Dipl.-Psych.
Matthias Glöckner

Psychologischer Psychotherapeut

Georg-Landgraf-Straße 22
09112 Chemnitz

Telefon: 0371 / 28 333 64
Telefax: 0371 / 28 333 65
praxis@matthias-gloeckner.de

04.09.2018

Entwurf einer sicheren Datenübertragung für die Psychotherapie

Mit viel Bewunderung und mit wenig Begreifen schaue ich auf die Funktionsweise eines Magnetresonanztomografen. Die Behandlungsstühle bei meinem Zahnarzt erinnern mich mit jedem Jahr mehr an das Inventar eines Raumschiffs. Jetzt soll die Gerätemedizin in die nächste Runde gehen – mit der Telematikinfrastruktur (TI). Doch anders als Tomografen und Raumschiffe empfinde ich die TI als eine Beleidigung meiner Intelligenz.
Ich bin technikinteressiert. Ich habe ein Vordiplom in Informatik. Ich bin in der DDR aufgewachsen und habe dort in der Schule gelernt, dass die Kontrolle über Produktionsmittel ein Machtfaktor ist. Die TI stellt die Machtfrage im Gesundheitswesen in weit größerem Umfang als bildgebende Diagnostik und Zahnarztstühle es je könnten. Der GKV-Spitzenverband gibt das unumwunden zu[1].
Die große Mehrheit der Entscheider über die TI, vom Krankenkassenvorstand bis zum Gesundheitsminister, hat mit uns Anwendern eines gemeinsam: das fehlende Wissen über Rechner- und Netzwerkarchitektur, über Verschlüsselung und Authentifizierung. Wenn wir bei der digitalen Transformation unseres Berufs Professionalität erwarten, müssen wir dieses Fachwissen selbst erwerben und können nicht auf potenzielle Prediger in der Wüste bei der Gematik oder in der Wirtschaft warten.
Wir sind diejenigen, die im Psychologie-Studium gelernt haben, statistisch-empirischen Aussagen im Zweifel mehr zu glauben als Worten. Die Überlegenheit der Mathematik über die Poesie ist bedauerlich und mag etwas mit dem Unbehagen in der Kultur zu tun haben. (Wer liest noch Freud?) Die TI erinnert uns einmal mehr an die schlechte Nachricht, dass auch nach erfolgreicher Psychotherapeutenprüfung die von den meisten von uns ungeliebte Statistik keineswegs hinter uns liegt. Die gute Nachricht ist, dass IT-Sicherheit uns nicht fremd ist, denn im Wesentlichen beruht sie auf der Wahrscheinlichkeitsrechnung[2].

---

1 https://www.aerztezeitung.de/politik_gesellschaft/krankenkassen/article/970720/telematik-staerkeres-stimmrecht-kassen.html

2 https://de.wikipedia.org/wiki/Stochastik

»Si qua occultius perferenda erant...«

Auch der römische Feldherr Gaius Julius Caesar kannte Verschlüsselung. In den Nachrichten an seine Truppen, die nicht in die Hand des Feindes fallen durften, ersetzte er jeden Buchstaben durch den an 3. Stelle nachfolgenden Buchstaben. Anstelle »Telematikinfrastruktur« hätte Caesar »Whohpdwlnlqiudvwuxnwxu« geschrieben. Dieser simple und dennoch einschüchternd wirkende Code ist als Caesar-Verschlüsselung[3] bekannt. (Für die Psychoanalytiker*innen unter uns: auch als Caesar-Verschiebung.)

Ein modernes Beispiel: das Kryptomodul der Kassenärztlichen Bundesvereinigung

Das Prinzip, das genutzt wird, um Daten zu verschlüsseln, ist bis heute gleich geblieben, nur die Verschlüsselungsschritte sind komplizierter geworden. Wer mit der Kassenärztlichen Vereinigung abrechnet, schickt dorthin am Ende jedes Quartals eine Datei mit den Abrechnungsdaten. Öffnet man diese Datei, die auf ».CON.XKM« endet, mit einem Texteditor, entdeckt man ähnlich unleserliche Zeichenfolgen wie die obige aus der Caesar-Verschlüsselung. In einer anderen Datei, die nur auf ».CON« endet, stehen die Abrechnungsdaten im Klartext. Wegen der Schweigepflicht darf diese Datei die Praxis nicht verlassen.
Wer das Verzeichnis seiner Praxisverwaltungssoftware weiter durchsucht, findet die Datei »Oeffentlich_KV_V06.key«, die den Schlüssel enthält, der ».CON« in ».CON.XKM« umcodiert. Beim Blick in die ».key«-Datei ist neben viel Kryptischem (dem binär abgespeicherten, eigentlichen Schlüssel) auch der Text »java.math.BigInteger« zu sehen. Ein kryptografischer Schlüssel ist immer eine ganze Zahl, auf Englisch: »integer«. Bei Caesar war es die Zahl 3. Heutige Schlüssel sind länger: im Fall des KBV-Kryptomoduls sind es 2048 Bit, das entspricht einer Dezimalzahl mit 617 Stellen. Und was für Caesar die Vertauschung war, ist für die KV-Abrechnung der Algorithmus nach Rivest, Shamir und Adleman[4].
Die meisten Bestandteile der Datenübermittlung zur KV-Abrechnung sind für jeden zugänglich: der RSA-Algorithmus und die Datei mit dem öffentlichen Schlüssel der Kassenärztlichen Bundesvereinigung[5]. Auch die verschlüsselten ».CON.XKM«-Dateien dürfen in fremde Hände gelangen. Sie sind durch das einzige Geheimnis im Verfahren geschützt: den privaten Schlüssel der Kassenärztlichen Bundesvereinigung. Als zusätzliche Sicherheit werden öffentlicher und privater Schlüssel regelmäßig ersetzt, zuletzt im Februar 2018.

»...qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.«

Im Jahr 1883 veröffentlichte der niederländische Linguist Auguste Kerckhoffs seine Schrift »La cryptographie militaire« (Die militärische Kryptografie). Darin formulierte er einen Grundsatz für sichere Kommunikation, der bis heute gilt: Die Sicherheit des Verfahrens darf sich allein auf die mathematische Stärke des Verschlüsselungsalgorithmus und auf die Geheimhaltung des Schlüssels stützen. Falls der Rest des Systems bekannt wird, darf kein Schaden entstehen. Wie

[3] https://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsselung

[4] https://de.wikipedia.org/wiki/RSA-Kryptosystem

[5] ftp://ftp.kbv.de/ita-update/KBV-Software/Kryptomodul/

weit die TI von Kerckhoffs´ Prinzip entfernt ist, macht der Hausarzt Dr. med. Stefan Streit in seinem Vortrag »Ich komme aus einem anderen Land - Telematik in der Medizin«[6] deutlich.
Als Mensch des 19. Jahrhunderts mag Kerckhoffs uns weniger cool erscheinen als ein junger, dynamischer Minister unserer Zeit. Viele Menschen sehnen sich eher nach einer Utopie als nach einer Statistik. Vielleicht aus diesem Grund schrieb Hans Jonas in seinem Buch »Das Prinzip Verantwortung«: »Was aber die so nötige Verbesserung der Bedingungen betrifft, so ist es höchst notwendig, die Forderung der Gerechtigkeit, der Güte und der Vernunft vom Köder der Utopie freizumachen.«

Quelloffen, Ende-zu-Ende, dezentral

Ich bin überzeugt, dass eine quelloffene[7] Ende-zu-Ende-Verschlüsselung[8] mit dezentraler Speicherung der Schlüssel alle Anforderungen erfüllt, die wir Psychotherapeut*innen auf absehbare Zeit an unsere digitale Kommunikation haben. Das Verstehen fremder Menschen habe ich zwar zu meinem Beruf gemacht. Dennoch interessiert es mich nicht, in welchen medizinischen Fächern die TI der möglicherweise einzige Weg für Patient*innen ist, Einsicht in ihre Patientenakte zu bekommen oder welche technischen Anforderungen für den Notfalldatensatz gelten.
Ich möchte auf möglichst sichere Weise elektronische Nachrichten mit Patient*innen, Ärzt*innen, Psychotherapeut*innen, Krankenkassen und der Kassenärztlichen Vereinigung austauschen. Auch wenn die »Fünf Augen« USA, Großbritannien, Australien, Kanada und Neuseeland ihre Anstrengungen verstärken, Verschlüsselung zu umgehen, weil sie mathematisch nicht unwirksam zu machen ist, müssen wir in Europa unsere Technologien nicht in möglicherweise vorauseilendem Gehorsam schwächen.[9]
Ähnlich der Akzeptanz- und Commitmenttherapie gehe ich von meinen Werten aus und richte meine Handlungen danach – nicht umgekehrt. Meine Werte in der digitalen Transformation der Psychotherapie folgen aus dem Datenschutz mit den Mitteln der Statistik, so wie Kerckhoffs sie in seinen sechs Punkten[10] formulierte. Dabei lehne ich die trügerische Sicherheit einer »Sicherheit durch Unklarheit«[11] ab, von der die TI nach jetzigem Wissen durchsetzt ist. Beispielsweise existiert trotz verpflichtender Einführung der TI bislang keine verbindliche Spezifikation der elektronischen Patientenakte.
Für uns Psychoterapeut*innen wünsche ich mir eine quelloffene, weitgehend softwarebasierte Lösung, die die Komplexität des KBV-Kryptomoduls und den Datenumfang von E-Mails kaum übersteigt. Ich denke, dass es unserem Berufsstand möglich wäre, etwas derartiges aus eigenen intellektuellen und finanziellen Mitteln zu entwickeln.
Als Grundlage bietet sich OpenPGP-Verschlüsselung[12] an, deren Benutzung schon jetzt zufriedenstellend ist, die jedoch insbesondere auf Smartphones und bei der Verwaltung ihrer öffentlichen Schlüssel auf Schlüsselservern noch einfacher werden muss. Nebenbei bemerkt: Bisher nutzen

6 https://www.youtube.com/watch?v=dCV8bkaaTJo&t=489

7 https://de.wikipedia.org/wiki/Open_Source

8 https://de.wikipedia.org/wiki/Ende-zu-Ende-Verschl%C3%BCsselung

9 https://twitter.com/dasSubjekt/status/1036909085306880000

10 https://de.wikipedia.org/wiki/Kerckhoffs%E2%80%99_Prinzip

11 https://de.wikipedia.org/wiki/Security_through_obscurity

12 https://de.wikipedia.org/wiki/OpenPGP

vier meiner Patient*innen OpenPGP, um mit mir über E-Mail zu kommunizieren. Es ist also nicht schwer zu erlernen.
Krankenkassen und ein Teil der Ärzteschaft werden ein solches System, das zwar unkompliziert ist, aber in Konkurrenz zur TI steht, wahrscheinlich nicht nutzen. An sie können wir weiterhin Briefe versenden. Für Patient*innen, denen nach differenzierter Aufklärung über Chancen und Risiken der flexible Umgang mit ihren Gesundheitsdaten wichtiger ist als bestmöglicher Datenschutz, könnten die von ihren Psychotherapeut*innen elektronisch signierten Dokumente an zentraler Stelle in die TI eingespeist werden, zum Beispiel bei den Psychotherapeutenkammern. Dorthin gelangen würden die Daten mit OpenPGP.
Inwieweit OpenPGP auch zur Verschlüsselung von Bildübertragungen bei Videosprechstunden taugt, weiß ich noch nicht. Sollte dort eine gesonderte Lösung notwendig werden, können wir zu gegebener Zeit die Vor- und Nachteile alternativer Übertragungstechniken zielgerichtet abwägen, ohne uns auf eine unüberschaubare Pauschallösung wie die TI einzulassen.
Forderungen, wie jene des GKV-Spitzenverbands, es dürfe bei der Digitalisierung des Gesundheitswesens keine Doppelentwicklungen geben, verwirren mich als gelernten DDR-Bürger. Ist das nicht Planwirtschaft? Verfechter der Zentralisierung sollten zur Kenntnis nehmen, dass die dezentrale Speicherung von Schlüsseln und Passwörtern sicherer ist als die zentrale[13]. Das Kryptomodul der Kassenärztlichen Bundesvereinigung belegt, dass mit den relativ geringen Mitteln mathematischer Stringenz und statistischer Wahrscheinlichkeitsabschätzung ein sehr guter Datenschutz zu erreichen ist. Dazu braucht es keine Maschinerie, die eines Zauberers von Oz[14] würdig wäre.
Apropos Homöopathie: Krankenkassen, die sagten, ihre Versicherten wünschten, in den Genuss der Vorteile der TI zu kommen, sagten auch, ihre Versicherten hätten ein Recht auf Kostenerstattung für Homöopathie.

»Wer die Psychologie liebt,...«

… der schiebt sich das LAN-Kabel des TI-Konnektors in seinen Praxislaptop? Wir Psychotherapeut*innen sind es gewohnt, wissenschaftliches Denken und berufliches Erfahrungswissen mit Geduld so lange zu wiederholen, bis Patient*innen es verstanden haben und fähig sind, es in ihr Verhalten zu integrieren. In ähnlicher Weise müssen wir nun gegenüber der TI zunächst uns selbst darüber bilden, was die Forderung Klaus Grawes »Von der Konfession zur Profession«[15] für die digitale Transformation bedeutet. Dieses Wissen müssen wir dann beharrlich und geduldig gegenüber den Entscheidungsträger*innen im deutschen Gesundheitswesen vertreten. Ihnen werden wir Psychotherapeut*innen über die Sicherheit der Daten unserer Patientinnen und Patienten sagen:

»Aber sie fällt nicht vom Himmel. Sie ist kein Weihnachtsgeschenk. Sie wächst nicht wie das Gras. Sie ist weder ein Wunder noch ein Naturprodukt. Sie ist Handlungsauftrag. Wir handeln, Sie reden. Das ist der Unterschied.«[16]

---

13 https://www.security-insider.de/mehr-passwort-sicherheit-durch-dezentrale-speicherung-a-623008/

14 https://www.youtube.com/watch?v=YWyCCJ6B2WE

15 https://www.hogrefe.de/shop/psychotherapie-im-wandel-64104.html

16 http://dipbt.bundestag.de/doc/btp/13/13198.asc