

# Praxisüberwachung

Die ärztlichen und psychotherapeutischen Praxen in Deutschland müssen bis zum Jahr 2011 einen Spionage-Router in ihre Computernetzwerke einsetzen. Ein Recherche- und Erfahrungsbericht.

*Lew Palm, lew@tzi.de, 27. September 2010*

## Zusammenfassung

Zur Zeit werden die meisten Praxen in Deutschland von den Kassenärztlichen Vereinigungen zu einer Anbindung an ein Netzwerk namens „KV-SafeNet“ über das Internet gezwungen. Ich bin Informatiker und betreue die Computersysteme einer psychotherapeutischen Praxis. Mir sind grobe Sicherheitsmängel in Konzeption und Ausführung dieser Umstellung aufgefallen, jedoch kein Nutzen für Ärzte, Therapeuten oder Patienten. Des Weiteren sehe ich gesellschaftliche und politische Gefahren und die Möglichkeit, dass die eingesetzte Technik sich sehr einfach zum Überwachen des gesamten internen Datenverkehrs jedes lokalen Praxis-Computernetzwerkes verwenden lässt.

Die niedergelassenen Ärzte und Psychotherapeuten in Deutschland rechnen ihre Leistungen nicht direkt mit den gesetzlichen Krankenkassen ab, sondern sie tun dies über Mittlerinnen, die Kassenärztlichen Vereinigungen (KVen). In jedem Bundesland gibt es eine KV und gemeinsam sind sie in der Kassenärztlichen Bundesvereinigung (KBV) organisiert, die vom Gesundheitsministerium kontrolliert wird. Vereinfacht gesagt haben die KVen auch noch den öffentlichen Auftrag, die knapp 150000 Praxen so zu organisieren, dass sie im Interesse der etwa 72 Millionen gesetzlich Krankenversicherten wirken können<sup>1</sup>.

In der von mir betreuten Praxis wurde bislang das Versenden der KV-Abrechnung, welches quartalsweise ansteht, durch das persönliche Überbringen von feststofflichen Datenträgern bewerkstelligt. Dazu wurden eine CD, Diskette oder Papiere direkt zur Geschäftsstelle der Kassenärztlichen Vereinigung gebracht. Dem Praxispersonal war das recht, der Aufwand ist nicht sehr groß. Mir als IT-Verantwortlichem gefiel es auch, denn so muss-

te kein Praxisrechner am Internet hängen (und die Sicherheit der persönlichen Datenübertragung ist ungeschlagen hoch). Die für Abrechnungen in dieser Praxis verwendbare und auf dem Markt existierende Software setzt zwingend ein Microsoft Windows als Betriebssystem voraus. Es wird mit sehr schützenswerten Daten der Patienten umgegangen, aber und eine Vielzahl von nachlässig betreuten Windows-Computer ist mit Backdoors bzw. Rootkits verseucht. Deswegen wollte ich eine Anbindung der Praxis an das Internet vermeiden, da sie einen unverhältnismäßig hohen Aufwand an Sicherheitsmaßnahmen erforderlich gemacht hätte. Alle mir bekannten psychotherapeutischen Praxen der Umgebung lieferten die Abrechnungsdaten persönlich bei der KV ab; es ist aber zu vermuten, dass viele andere (bei größerer räumlicher Entfernung zum nächsten KV-Büro) ihre Abrechnung per Einschreiben über den Postweg versendeten.

Doch nun hat sich die Situation geändert – die KVen haben die bisherige Vorgehensweise verboten und zwingen die niedergelas-

<sup>1</sup> [http://www.kbv.de/wir\\_ueber\\_uns/83.html](http://www.kbv.de/wir_ueber_uns/83.html)

<sup>2</sup> Pressemitteilung der KBV dazu: <http://www.kbv.de/presse/36724.html>

senen Ärzte und Psychotherapeuten ab dem Jahr 2011 zur Online-Abrechnung<sup>2</sup>. Der Sinn des Zwangs erschloss sich mir erst nicht. Dem minimal höheren Aufwand des manuellen Einlesens eines Datenträgers pro Arzt bzw. Therapeuten und Quartal bei den KVen steht ein erhöhtes Sicherheitsrisiko durch IT-unkundige Praxismitarbeiter gegenüber, die ihre Computer mit dem Internet verbinden müssen. Mir schien eher ein sukzessiver und zwangfreier Umstieg von persönlicher oder postalischer zur online-Übertragung sinnvoll, falls dieser von den Betroffenen überhaupt gewünscht ist.

Auch ging ich davon aus, dass ein *einfaches* und *sicheres* Verfahren gewählt würde. Eine Grundregel beim Entwerfen eines jeden technischen Systems ist, es so einfach wie möglich (und nötig) zu halten, da jedes zusätzliche Element Risiken birgt. Es würde sich anbieten, die Abrechnungs-Datei auf dem Arzt-Computer mit dem öffentlichen PGP-Schlüssel der KV zu verschlüsseln (z.B. mit GnuPG<sup>3</sup>), und sie dann über eine beliebige Dateiübertragungstechnik (z.B. Secure CoPy) auf den KV-Server zu transportieren. Dafür sind alle Programme vorhanden und ausgiebig erprobt; die Einbindung in jede bestehende Arzt-Abrechnungs-Software wäre trivial. Der größte Vorteil läge in der *Überprüfbarkeit* der Sicherheit der technischen Vorgänge durch die Öffentlichkeit (bzw. durch unterschiedliche Experten, die für keine oder zumindest unterschiedliche Lobbys arbeiten), denn der Quellcode der genannten – im Sicherheitsbereich wichtigen und populären – Programme liegt offen vor.

Es kam aber ganz anders. Die KVen entschieden sich, mit Kanonen auf kleine, niedliche Vögel zu schießen. Sie bildeten ein Computernetzwerk namens „KV-SafeNet“, wobei die Rechner der Bundesländer-KVen und der KBV-Zentrale über dicke Datenleitungen (Backbones) verbunden sind. Den Anschluss dieser Server an das (bzw. die Schnittstelle zum) Internet organisieren momentan 25 privatwirtschaftliche Firmen<sup>4</sup>. Von der Praxis aus wird durch einen *Tunnel* über einen DSL-Anschluss und das Internet ein Virtuelles Privates Netzwerk zu ei-

nem Server dieser Firmen aufgebaut. Aus der Sicht der auf einem Praxis-Rechner laufenden Software wirkt das so, als sei der Computer in einem lokalen Netzwerk mit den anderen Praxen, den KV-Servern und den Servern der eben genannten Firmen.

Das Konzept ist nicht schlecht – wenn man von einer Zentrale aus eine permanente Verbindung zu allen Praxiscomputern haben möchte. Für die KV-Abrechnung und so gut wie alle anderen Datenverarbeitungs-Bedürfnisse der Ärzte, Psychotherapeuten und Patienten ist es völlig unnötig.

Es geht noch weiter: Die KVen haben angeordnet, dass der Aufbau des Tunnels nicht durch einen Praxiscomputer selbst geschieht (was problemlos möglich wäre), sondern durch einen speziellen Router. Dieser Router muss von den Praxisbetreibern bei einer der 25 „Provider“-Firmen gekauft werden. Von den KVen wird er offiziell treffenderweise „Black Box“ genannt, denn *in seine Funktionsweise darf von den Ärzten und Psychotherapeuten bzw. ihren IT-Betreuern keine Einsicht genommen werden*. Als Router ist er meistens das Zentrum auch des internen Netzwerk-Datenverkehrs in der Praxis. Er darf aber vom Praxisbetreiber weder konfiguriert werden, noch kann dieser nachvollziehen zu welchen Servern im Internet der Router Verbindungen aufnimmt und welche Daten er überträgt. Eine Überwachung und Protokollierung der gesamten lokalen Netzwerkdaten durch die entsprechende KV-SafeNet-Provider-Firma ist problemlos möglich, da diese den Router ohne das Wissen des Arztes bzw. Therapeuten fernsteuern und einrichten kann. Kein zurechnungsfähiger IT-Administrator würde eine *Black Box* mit einer verschlüsselten Schnittstelle nach außen in das Zentrum seines Netzwerkes einbauen und danach noch einen Pfifferling auf die Sicherheit des Systems wetten – denke ich. Die KVen scheinen das anders zu sehen; sie haben ja auch keine Hemmungen, die Praxen zu einer Installation eines solchen Box zu zwingen.

Man muss also als Arzt, Psychotherapeut (und als deren Patient) seiner SafeNet-

<sup>3</sup> <http://www.gnupg.org/>

<sup>4</sup> Eine Liste ist unter <http://www.kbv.de/13815.html> einsehbar.

Anbieter-Firma (zu denen auch die *Telekom* gehört) vollkommen vertrauen. Ebenso muss man darauf vertrauen, dass, sollte die „Black Box“ immerhin ordnungsgemäß funktionieren, allen anderen am Gesamtnetzwerk beteiligten keine sicherheitstechnischen Schnitzer passieren. Dies sind immerhin 25 Provider-Firmen, 17 KVen, die KBV und mehrere zehntausend Praxen. Allein die Größe des Netzwerkes und seine vielen Schnittstellen zum Internet machen klar, dass eine Abschottung gegen ernsthafte Angreifer von außen eher Minuten als Tage hält. Man muss davon ausgehen, dass Datendiebe oder -manipulateure sich sehr schnell zumindest einen Praxis-Account bei einem der Provider besorgen können und damit Teil des Netzes werden.

Der Begriff „Black Box“ ist auch nur aus Sicht der Praxis und Patienten treffend – für die verkaufende „Provider“-Firma handelt es sich um eine *White Box*, denn ihre interne Funktionsweise ist dort vollständig bekannt. Zumindest muss man hoffen, dass dies zutrifft und keiner der Firmen relevante Fehler oder unerwünschte sicherheitskritische Funktionen in ihrer Box übersieht. Wie gut die Firmen in diesem zentralen Punkt ihre Arbeit machen ist aber prinzipiell nicht überprüfbar, denn für ihre Kunden ist die *Box* ja *black*.

Die Übertragung der Patientendaten im „SafeNet“ wird allerdings noch einmal verschlüsselt – per PaDok bzw. D2D, der gleichen Technik, die auch auf der „Elektronischen Gesundheitskarte“ zum Einsatz kommen soll (der CCC hat sich in der Datenschleuder #85 damit beschäftigt<sup>5</sup>). Diese Technik hat mit dem „Black Box“-Router im Praxis-Netzwerk eines gemeinsam: Die Hersteller verraten nicht, wie sie funktioniert<sup>6</sup>. Das soll vermeintlich die Sicherheit des System erhöhen, da angreifende Kriminelle etwas Zeit zur Analyse brauchen. Diese Vorgehensweise nennt man „security by obscurity“. Sie ist kontraproduktiv, da eine Analyse wohlmeinender Sicherheitsexperten unterbunden wird, die Kriminellen auf Dau-

er aber selten am Verstehen des Systems gehindert werden. So ließen sich die gesamten geheimen Einstellungen der „Black Box“ meiner Praxis mit wenigen Stunden Arbeit auslesen, wenn man das Gerät in den Händen und die Motivation zu einer kriminellen Handlung hat. Die Black-Boxerei stellt also keineswegs einen ernstzunehmenden Schutz gegen Kriminelle und bösartige Datendiebe dar, sondern sie hindert einzig die Betreiber der Praxen an der Kontrolle über ihre eigene IT-Infrastruktur.

Claude Shannon, der Begründer der Informationstheorie, äußerte sich schon in den 40er Jahren zu diesem Thema: „The enemy knows the system“. Auguste Kerckhoffs schrieb 1883 in seinen Grundsätzen der modernen Kryptographie „The system must not require secrecy and can be stolen by the enemy without causing trouble“<sup>7</sup>. Mit „system“ bezog er sich auf den technischen Verschlüsselungsapparat. Damit meinte er, dass die Kenntnis vom Verschlüsselungs-Algorithmus, die ein Spion durch das Stehlen des Apparates erlangt, diesem beim Entschlüsseln der geheimen Nachrichten nicht helfen dürfe. Seit über einhundert Jahren ist es allen Kryptographen bekannt, dass man Sicherheit durch die hohe Qualität der Kodierverfahren und nicht durch die Geheimhaltung derselben herstellen sollte. Eine Verschleierung der Verfahren selbst spricht immer für ihre mindere Qualität – und hält nie lange.

Ein weiterer Nachteil des „SafeNets“ sind die hohen Kosten für die Praxen. Ein Black-Box-Router kostet zwischen 190 € und 500 €. Die Provider-Firmen verlangen von jeder Praxis eine monatliche Gebühr von mindestens 17 € (zusätzlich zum DSL-Anschluss). Jährliche Kosten von über 200 € sind unverhältnismäßig teuer bei einem Übertragungsvolumen von oft weniger als einem Megabyte (so zumindest in der von mir betreuten Praxis) pro Quartal. Hier könnte man darüber nachdenken, ob die Preisgestaltung nicht nach § 138 Abs. 2 BGB als sittenwidrig einzuschätzen ist.

Die Entwickler bzw. Entscheider hinter dem

<sup>5</sup> <http://chaosradio.ccc.de/media/ds/ds085.pdf>

<sup>6</sup> Im Falle des Routers stimmt das nicht ganz: Die Funktionsweise ist bekannt – IPsec-VPN – aber die Konfiguration und Zusatzfunktionen nicht.

<sup>7</sup> <http://www.petitcolas.net/fabien/kerckhoffs/>

SafeNet bauen also ein System, das nicht mal den Sicherheitskonzepten von 1883 entspricht (security by obscurity). Es ist für die KVen wie auch für die Ärzte sehr teuer, dabei für die Abrechnung unnötig. Allein die Größe und Menge der involvierten Parteien (u.A. 25 Privatfirmen) macht das Netz angreifbar. Die Abrechnungen wären über bestehende Techniken (PGP) einfacher, billiger und sicherer zu übertragen. Jeder Netzwerk-Administrator wird auf die Barrikaden gehen, wenn er eine ferngesteuerte Black Box in das Zentrum seines Netzes einsetzen soll, wie dies nun in den Praxen geschehen muss. Hier drängt sich nach Marcus Cicero die Frage auf: „Wem nützt es?“ Die erste Antwort darauf ist merkwürdig. Auf den ersten Blick scheint es nur den 25 Provider-Firmen zu nutzen, die daran kräftig verdienen. Diese sind aber nicht die Initiatoren. Alle anderen haben mit dem „SafeNet“ erstmal nur Ärger.

Doch vor Spekulationen über die Interessen hinter „SafeNet“ möchte ich über die Erfahrungen berichten, die ich als IT-Administrator meiner Praxis in den letzten Tagen gemacht habe.

Zur Zeit bekommen die Ärzte und Psychotherapeuten vieler Bundesländer von den KVen eine motivationsfördernde „Prämie“ von mehreren hundert Euro, wenn sie innerhalb von kurzer Zeit die ferngesteuerte „Black Box“ für ihr Praxis-Netzwerk anschaffen<sup>8</sup>. Wohlgermerkt müssen die Praxen dies sowieso tun, denn andere Arten der Abrechnungen werden nicht mehr akzeptiert. Wieso für eine verpflichtende Handlung noch eine „Prämie“? Es soll wohl der passive Widerstand vieler Ärzte und Psychotherapeuten gebrochen werden, die durch ein Verschleppen der Anschaffung die Einführung des neuen System verzögern oder behindern.

Die Bestechung funktionierte auch bei meiner Praxis. Ich schaute mich um nach dem billigsten Angebot und stieß auf die Deutsches Gesundheitsnetz Service GmbH<sup>9</sup>. Dort kostet der

Router „nur“ 190 €, die jährlichen Gebühren für die Berechtigung zur Verbindungsaufnahme zum VPN-Server belaufen sich auf 204 €.

Die mysteriöse „Black Box“ interessierte mich besonders. Sie entpuppte sich als „Fritz!Box Fon Wlan 7170“<sup>10</sup>, hergestellt von der AVM GmbH aus Berlin. Ein nachträglich angebrachter Aufkleber etikettierte sie um in einen „DGN Safenet-Konnektor“. Dieses Gerät (ohne den Konnektor-Aufkleber) bekommt man nicht nur bei Media Markt und ähnlichen Geschäften, sondern auch im Versandhandel ab 120 €<sup>11</sup>. Der mit 70 € bezahlte „Mehrwert“ des an meine Praxis gelieferten Routers gegenüber dem Versandhandel-Modell liegt in der Konfiguration: Durch die DGN GmbH wurde die Verbindung zu ihrem Virtuellen Privaten Netzwerk (und vielleicht noch andere Funktionalitäten) eingestellt, sowie ein dem Käufer unbekanntes Login-Passwort gesetzt. Ebenjenes geheime Passwort macht für die Praxis dann aus der Fritz!Box eine Black Box.

Eine Untersuchung des Routers im Netzwerk (genauer gesagt: ein Portscan) ergab dann, dass diverse Server auf dem Gerät laufen und auf Verbindung warten, d.h. verschiedene Ports offen waren<sup>12</sup>. Dies ist für die angedachte Funktionalität des VPN-Routers unnötig; es stellt mindestens ein erhöhtes Sicherheitsrisiko dar. Beispielsweise der laufende Dienst für Telefonie (SIP) ist überflüssig, da das Gerät weder für diesen Zweck angeschafft wurde, noch es mangels Passwort dafür konfigurierbar wäre.

Unter Anderem lief auch ein Webserver. Die dort angezeigte Seite ist die übliche Fritz!Box-Login-Page. Unter dem Passwort-Feld steht die freundliche Aufforderung „Wenn Sie Ihr Kennwort vergessen haben, klicken Sie [hier](#)“. Da konnte ich mich nicht zurückhalten und habe es getan. Das Ergebnis war wie erwartet, dass die Fritz!Box ihre Konfiguration löschte und sich

<sup>8</sup> Z.B. in Bremen gibt es 600 €: <http://www.aerzteblatt.de/v4/archiv/artikel.asp?id=67269>

<sup>9</sup> <http://www.dgn.de/>

<sup>10</sup> Technische Details zum dem Gerät sind unter [http://www.wehavemorefun.de/fritzbox/index.php/FRITZ!Box\\_Fon\\_WLAN\\_7170](http://www.wehavemorefun.de/fritzbox/index.php/FRITZ!Box_Fon_WLAN_7170) zu finden.

<sup>11</sup> Einen Überblick bezüglich der Endkundenpreise kann man sich unter <http://www.heise.de/preisvergleich/a178963.html> verschaffen.

<sup>12</sup> Der benannte „SafeNet-Router“ der Firma DGN hat folgende offene tcp-Ports: 80, 2049, 5060, 8080, 49000 und 49443

damit in den Zustand versetzte, den sie auch hat, wenn man sie frisch aus dem Media Markt trägt.

Auf die Anfrage an die DGN GmbH nach den Konfigurationsdaten wurde ebenfalls wie zu vermuten reagiert: Ich solle das Teil einschicken und eine Gebühr von 30 € entrichten, damit die Firma den Router neu konfiguriert.

Bei der ganzen Geschichte gibt es mehrere Hässlichkeiten. Die Firmen verlangen sehr viel Geld für sehr wenig Leistung – besonders die monatlichen 17 € für die üblicherweise nur einmal im Quartal genutzte Berechtigung zur Teilnahme am VPN sind unverschämt. Ein happiger Aufschlag von 70 € für die Vorkonfiguration eines Routers ist auch nicht wenig. Das ganze Konzept des fremdkontrollierten Routers im Praxis-LAN ist unsicher, aber wieso laufen auf dem Gerät auch noch unnötige Dienste? Wieso hat die DGN eine Fritz!Box mit WLAN- und Telefonie-Hardware verwendet, wenn solche Funktionalitäten gar nicht genutzt werden dürfen? Es stellt sich auch die Frage, ob ein solches Konsumenten-Endgerät den an eine ärztliche Praxis gestellten Sicherheitsanforderungen genügt. Offenbar hat die DGN mit den überflüssigen Serverdiensten in der Konfiguration geschlampt. Bei einem solchen groben Patzer, einem Fehler, durch den jeder Auszubildende in den entsprechenden Lehrberufen durch eine Prüfung fallen würde, drängt sich die Frage auf, wie denn die restliche Konfiguration aussieht. Leider ist das nicht auf legalem Weg überprüfbar, denn die Firma rückt – auf Weisung der KV, es muss ja eine Black Box sein – mit dem Passwort nicht heraus.

Von Seiten des „SafeNets“ bzw. der Provider-Firma aus ist der Router ebenso erreichbar wie aus den lokalen Netzwerk (dank VPN). Deswegen können sich die Angestellten der DGN in unsere Fritz!Box jederzeit einloggen, sie haben ja auch das Passwort. Beworben wird das auf deren Homepage mit „Kostenlose und komfortable Fernwartung durch unsere Hotline-Mitarbeiter“<sup>13</sup>. Das bedeutet schlicht, dass jede ärztliche und psychotherapeutische Praxis in Deutschland die Kontrolle

über ihren herausgehenden und *internen* Datenverkehr an eines der privatwirtschaftlichen „SafeNet“-Unternehmen „outsourcen“ muss.

Im Fall der DGN hat die Sache noch ein Sahnehäubchen: Die Fritz!Box hat eine Funktion zum Mitschneiden des gesamten Datenverkehrs schon eingebaut. Auf der Seite <http://router-adresse/html/capture.html> – wobei `router-adresse` durch die IP-Adresse der jeweiligen Praxis-Fritz!Box zu ersetzen ist – kann ein DGN-Angestellter bequem und ohne besondere Computerkenntnisse über den Webbrowser das Mitschneiden des gesamten internen Netzwerk-Datenverkehrs in der jeweiligen Praxis ein- und ausschalten und die Daten zu sich herunterladen<sup>14</sup>.

Aber warum sollte das denn jemand tun? Weiter gefasst führt das zu der weiter oben gestellten und noch nicht beantworteten Frage: Warum das alles? Wem nützt es? Hier kann nur spekuliert werden. Es ist jedoch offensichtlich, dass die vorgegebenen Argumente für das „SafeNet“ nicht mit den echten Interessen übereinstimmen. Wollte man wirklich ein gutes System für die online-Übertragung der Abrechnung über das Internet, so hätte man das einfacher, schneller, besser, sicherer und deutlich billiger haben können.

Die Praxen sollen offensichtlich mit aller Gewalt dazu gebracht werden, dass ihre Informationstechnik permanent verbunden ist mit dem Zentralserver der KVen bzw. der KBV, und dass sie durch diese besser überwachbar sind. Die zentrale Anbindung und Vernetzung der Praxen ist für sich allein nicht zweckmäßig; Sinn ergibt das Ganze erst, wenn noch weitere Schritte folgen. Man kann also vermuten, dass die KBV oder das Gesundheitsministerium Erweiterungen des Systems plant, für die die momentan aufgebaute Vernetzung Voraussetzung ist. Was könnte das sein? Es wäre möglich die Abrechnungsdaten, d.h. Daten über Patientenbesuche, Medikamente, Therapien, schon zum Zeitpunkt der Erzeugung zentral bei der KV zu speichern; keine Abrechnung pro Quartal ist dann mehr notwendig, sondern alles geht online und on-the-fly. Die Auslagerung der Informati-

<sup>13</sup> [http://www.dgn.de/50produkte\\_tarife/05kvsafenet/10easy/index.html](http://www.dgn.de/50produkte_tarife/05kvsafenet/10easy/index.html)

<sup>14</sup> [http://www.wehavemorefun.de/fritzbox/Versteckte\\_Features](http://www.wehavemorefun.de/fritzbox/Versteckte_Features)

---

onstechnik aus der Praxis in den KV-Server im „SafeNet“ lässt sich noch deutlich weiter treiben. Warum nicht alle Patientendaten in die Zentrale? Diagnosen, chronische Krankheiten, Arztnotizen... die Datenhaltung wird viel effizienter und die Praxen müssen sich kaum noch mehr um die Wartung von irgendwelchem Computerkrams kümmern. Alle Gesundheitsdaten

fast der gesamten Bevölkerung (mit Ausnahme der Privatversicherten) wären an einer Stelle und in einer Hand. Daten sind Macht und eine Datenbank ist mehr als die Summe ihrer Einzelteile. Besonders bei der Pharmaindustrie dürfte eine solche, technisch leicht auszuwertende, Datensammlung Begehrlichkeiten wecken.