Ethikkommission der ÖGWG, Mag. Jürgen Kroemer, 2011

Datenschutz am PC in der Psychotherapie

Die rasante technische Entwicklung geht auch an unserem Arbeitsfeld nicht spurlos vorbei.

Der PC ist für die meisten von uns selbstverständliches Arbeitsutensil und ersetzt den Notizblock, den Karteikasten, das Adressbuch samt Kalender oder den Kassettenrecorder.

Die sichere Verwahrung der uns anvertrauten Informationen bekommt dadurch eine neue Dimension. Einmal in den Computer eingegeben, sind die Informationen im wahrsten Sinne des Wortes nicht mehr greifbar.

Um die Sicherheit eines Karteikastens zu gewährleisten, genügt der „gesunde Menschenverstand": Jeder weiß, wer seine Praxis betreten kann, das Absperren der Türe ist so selbstverständlich, dass niemand darüber nachdenkt.

Was wäre die Analogie am Computer?

Das generelle Passwort, das den gesamten Rechner schützt, entspricht etwa dem Haustor. Nicht sehr sicher, einmal geöffnet ist der Rechner wie ein Haus in dem alle Türen offen stehen.

Welche „Türen" gilt es nun in unserem Daten-Haus zu versperren?

Drei Bereiche lassen sich differenzieren:

- 1. Die personenbezogenen KlientInnendaten selbst, also Name, Adresse, Sozialversicherungsnummer, Geburtsdatum.
- 2. Die Aufzeichnungen über die KlientInnen, also die gesetzlich vorgeschriebene Dokumentation inkl. Diagnose und die persönlichen Aufzeichnungen. Dazu gehören insbesondere Audioprotokolle der KollegInnen in Ausbildung und jener KollegInnen, die an Hand der Aufzeichnungen Forschung betreiben.
- 3. Die Kommunikation mit den KlientInnen und der Austausch vertraulicher Information in der Ausbildung und der Supervision.

ad 1.:Personenbezogene Daten

Die virtuellen Adressbücher, die auf jedem System vorinstalliert sind, eignen sich nicht für die Speicherung von KlientInnen - Daten. Man könnte sie mit einer Telefonliste vergleichen, die offen an der Wand neben dem Apparat hängt und von jedem gelesen werden kann. Diese Daten werden innerhalb des Computers automatisiert und wenig beeinflussbar zwischen den Programmen ausgetauscht. Wenn mehrere Geräte vorhanden sind, also z.B. Handy (Smartphone) oder Laptop werden auch hier die Daten meist automatisch abgeglichen. Eine automatische Weitergabe der Daten erfolgt oft sogar ins www, z.B. bei Synchronisation mit Facebook. Für den privaten Bereich mag das in Ordnung sein, für vertrauliche Daten stellt es ein Sicherheitsrisiko dar.

Es empfiehlt sich also, KlientInnen - Daten in extra Dateien, z.B. einer Excel Liste oder einer eigenen Datenbank zu führen, die gesondert und verschlüsselt abgespeichert werden.

ad 2.: Aufzeichnungen über die KlientInnen

Unverschlüsselte Dateien sind wie offen auf dem Schreibtisch liegende Akten. Jeder, der gerade vorbeikommt, kann sie sehen und das ist im realen wie im virtuellen Sinne zu verstehen.

> Die einzige sichere Methode, um KlientInnen - Daten vor unberechtigtem Zugriff zu schützen, ist die Verschlüsselung.

Es existieren viele Programme für die Verschlüsselung von Daten.

Wir haben uns für das (kostenlose) Open source - Programm „truecryt" (www.truecrypt.com) entschieden und damit exzellente Erfahrungen gemacht.

Beim Einsatz einer Praxissoftware ist zu überprüfen, ob die Daten tatsächlich verschlüsselt abgespeichert werden und ob es möglich ist, verschlüsselte E-mails zu versenden.

ad 3.: Kommunikation

Der Kommunikation via E-Mail entspricht eine Postkarte ohne Umschlag.

E-Mails sollen daher nur Informationen enthalten, die man auch auf eine Postkarte schreiben würde.

Das Risiko, dass vertrauliche Informationen in falsche Hände geraten, ist für E-Mails um ein Vielfaches höher, als für den privaten Computer, da die Internet-Provider und Netzwerke weitaus eher Hacker-Attacken ausgesetzt sind, als der einzelne User.

> Auch für E-Mails gilt daher die Notwendigkeit, vertrauliche Inhalte zu verschlüsseln.

Für den E-mail-Verkehr verwenden wir den Verschlüsselungsstandard Open-PGP (Windows: www.gpg4win.org, Mac: www.gpgtools.org), der weltweit den meist verbreiteten Standard darstellt. Die Programme sind ebenfalls Open source und kostenlos.

Soziale Netzwerke (z.B. Facebook, Twitter, MSN ...) sind zum Austausch vertraulicher Informationen absolut ungeeignet. Es ist auch davon abzuraten, KlientInnen als „Freunde" in sozialen Netzwerken anzunehmen, da dadurch automatische Verknüpfungsmechanismen in Gang gesetzt werden, die zum unfreiwilligen Outing der KlientInnen führen können[1]. Die Anbieter kostenloser Dienste verdienen am Austausch, dem Verkauf und der Verknüpfung von Daten zu Werbezwecken. Wem hier Was zur Verfügung gestellt wird ist vom User kaum bis gar nicht zu kontrollieren.

Ebenso ist abzuraten, Firmen – Accounts zu benutzen. Das Lesen fremder Mails durch Vorgesetzte oder KollegInnen ist zwar verboten, aber in der Praxis ist die Vertraulichkeit der Informationen nicht sicher gestellt.

[1] Es genügt bereits, die e-mail Adressen in irgendeiner Form in Facebook einzuspeisen. Es wird dann automatisch versucht, die Nutzer dieser E-mail Adressen miteinander als „Freunde" zu verknüpfen.

Rechtliche Aspekte

Die Wahrung der Verschwiegenheit wird auch im Rechtssystem unter dem Titel „Datenschutz" prominent abgesichert.

Im rechtlichen Diskurs leitet sich der Datenschutz aus Artikel 8,1 der Europäischen Menschenrechtskonvention (EMRK) ab, der die Privatsphäre schützt[2].

Das österreichische Datenschutzgesetz (DSG) ist die nationale Umsetzung von Art. 8 der europäischen Menschenrechtskonvention. Es hat Verfassungsrang.

Alle Informationen, die wir von und über unsere KlientInnen haben, gelten als „sensible Daten" (§4, DSG), die den höchstmöglichen (i.e. dem aktuellen technischen Stand angemessenen) Schutz erfordern (§14, DSG).

Weitere Gesetze und Verordnungen definieren, was genau darunter zu verstehen ist:

Das Gesundheitstelematikgesetz (GTelG) verlangt für den Austausch von Gesundheitsdaten zwingend den Einsatz kryptographischer Verfahren (§6, GTelG).

Ebenso verlangt die Internetrichtlinie des Gesundheitsministeriums für E-Mails zwischen TherapeutIn und KlientIn (die inhaltlich über allgemeine Information und Terminvereinbarung hinausgehen) zwingend Verschlüsselung (3.6, 3.7.1-2).

Zusammenfassend lässt sich sagen:

Sämtliche Informationen von und über KlientInnen gelten als sensible Daten.

Es ist sicher zu stellen, dass nur berechtigte Personen Zugang zu diesen Informationen haben.

Sensible Daten sind in digitaler Form daher nur verschlüsselt abzuspeichern oder weiterzugeben.

---

[2] „Artikel 8

Recht auf Achtung des Privat- und Familienlebens

(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz."