraten.

Mehr Erfolg. Mehr interessante Mandate. Mehr Prestige.
**Exzellentes Internet Kanzleimarketing für
Rechtsanwälte mit www.rechtsanwalt.com**

Jetzt informieren und Broschüre anfordern
unter info@arenonet.com

ArenoNet GmbH · Bürohaus Lindenhof · Steubenstraße 46 · 68163 Mannheim · Tel.: 0621-97692950 · Fax: 0621-97692959

Rubrikschwerpunkt EDV

So kann für den Mitarbeiter nicht manipulierbar protokolliert werden, wann ein Dokument von wem angelegt oder verändert oder nur aufgerufen worden ist. Ebenso können Dokumente als grundsätzlich unveränderbar und unlöschbar gespeichert werden, wobei Änderungen nur als weitere Versionen zugelassen werden. Darüber hinaus ist es leicht möglich, Akten samt Inhalt nur für einzelne Mitarbeiter oder Anwälte freizuschalten und für andere unsichtbar zu machen.

In jedem Falle kann mit einer wesentlich höheren Wahrscheinlichkeit ausgeschlossen werden, dass Unbefugte ohne Passwort an Mandantendokumente gelangen oder diese womöglich vollständig kopieren. Selbstverständlich sind trotzdem begleitende Maßnahmen notwendig, beispielsweise in der Rechtevergabe und Protokollierung der Datensicherung.

Aus der haftungsrechtlichen Perspektive des Anwaltes ist jedenfalls zu prüfen, ob die datenschutzrelevanten Vorkehrungen in der Kanzlei dem Stand der Technik entsprechen oder nicht. Bei einer offenen Speicherung von Personendaten und vertraulichen Dokumenten nach dem Stand der Technik von 1985 wird dies möglicherweise zu verneinen sein. Vielen Kanzleien verlassen sich leichtsinnig auf die Annahme, dass die eingesetzte Software schon dem Stand der Technik entsprechen werde, schließlich bezahle man regelmäßig die Updates. Aber selbst wenn dies so wäre, liegt die Verantwortung für den Datenschutz zunächst immer noch bei der Kanzlei selbst, da die EDV aus zahlreichen Komponenten besteht, die sehr unterschiedlich installiert werden können. Auch ein uraltes Programm kann theoretisch betriebssystemseitig so installiert werden, dass alle datenschutzrechtlichen Bedenken entfallen. Mit diesem Einwand ist zu rechnen. Für den täglichen Einsatz ist so ein Programm dann aber nicht mehr zu gebrauchen. Der Liechtensteiner Datenklau hat auf jeden Fall gezeigt, wie sensibel dieses Thema besonders für größere Sozietäten sein kann. Die Lösung ist nicht trivial.

Nächster Rubrikschwerpunkt

EDV:

NJW 44/2008

vom

24. Oktober 2008



LEGAL MANAGEMENT SOFTWARE

*„Herausforderungen
gewinnen wir mit
perfekter Technologie
und optimaler
Crewarbeit“*

*Dr. Tobias Beckmann
Wirtschaftsanwalt und Navigator*

*1. Platz Kieler Woche Senatspreis 2007
1. Platz Bornholm Race 2007
1. Platz Real Race 2007*



WWW.LECARE.COM

Goernestraße 27, 20249 Hamburg
Tel. 040 / 48 00 17-0, Fax 040 / 48 00 17-20,
info@lecare.com

LECARE GMBH