Bericht zur Kammerveranstaltung „Datensicherheit“ am 12.6.15 in Frankfurt

Auf Einladung der Psychotherapeutenkammer Hessen fand in den Räumen der KVH in Frankfurt am 12.6.2015 eine zweite, gut besuchte Veranstaltung zum Themenbereich „Datensicherheit“ statt. Während es im Mai 2014 um rechtliche Fragen ging, lag nun der Fokus auf dem technischen Datenschutz und um das aktuell im Gesetzgebungsverfahren befindliche E-Health-Gesetz. Vorstandsmitglied **Yvonne Winter** eröffnete den Abend mit der Einleitung, Datenschutz in der Psychotherapie sei ein wichtiger und hochsensibler Bereich. Datenschutz und Datensicherheit sei das Fundament einer Vertrauensbeziehung zwischen Psychotherapeut und Patient. Die absolute Vertraulichkeit (Diskretion) ist die Vorbedingung dafür, dass Menschen sich öffnen und mitteilen können, sie begeben sich in eine geschützte und vom Psychotherapeuten zu schützende Vertrauensbeziehung. Es gehe also nicht nur um ein Betätigungsfeld für einige wenige Technikfreaks, für Psychotherapeuten geht es bei Datensicherheit und Datenschutz um den Schutz einer Vertrauensbeziehung.

In seinen Grußworten erinnerte Kammerpräsident **Alfred Krieger** daran, dass der Deutsche Bundestag gerade erst Ziel eines Hacker-Angriffs geworden ist. Ein Datengroßschadensereignis. Der viel größere Schaden jedoch bestehe im Verlust von Vertrauen. Wer könne trotz vollmundiger Versprechen „Ihre Daten sind sicher“ den Bürgern garantieren, dass mit hochsensiblen Gesundheitsdaten nicht Vergleichbares passiert? Sind sie etwa besser geschützt als der Bundestag? Gesundheitsdaten sind gerade für Wirtschaftsunternehmen hochattraktiv: nicht nur für Krankenkassen und Arbeitgeber, sondern auch für Pharmaindustrie, Medizintechnikfirmen, Versicherungen und Banken. Krieger verwies auf eine Stellungnahme der BPtK zum E-Health-Gesetz wonach die Möglichkeit der offenen und vertrauensvollen Äußerung „nicht erst in Frage gestellt wird, wenn tatsächlich Dritte von der Therapie erfahren, sondern bereits dann, wenn der Patient sich subjektiv nicht mehr auf die Vertraulichkeit verlässt.“ Eine Resolution der hessischen Kammerdelegierten fordert: „Die sensiblen Daten von Patientinnen und Patienten müssen geschützt werden. Sie dürfen auch nicht aufgrund technischer Innovationen, die eine forcierte Datenübermittlung möglich machen, gefährdet werden. Der Schutz der Patientinnen und Patienten und deren Daten muss auch hier Vorrang haben.“ Nicht alles, was technisch realisierbar ist, ist auch ethisch vertretbar.

Wieweit gibt es Datensicherheit angesichts der zahllosen Erfahrungen mit den erfolgreichen Hacker-Angriffen in der letzten Zeit fragte **Dr. Doubrawa**, Datenschutzbeauftragter der Psychotherapeutenkammer Hessen, wenn in nur 5 Minuten ein im WLAN angemeldetes Smartphone entsperrt, Zugriffsrechte geändert, gespeicherte Passwörter und Adressverzeichnisse kopiert werden können? In dieser zunehmend digitalisierten Welt einen verlässlichen Schutz unserer sensiblen Patienten-/Praxisdaten zu errichten ist die zentrale Herausforderung für alle Psychotherapeuten, ob angestellt oder niedergelassen. Er hob hervor, dass es in keinem Bereich absolute Sicherheit geben könne, möglich sei nur eine relative und nach aktuellen Erkenntnissen momentane Sicherheit. Um die Aufrechterhaltung dieser relativen Sicherheit sensibler Patientendaten werden wir Psychotherapeuten uns ständig sorgen müssen!

In dem ersten Vortrag stellte Frau **Carolin Böhmig**, Rechtsanwältin und Referentin der Bundespsychotherapeutenkammer, den Anwesenden das E-Health-Gesetz vor und machte sie mit den für Psychotherapeuten relevanten Regelungen bekannt. Der aktuelle Stand des Gesetzgebungsverfahrens wurde wiedergegeben. Änderungen bis zum voraussichtlichen Inkrafttreten Anfang 2016 sind möglich.

Mithilfe des Gesetzes sollen der Aufbau einer Telematikinfrastruktur gefördert und moderne Informations- und Kommunikationsverfahren in die medizinische Versorgung integriert werden. Die Interoperabilität der aktuell genutzten IT-Systeme soll verbessert werden mit dem Ziel, dass die Infrastruktur der Telematik die zentrale Datenautobahn im deutschen Gesundheitswesen wird und regionale „Insellösungen" vermeidet. Die im Gesetz enthaltenen Maßnahmen, Anreize und Sanktionen zielen auf die zügige Einführung und Nutzung medizinischer und administrativer Telematik-Anwendungen, damit die Telematikinfrastruktur mit ihren Sicherheitsmerkmalen die zentrale elektronische Infrastruktur im Gesundheitswesen wird.

Die Einführung nachfolgender Anwendungen ist ab 2016 vorgesehen: Der Versichertenstammdatendienst (VSDD) soll bis Juni 2016 technisch umsetzbar sein, Ärzte müssen ab 2018 eine Stammdatenprüfung der Versicherten in der Praxis durchführen, wenn sie Honorarabzüge vermeiden wollen. Dabei wird beim ersten Einlesen der elektronischen Gesundheitskarte (eGK) im Quartal eine Verbindung zur Krankenkasse hergestellt und ein Prüfprozess durchlaufen, bei dem die Daten der eGK mit denen der jeweiligen Krankenkasse abgeglichen werden. Für zwei Jahre wird eine „Anschubfinanzierung" gewährleistet beim Einlesen eines elektronischen Entlassbriefes sowie bei der sicheren Übermittlung eines elektronischen Arztbriefes. Für das Erstellen und Pflegen eines Notfalldatensatzes erhalten Ärzte ab 2018 eine Vergütung, dieser Datensatz umfasst Befunde, Medikation und gegebenenfalls zusätzliche freiwillige Informationen. Ab Oktober 2016 haben Versicherte, die mindestens 3 verordnete Medikamente anwenden, einen Anspruch auf die Erstellung eines Medikationsplans durch den Hausarzt, zunächst in Papierform und später auch elektronisch abrufbar auf der Gesundheitskarte. Der Patient hat die Hoheit über seine Daten, d.h. bei allen Anwendungen muss er seine Einwilligung erklären.

Psychotherapeuten haben auf alle Anwendungen der Telematikinfrastruktur Zugriff, sofern ihn Patienten gestatten. Dazu erforderlich ist ein elektronischer Psychotherapeutenausweis (ePtA). Von der Industrie werden diese sogenannten G2-Karten ab Herbst 2015 bereitgestellt werden können, diese Heilberufsausweise sollen die volle Funktionalität nach den Anforderungen der Telematikinfrastruktur enthalten. Die Psychotherapeutenkammern werden allerdings zunächst die Evaluation des Probebetriebes abwarten und dann mit der Ausgabe beginnen. Sie beginnt mit der Antragstellung auf dem Portal eines zugelassenen Anbieters. Die Kammern nehmen dann eine Prüfung vor und erteilen die Freigabe.

Folgende Forderungen hat die BPtK für die Psychotherapeutenschaft:
* Aufnahme und Konkretisierung der Leistungen für die Berufsgruppe der Psychotherapeuten zur Nutzung der Telematikinfrastruktur
* Streichung der Sanktionen
* Zuschläge in Abhängigkeit der Nutzungsfrequenz
* Telemedizinische Leistungen nur bei berufsrechtlicher Unbedenklichkeit
* Aufnahme der BPtK als Gesellschafterin in die Gematik.

Patienten sollen die Hoheit über ihre Gesundheitsdaten haben. Dies betrifft auch die auf der eGK gespeicherten Informationen wie Medikationsplan und Notfalldatensatz.

Über grundlegende technische Voraussetzungen für einen IT-Basisschutz in der Praxis informierte **Frank Micus**, IT Sicherheitsexperte von der SIZ GmbH in Bonn in seinem anschaulichen, praxisnahen Vortrag. Unter Einbeziehung

der Teilnehmer wurden die zur Infrastruktur in der Praxis gehörigen Kommunikationssysteme, auf denen Patientendaten bearbeitet werden können, erörtert. Die Anforderungen, die an den Schutz sensibler Daten gestellt werden, ändern sich von sichtbarem physikalischem Schutz, bspw. verschließbarem Metallschrank hin zu „unsichtbaren“ elektronischen Schutzmaßnahmen.

Mittels des anschaulichen Beispiels eines Hauses, bei dem die verschiedenen Türen und Fenster abgesichert werden, wurden in Analogie die Zugriffsmöglichkeiten auf Computer illustriert. So sollten zur Risikominimierung bei Computern regelmäßig Sicherheitsupdates des Betriebssystems aufgespielt und Aktualisierungen aller Betriebssysteme und zusätzlicher auf dem Rechner genutzter Software (auch Praxisverwaltungssysteme) durchgeführt werden. Natürlich gehören dazu auch aktualisierte Virenschutzprogramme. Einer aktuellen Untersuchung zufolge erfolgen 64% der von Cyberkriminellen ausgenutzten verwundbaren Anwendungen über den Browser. Auch wenn alle diese „Türen“ verschlossen gehalten würden, stellten Mails das wichtigste Einfallstor für Viren und Schadprogramme dar, wie gerade beim Angriff auf den Bundestag geschehen. Sie enthalten sogenannte Links zu möglicherweise bekannt wirkenden Webseiten, um zum Öffnen einer Datei mit schädlichem Programm zu motivieren, was eine „Drive-by-Download“ Aktion startet, bei dem Trojaner/Viren auf den Rechner geladen werden. Anhand von screenshots solcher aktueller Mails konnten sich die Teilnehmer am Erkennen der oft sehr gut kopierten Phishing-Mails erproben.

Ein weiteres Augenmerk galt den heutigen Routern, die selber kleine Computer mit eigener Firewall, Systemsoftware und zahlreichen ergänzenden Funktionen sind. Häufig werden gerade bei diesen zentralen Systemen regelmäßige Sicherheitsupdates vergessen. Im Gegensatz zu früher stellen sie eine dauerhafte Internetverbindung her, weswegen eine sichere WLAN-Verschlüsselung mit einem sicheren Passwort unabdingbar ist. Über Alternativen der sicheren WLAN Nutzung in öffentlichen Räumen (Hotel, Zug, Café) über das eigene Mobilfunktelefon (tethering) oder VPN-Verbindungen wurde ebenfalls informiert. Beim Einsatz von Mobiltelefonen/Smartphones als auch bei Tablets hängen Sicherheitslücken stark von der Aktualität der verwendeten Betriebssysteme ab. So stellt Apple ein geschlossenes Betriebssystem dar, bei dem sich neue Systemupdates sehr schnell im Markt durchsetzen, die Apps werden zentral entwickelt und verbreitet. Bei Android ist das Betriebssystem offen, verwendet werden zahlreiche speziell an Telefonhardware angepasste Versionen und die Apps werden über unterschiedliche Quellen in Umlauf gebracht.

Für alle Geräte -Computer, Telefon/Mobiltelefon (Smartphone), Tablet- empfiehlt sich dringend, eine Verschlüsselungstechnik zu installieren, mit der vertrauliche Daten auf Festplatten, USB-Sticks, Ordner/Dokumente, Kontaktdaten und Mailkommunikation verschlüsselt werden können. Solche Maßnahmen können auch den Schaden bei der neusten Masche von Datendieben begrenzen: Sorglosen Geschäftsreisenden würden in Großraumwagen eines ICE Smartphone oder Laptop entwendet, um mittels der erbeuteten Firmendaten von den Besitzern Lösegeld zu erpressen.

Zum Ende der Veranstaltung stellte **Herr Rückert**, Abteilungsleiter Informationstechnologie der KV Hessen, das KV-SafeNet vor. Aufgrund der vorgerückten Zeit und des sichtbar hohen Informationsstandes der Teilnehmer wurde auf eine Präsentation verzichtet. Es entwickelte sich eine lebhafte, differenzierte und zu großen Teilen kritische Diskussion zu der beschlossenen Einführung des KV-SafeNet. Dies ging von Fragen zu dem für einen „schlichten“ Router relativ hohen Preis, hin zu Hinweisen, dass andere Länder-KVen sich auf andere Modelle der sicheren Datenübermittlung geeinigt hatten und zu der Bitte nach spezifischen Erläuterungen, inwieweit dieses Verfahren sicherer sei als die Datenübermittlung über den bisher verwendeten e-Token.

Kritisiert wurde, dass im Unterschied zur Router-Lösung der e-Token nicht nur kostengünstiger sei, sondern gerade für den kleinen Anwendungsbereich in der psychotherapeutischen Praxis angemessen. Da der Psychotherapeut auf die Konfiguration des Routers keinen Zugriff habe und per Router permanent mit dem Internet verbunden sein müsste, sei der e-Token auch unter Sicherheitsaspekten vorzuziehen.

Herr Rückert verwies darauf, dass nach den Vorgaben der Kassenärztlichen Bundesvereinigung (KBV) nur das KV-SafeNet und das KV-FlexNet künftig zur Übertragung von Abrechnungsdaten zugelassen sind, was die Fortführung des hessischen e-Token ausschließt. Dessen weitere Verwendung in anderen KVen basiert auf dem KV-FlexNet, was aber in Hessen nicht eingeführt wurde. Die Vertreterversammlung habe sich u.a. aus Kostengründen gegen das KV-FlexNet entschieden. Zur Frage der Sicherheit verwies er auf das Zertifizierungsverfahren der KBV für die Router. Diese Prüfung und die dabei von der KBV festgesetzten Gebühren seien im Zusammenspiel mit der begrenzten Nutzergruppe mitverantwortlich für die Höhe der Preise.

Weiterführende Informationen finden Sie auf der Homepage: LPPKJP.de, die Präsentationen sind im Mitgliederbereich hinterlegt.

Yvonne Winter

Juni 2015