Deutscher Arbeitskreis für Jugend-
Ehe- und Familienberatung (DAKJEF)

Empfehlung zum Datenschutz bei der Nutzung des Internet durch Beratungsstellen

Der Schutz der Vertrauensbeziehung zwischen Ratsuchenden und den beratenden Fachkräften ist für die Institutionelle Beratung konstitutiv[1]. Diese Pflicht der Beraterinnen und Berater ist nach § 203 Abs. I Nr. 4 und 4a strafbewehrt. Die Träger der Beratungsstellen sind gehalten, die Arbeitsbedingungen so zu gestalten, dass die Fachkräfte ihrer Pflicht zur Wahrung von Privatgeheimnissen nachkommen können.

In der Praxis ist dieser Grundsatz unstrittig und der Schutz von Klientendaten gesichert. Die neuere Entwicklung der Kommunikationstechnik macht es aber erforderlich, auf Risiken hinzuweisen, die bei der Nutzung des Internet durch Beratungsstellen entstehen können. In den letzten Jahren haben auch Einrichtungen der Institutionellen Beratung Internetzugänge installiert, die sie für unterschiedliche Aufgaben nutzen. Unter anderem wird auch Beratung selbst über das Internet angeboten. Dazu müssen Sicherheitsstandards beachtet werden.

Grundsätze

Für die Verwendung der Informationstechnik (IT) gelten allgemeine Grundsätze, die auch ohne Zugang zum Internet beachtet werden müssen. Sie stellen sicher, dass Daten vor dem Zugriff Unbefugter geschützt sind. Diese sog. "Organisationskriterien" finden sich sinngemäß im Bundesdatenschutzgesetz (BDSG) und den Datenschutzgesetzen der beiden Kirchen. Die Verantwortlichkeiten beim Umgang mit personenbezogenen Daten sollten in einer Betriebsvereinbarung festgelegt sein.

Gefährdungen durch das Internet

Durch einen Internetzugang entstehen spezifische Gefährdungen für sensible Daten, die sich auf dem genutzten Personalcomputer befinden.

(1) Äußerer Zugriff auf den Personalcomputer

Wenn eine Verbindung zwischen einem örtlichen PC und dem Internet hergestellt wird, besteht grundsätzlich die Möglichkeit, dass von Fremd-Computern im Internet ein Zugriff auf den PC der Beratungsstelle erfolgt. Dabei können personenbezogene Daten gelesen oder verändert werden.

[1] Siehe "Institutionelle Beratung im Bereich der Erziehungsberatung, Ehe-, Familien- und Lebensberatung, Partnerschafts- und Sexualberatung" (1993) in: Grundsatztexte des Deutschen Arbeitskreises für Jugend-, Ehe- und Familienberatung (DAKJEF), 2001, S. 10.

Dagegen bestehen folgende Abwehrmöglichkeiten:

a) Nutzung eines allein stehenden PC
Die einfachste Möglichkeit sich gegen Zugriffe aus dem Internet zu schützen besteht darin, für die Verbindung zum Internet einen (auch älteren) PC zu nutzen, der für andere Aufgaben, insbesondere zur Verarbeitung personenbezogener Daten, nicht benötigt wird. Angreifer von außen treffen dann auf einen PC, der keine wie auch immer gearteten sensiblen Daten enthält.

b) Nutzung einer Firewall
Steht ein eigener Personalcomputer für die Verbindung zum Internet nicht zur Verfügung, sondern muss sie von dem PC aus aufgebaut werden, auf dem auch alle anderen computergestützten Arbeiten, insbesondere Speicherung und Verarbeitung personenbezogener Daten, erfolgen, dann muss dieser PC durch eine Firewall, einen technischen Schutzwall, vor Zugriffen aus dem Internet abgeschottet werden. Die Firewall sollte vorzugsweise als Hardware installiert werden; es ist jedoch auch möglich, eine entsprechende Software auf dem PC aufzuspielen. Die Schutzwirkung der zweiten Variante ist jedoch eingeschränkt.

Wenn in einer Einrichtung von mehreren Personalcomputern aus das Internet genutzt werden muss, dann wird auf die verschiedenen Mail- oder Webserverdienste über das interne Netzwerk (LAN) zugegriffen. Bei dieser Variante ist es erforderlich (und dürfte in der Praxis regelmäßig der Fall sein), das Netzwerk durch eine Firewall (Hardware) zu schützen.

(2) Schädigung durch Viren etc.

Auch dann, wenn ein Personalcomputer durch eine Firewall vor einem direkten äußeren Zugriff geschützt ist, bleibt er aus dem Internet gefährdet. Anhänge eingehender E-Mails können Viren oder andere Schadroutinen enthalten, die beim Lesen der Mail auf dem PC aktiviert werden. Ebenso können aufgerufene Internetseiten präparierte Codes enthalten, die nach der Aktivierung Zugriff auf dem Rechner erlauben. Hiergegen sollte ein stets aktualisiertes Virenprogramm installiert sein, das eingehende Mail-Anhänge automatisiert überprüft, am besten schon vor der Anzeige der Anhänge im Mailprogramm. Die bekannten Mailprogramme übertragen nicht nur den Kopf der Nachricht (Absender, Betreff), sondern den kompletten Inhalt, alternative Mailprogramme können konfiguriert werden, nur den ungefährlichen Header zu übertragen und vor einer Übertragung des Inhalts zu bestimmen, ob die Mail angenommen oder gelöscht werden soll. Gegen die Schadwirkung speziell präparierter Internetseiten helfen so genannte sichere Browser, die ausführbare Codes in html- oder php-Dokumenten erkennen und mit Plugln s (Zusätzen zum Abspielen von Videos, Flashfilmen etc.) sehr sparsam umgehen.

(3) Browser-Fehler

Das auf dem Personalcomputer installierte Programm zur Nutzung des Internet (Browser) kann fehlerhaft programmiert sein und Sicherheitslücken aufweisen. Deshalb sollte der Browser vom Nutzer möglichst "restriktiv" konfiguriert werden (z.B. Deaktivierung von ActixeX-Objekten, JavaScript-Objekten, Java-Objekten etc.).

Nutzung des Internet für Beratung

Beratung kann im Internet derzeit per E-Mail, per Chat oder in Diskussionsforen erfolgen. Software für diese unterschiedlichen Kommunikationsformen ist zu niedrigen Preisen erhältlich. Allerdings ist die Nutzung dieser Software datenschutzrechtlich bedenklich.

E-Mail-Beratung

Ratsuchende nutzen die neuen technischen Kommunikationsmöglichkeiten und wenden sich mit ihren Beratungsanliegen per E-Mail an Beratungsstellen, wenn diese über eine E-Mail-Adresse verfügen - auch dann wenn die Beratungsstellen kein Angebot zur Beratung im Internet macht.

Wenn Beratungsstellen mit gängigen E-Mail-Programmen (z.B. Outlook, Mozilla) Beratung im Internet durchführen, müssen sie sich bewusst sein, dass diese Form der Kommunikation grundsätzlich von Dritten bei der Datenübertragung mitgelesen werden kann. Der Empfänger einer E-Mail kann nicht erkennen, ob die an ihn gerichtete Mail mitgelesen worden ist. Die Mail-Kommunikation kann von Dritten auch verändert werden. Auch dies ist einer Mail nicht anzumerken.

Eine Kommunikation im Internet, die den Erfordernissen des Datenschutzes entspricht, kann auf zwei Wegen gewährleistet werden:

(1) Verschlüsselung durch die Ratsuchenden selbst

Die für einen Mailaustausch genutzten Protokolle smtp und pop3 sind unverschlüsselt. Wenn eine Kommunikation im Internet erfolgen soll, bei der Dritte den Datenaustausch nicht einsehen können, müssen Sender und Empfänger den Modus der Verschlüsselung miteinander vereinbaren und den Schlüssel austauschen, der die Nachricht wieder lesbar macht. Hierzu stehen Programme wie pgp oder gpg zur Verfügung. Sie müssen von Sender und Empfänger installiert werden. Eine bloß einseitige Verschlüsselung (etwa durch die Beratungsstelle) bzw. der Einsatz unterschiedlicher Verschlüsselungsprogramme auf dem Rechner von Sender und Empfänger bewirken einen unverschlüsselten Versand der E-Mail.

Die Installation und der Gebrauch von Verschlüsselungssoftware wirken hochschwellig, weil sie vom Ratsuchenden technisches Geschick und Zeitaufwand abfordert.

(2) Verschlüsselung durch den Leistungsanbieter

Eine Alternative besteht darin, die Kommunikation über einen WebServer zu führen. Dabei werden keine Dokumente über das Internet verschickt, sondern Ratsuchende und Beratungsfachkraft exportieren eine Maske des WebServers auf den eigenen Rechner, in das sie ihre Problemanfrage bzw. die darauf bezogene Antwort eingeben, der Text wird auf dem Webserver abgelegt. Auch hier müssen Daten verschickt werden. Doch die Verbindung zwischen dem WebServer und den Ratsuchenden, die technisch auf der Grundlage des http-Protokolls erfolgt, kann verschlüsselt werden, ohne dass beide Seiten dafür etwas ändern oder einrichten müssen. Dafür wird in der Regel die bei Banken eingeführte SSLVerschlüsselung (Secure Socket Layer) genutzt. Technisch neuer ist die TSL (Transport Security Layer) -Verschlüsselung. Bei beiden Verschlüsselungsvarianten ist keine technische Kenntnis des Anwenders erforderlich, die Verschlüsselung erfolgt durch den WebServer. Die gängigen Browser beherrschen die Umschaltung in den sicheren https-Modus ohne manuelle Konfiguration.

Es reicht auf dieser technischen Grundlage aus, wenn der Rat Suchende für sich bei der Anmeldung einen Nicknamen definiert und ein selbst gewähltes Passwort angibt. Die webgestützte Mail-Beratung ist daher für die Rat Suchenden als niederschwellig einzustufen.

Beratung im Chat

Während bei der Mail-Beratung zeitlich versetzt zwischen Ratsuchenden und Beratungsfachkraft quasi Briefe ausgetauscht werden, bietet die Beratung im Chat die Möglichkeit - wie in der örtlichen Beratungsstelle - zeitgleich miteinander zu kommunizieren. Der Datenaustausch erfolgt üblicher Weise auf der Basis des IRC-Protokolls (Internet Relay Chat). Die zwischen den Gesprächsteilnehmern ausgetauschten Daten werden auf der Grundlage des IRC-Protokolls nicht verschlüsselt. Deshalb genügen die handelsüblichen Chat-Programme den datenschutzrechtlichen Anforderungen für Beratungsprozesse nicht. Erforderlich ist vielmehr eine Verschlüsselung des IRC-Protokolls. Ein verschlüsselter Beratungschat ist technisch auch auf der Basis des https-Protokolls möglich.

Diskussionsforen

Die Diskussion in Foren erfolgt im Internet grundsätzlich öffentlich. Nutzer, die sich bei einem Forum (unter Angabe eines Nicknamens und eines Passworts) angemeldet haben, können Beiträge setzen bzw. auf Beiträge anderer antworten. Datenschutzrechtlich ist zu beachten, dass in diesen Beiträgen (Postings) auch Informationen über Dritte preisgegeben werden können, die aus Gründen des informationellen Selbstbestimmungsrechts dieser Dritten zu löschen sind. Deshalb sollte in Beratungskontexten kein Diskussionsforum ohne Moderation zur Verfügung gestellt werden.

Empfehlung

Die Träger der Einrichtungen der Institutionellen Beratung sind verpflichtet, das Leistungsangebot so zu gestalten, dass für die Ratsuchenden der Schutz ihres Privatgeheimnisses sichergestellt ist. Sie sind zugleich verpflichtet, die Arbeitsbedingungen der Beratungsfachkräfte so zu gestalten, dass diese ihrer Pflicht aus § 203 Abs. I Nr. 4 StGB nachkommen können. Daher empfiehlt der Deutsche Arbeitskreis für Jugend-, Ehe- und Familienberatung Beratungen im Internet mit einer Software durchzuführen, die eine servergestützte (webbasierte) und SSL-verschlüsselte Kommunikation zwischen Ratsuchenden und Beratungsfachkräften gewährleistet.

4.12.2006