Über die Gefahren und Risiken des Internets in der Praxis

Für Ärzte ist das Internet sowohl Fluch als auch Segen

Eine Schönheitsklinik bekommt plötzlich eine E-Mail von Erpressern. Die Forderung: 50.000 Euro oder sämtliche Patientenakten werden im Internet veröffentlicht. Ohne große Mühe hatten sich die kriminellen Hacker Zugriff zu den hochsensiblen Patientendaten verschafft, denn das Netzwerk der Schönheitsklinik war nicht ausreichend geschützt. Der IT-Sicherheitsexperte Götz Schartner kennt solche Fälle zuhauf. Er berät seit Jahren kleinere und größere Unternehmen im In- und Ausland bezüglich der Datensicherheit. Nun hat er ein Buch über das Thema geschrieben, in dem er echte Fälle beschreibt und gleichzeitig Sicherheitstipps und Checklisten für kleinere Netzwerke zur Verfügung stellt. Wir haben mit Götz Schartner darüber gesprochen, worauf Arztpraxen besonders achten sollten.

Götz Schartner
IT-Sicherheitsexperte, Unternehmensberater für Datensicherheit und Buchautor

© contrastwerkstatt / Fotolia

Herr Schartner, der Internetzugang ist mittlerweile sowohl privat als auch beruflich unverzichtbar. Ärzte nutzen das Internet zur Kommunikation, Recherche und für Online-Abrechnungen. Welche Gefahren ergeben sich daraus insbesondere für diese Berufsgruppe und für die Patienten?

Leider sichern viele Arztpraxen ihre Computer oder Netzwerke nur unzureichend ab. Daher besteht grundsätzlich die Gefahr, dass Hacker Zugriff auf die Patientendaten erlangen können. Häufig wird für den Internetzugang lediglich ein DSL-Router verwendet und zum Schutz der Computer eine Antivirensoftware. Das ist zu wenig und aus Sicht der Datensicherheit grob fahrlässig. Hacker können solche Sicherheitsmaßnahmen meistens spielend umgehen und erhalten damit über das Internet Zugriff auf hochsensible Gesundheitsdaten.

Wie groß ist das Problem? Wie häufig werden Arztpraxen angegriffen?

Kleinere Praxen werden in der Regel nicht gezielt angegriffen, sondern fallen eher sogenannten ungezielten Massenangriffen zum Opfer. Bei größeren Praxen oder Kliniken sieht das anders aus. Hier kommen gezielte Angriffe durchaus vor. Sobald kriminelle Hacker dann in ein Praxisnetzwerk eingedrungen sind, stehlen sie Daten und schauen dann, was man mit diesen machen kann. Ob sie die Daten verkaufen, sie zur Erpressung nutzen oder verwenden können, um beispielsweise das Online-Banking der Praxis zu manipulieren und so Geld zu stehlen. Das passiert permanent, jede Praxis kann davon jederzeit betroffen sein.

Worauf muss man achten, wenn man ein Netzwerk für eine Praxis einrichtet?

Ärzte müssen technisch ausreichende Maßnahmen ergreifen, um Patientendaten vor unberechtigten Zugriffen zu schützen. Das verlangt auch das Bundesdatenschutzgesetz. Konkret heißt das: Die Technik muss auf dem neuesten Stand sein. Am besten sind zwei Netzwerke. Ein Netzwerk, in welchem die sensiblen Daten gespeichert werden – ohne Internetverbindung. Und ein weiteres Netzwerk, mit Internetzugang, über das man beispielsweise Online-Abrechnungen tätigen kann. Das ist die einfachste und sicherste Lösung. Ist das Arztnetzwerk mit dem Internet verbunden, dann sollte auf jeden Fall eine Hardware-Firewall verwendet werden, keinesfalls nur ein DSL-Router. Ebenfalls sollte eine professionelle Antivirensoftware im Einsatz sein – die kostenfreien gehören definitiv nicht dazu. Auch sollten unbedingt aktuelle Betriebssysteme verwendet werden, beispielsweise Windows 7 oder 8. Regelmäßige Updates für das Betriebssystem aber auch für die Anwendungen, beispielsweise für den Acrobat Reader und die Office-Anwendungen sind obligatorisch. Und ich rate dringend davon ab, Java zu installieren, da Java immer wieder Sicherheitslücken auf-

weist, die Hacker ausnutzen können, um in fremde Netzwerke einzudringen.

Wie ist es mit WLAN in der Praxis?

Ein WLAN sollte für eine Arztpraxis tabu sein. Die einzige Möglichkeit wäre ein separates Netzwerk einzurichten, in welchem keine Patientendaten gespeichert werden.

Solche Sicherheitsstandards stellen eine hohe Anforderung für kleinere Praxen dar.

Das ist richtig, aber das ist auch absolut notwendig! Bedenken Sie: Auch kleinere Arztpraxen sind häufig Opfer von Hackerangriffen. Wie vorhin bereits erwähnt, müssen diese gar nicht gezielt durchgeführt werden. Sie geschehen meist in der Masse und sehr oft merkt man ganz lange nichts vom Schaden. Das ist wirklich ein ganz großes Problem.

Was können Arztpraxen sonst noch tun, um den Internetanschluss und die Datenübertragung z. B. an andere Ärzte oder Krankenkassen abzusichern?

In dem Fall möchte ich einfach mal ganz frech auf mein Buch „Tatort www“ verweisen. (lacht) In dem Buch finden sich gerade für kleine Praxen gute Tipps. Außerdem halte ich regelmäßig Vorträge vor Ärzten zu genau diesem Thema. Die Größe des Netzwerks einer solchen Praxis ist in etwa mit der Größe eines größeren Familienhaushalts zu vergleichen. In dem Buch finden sich komplette Schritt-für-Schritt-Anleitungen zum Absichern des privaten Netzwerks oder eines kleinen Praxis-Netzwerks. Außerdem finden sich im Buch Checklisten, anhand derer jeder überprüfen kann, ob alle notwendigen Schritte unternommen

Buchverlosung als „Buch des Monats“ 10.2013, siehe Seite 6

worden sind. Im Grunde kann jeder Arzt, jede Ärztin alles selbst machen, ohne die Hilfe eines ITDienstleisters. Man muss sich nur damit befassen.

Wie häufig sollten Software-Updates durchgeführt werden?

Updates müssen permanent durchgeführt werden. Einmal pro Monat ist definitiv zu wenig, ja regelrecht gefährlich, denn damit lade ich Hacker praktisch ein. Heute existieren spezielle Programme, die zur Hilfe verwendet werden können, wie zum Beispiel die Software Secunia. Diese prüft, ob alle Updates für das Betriebssystem und für Programme installiert worden sind. Privat kann diese Software übrigens kostenfrei verwendet werden.

Woran merkt man, dass man Opfer eines Hackers wurde?

Das merkt man zunächst kaum. Erst recht, wenn es ein professioneller Angriff war. Man merkt es erst, wenn der Schaden eintritt, also wenn die Staatsanwaltschaft oder der Landesdatenschutzbeauftragte vor der Tür steht oder man erpresst wird. Es gibt aber klassische Indizien. Der Rechner wird beispielsweise ungewöhnlich langsam, es werden immer wieder Internetverbindungen aufgebaut, der Web-Browser oder der Acrobat Reader stürzen oft ab. Es sind zwar lediglich Indizien, aber man sollte bei so was lieber auf der Hut sein.

Gut getarnte Trojaner werden in der Regel nicht durch installierte Antivirenprogramme gefunden. Hier würden aber spezielle Antiviren-Boot-CDs Abhilfe schaffen können. Wie das funktioniert, habe ich in meinem Buch beschrieben.

Angenommen der Fall ist eingetreten: Das Netzwerk der Arztpraxis wurde gehackt. Welche Schritte sollte man unternehmen?

Hier gilt: Sofort Fachhilfe holen, entweder die Polizei einschalten oder ein darauf spezialisiertes Unternehmen* kontaktieren.

Worauf sollte man als Arzt bei der Kommunikation mit Patienten achten?

Wenn ich als Arzt etwas per E-Mail verschicke, dann muss es verschlüsselt sein. Das ist gesetzlich vorgeschrieben. Der Arzt darf zudem nur Inhalte kommunizieren, denen der Patient zugestimmt hat – auch gegenüber der Krankenkasse. Die Krankenkassen untereinander oder die Ärzte untereinander können ebenfalls nicht frei Daten über einen Patienten austauschen, ohne dass dieser vorher zugestimmt hat. Als Arzt sollte man sich daher absichern und die Einwilligung des Patienten schriftlich einholen. Man sollte außerdem sicher gehen, dass man tatsächlich an die private Mail-Adresse des Patienten schreibt – und nicht an eine Familien- oder Arbeitsadresse. Dadurch vermeidet man, dass eine falsche Person an die privaten Daten des Patienten gerät.

Der Arzt muss also Vieles beachten, wenn er einen Internetzugang in der Praxis haben will. Es klingt fast so, als wäre das Internet für die Praxis eher Fluch als Segen.

Das Internet birgt zwar viele Gefahren, aber diese können auf ein vertretbares Niveau reduziert werden. Um den Nutzern das nötige Werkzeug dafür an die Hand zu geben, habe ich auch mein Buch „Tatort www“ geschrieben.

© Creativa / Fotolia

* 8com GmbH & Co. KG (http://www.8com.de), GF Götz Schartner

1. Internationaler Cybermobbing-Kongress in Berlin

Soziale Medien als Schlachtfeld – ein globales Problem

Anfang September fand der 1. Internationale Cybermobbing-Kongress in Berlin statt, zum dem das Bündnis gegen Cybermobbing e. V. eingeladen hatte. Cybermobbing unter Kindern und Jugendlichen ist ein globales Problem, zu dem internationale Experten referierten und diskutierten.

© fotogestoeber / Fotolia

Der erste Vortrag wurde von Prof. Justin Patchin, Co-Direktor des Cyberbullying Research Centre an der Universität Wisconsin gehalten. Nach seinen Ausführungen werden nach einer Meta-Studie aus dem englischsprachigen Raum 21,3 Prozent der Jugendlichen im Laufe ihres Lebens irgendwann einmal zum Opfer und 15,2 Prozent zu Tätern von Cybermobbing.

Prof. Donna Gross von der Edith Cowan Universität in Australien sagte, dass Cybermobbing in Australien offiziell als Gesundheitsproblem betrachtet wird, weil hohe Korrelationen zu Ängsten, Depressionen, Suizidalität, Alkoholismus bestehen. Festgestellt wurde, dass 80 Prozent derjenigen, die in Cybermobbing-Aktivitäten verstrickt waren, auch herkömmliche Mobbinghandlungen ausübten.

Die gleichen Täter im Internet

Die neuen Medien erzeugen also in der Regel keine „neuen" Täter, sie erweitern nur die Möglichkeiten. Herkömmliches Mobbing ist also der beste Prädiktor für Cybermobbing. Als wirkungsvollstes Mittel der Prävention betrachtet sie ein gutes Klima an der Schule. Es zeigte sich, dass entsprechende Handlungen an Schulen, wo die Lehrer die Namen der Schüler kennen und diesen als Vorbild dienen, weniger häufig vorkommen. Erklärt wurde dies mit der Annahme, dass die Schüler sich vorstellen würden, ihre Lehrer fänden ein solches Verhalten nicht gut. Das Gefühl, „gesehen zu werden", führt demnach also zu einer deutlichen Verminderung destruktiver Handlungen. Auch stellte sie dar, dass ein früherer Zugang zu entsprechenden Medien nicht dazu führt, dass Kinder früher damit anfangen, sich gegenseitig anzugreifen. Die Hochphase liegt in dem Alter zwischen 13 und 14 Jahren. Beleidigende Nachrichten sollten als Beweis gespeichert und nicht darauf geantwortet werden, um eine Eskalation zu vermeiden. Auch rief Prof. Donna Gross dazu auf, die Zuschauer noch stärker in die Präventions- und Interventionsprogramme mit einzubeziehen. Es sollten Anregungen gegeben werden, was man als Zuschauer von Cybermobbing-Handlungen konkret tun kann, wie zum Beispiel klar darauf hinzuweisen, dass so etwas nicht in Ordnung ist.

Die Angst darüber zu sprechen

Prof. Dorit Olenik-Shemsh von der Universität Israel berichtete unter anderem davon, dass Kinder und Jugendliche dazu neigen, nicht mit ihren Eltern oder Lehrern darüber zu sprechen, wenn sie zum Opfer von Cybermobbing werden und begründete dies mit der Angst vor einem Verbot, die entsprechenden Medien weiter nutzen zu dürfen, sowie damit, dass diese „keine Ahnung" haben und durch ihr Eingreifen alles nur noch schlimmer machen könnten. Dies führe zu einer stärkeren Isolation als beim herkömmlichen Mobbing, obgleich auch sie feststellte, dass beide Formen oftmals miteinander einhergehen. Circa 90 Prozent der von Cybermobbing betroffenen Kinder und Jugendlichen sprachen mit niemandem über ihre Erlebnisse.

Mobbing Zahlen steigen

Einer israelischen Studie zufolge kannten im Jahr 2010 etwa 31,8 Prozent der Befragten jemanden, der oder die bereits betroffen war. Im Jahr 2013 waren es bereits 49 Prozent. Die Zahlen sind also deutlich angestiegen. Allerdings war dieser Anstieg beim herkömmlichen Mobbing noch deutlicher. Im Verlauf ihres Vortrages sprach Olenik-Shemsh auch über den Teufelskreis aus Einsamkeit und Viktimisierung, die sich gegenseitig verstärken. In einer von ihr erwähnten Untersuchung wurde festgestellt, dass der SWB-Wert (subjective well-being) auch bei den Tätern niedriger als bei Nicht-Tätern war, diese also auch oftmals erhebliche Probleme haben.

Kriminalhauptkommissar und Leiter der Prävention der Polizeidirektion Heidelberg Günther Bubenitschek und Dr. Melanie

Wegel (Universität Zürich) stellten dar, dass Cybermobbing (ebenso wenig wie das herkömmliche Mobbing) kein eigenständiger Straftatbestand ist. Beleidigung, Nötigung, Nachstellung, Verletzung der Privatsphäre aber sehr wohl geahndet werden können. Auch das „Recht am eigenen Bild" wurde in diesem Zusammenhang erwähnt. Das Grundproblem ist aber das Mobbing, die Medien sind nur die Werkzeuge. Sie wiesen darauf hin, wie wichtig es sei, Beweise zu sichern zum Beispiel als Screenshots.

Opfer und Täter haben Defizite

Sie machten deutlich, dass sowohl Täter wie auch Opfer oftmals Defizite im Erziehungsstil der Eltern aufweisen. Die Opfer wachsen gehäuft überbehütet auf, während die Täter vielfach sehr autoritär erzogen werden oder durch die Eltern „verwahrlosen". Brisant ist auch der Befund einer Untersuchung, der aufzeigt, dass die technische Ausstattung der Kinder umso besser ist, je schlechter die Eltern sozial gestellt sind.

88 Prozent aller Kinder haben bereits ab dem 6. Lebensjahr ein Handy und 83 Prozent von ihnen nutzen das Internet. Als Gründe für das aktive (Cyber-)Mobben wurden von den Kindern genannt, dass sie sich „nur gewehrt" (21,4 %) beziehungsweise die Täter es verdient hätten.

Zum Abschluss der Veranstaltung diskutierten verschiedene Experten die Frage, welche Präventivmaßnahmen nötig sind. Mehrfach wurde darauf hingewiesen, wie wichtig es ist, sowohl die Eltern als auch die Kinder und Jugendlichen stärker mit einzubinden und klar zu benennen, welche Verhaltensweisen nicht in Ordnung sind. Als die wichtigsten Maßnahmen wurden schließlich eine kreative und flächendeckende Präventionsarbeit bereits mit Beginn der Grundschule inklusive einer entsprechenden Ausbildung der Lehrkräfte sowie die Förderung von Schulprojekten (mit Einbindung der Unternehmen wie Facebook & Co.) genannt. Das Fazit der Veranstaltung lautet also „Aufklärung und Einbindung".

Weitere Informationen und die Ergebnisse der Studie „Cyberlive" mit den Cybermobbing-Ergebnissen für Deutschland unter:

www.buendnis-gegen-cybermobbing.de

Rainer Müller

Quelle: Bündnis gegen Cybermobbing e. V.

Eine App in Verbindung mit Facebook

Informationen direkt aufs Smartpohne des Patienten

Bereits im Jahr 2011 nutzte laut einer Umfrage des Ärztenachrichtendienstes (ÄND) mehr als jeder zweite niedergelassene Arzt soziale Netzwerke wie Facebook. Nun können sie zusätzlich von einer App profitieren.

Ärzte können über eine Facebook-Seite ihre Praxis vorstellen und allgemeine Informationen wie Sprechzeiten, Anfahrtsbeschreibung und Bilder einstellen. Zudem bietet Facebook Möglichkeiten, aktuelle Praxisinformationen zu posten. Aber auch Hinweise auf eigene Veranstaltungen, Fortbildungen und Notdienste. Damit Inhalte tatsächlich bei allen Patienten ankommen, gibt es eine weiterführende App als Marketinginstrument. In der kostenlosen Software „chayns" werden ganz automatisch alle Inhalte, die eine Arztpraxis auf Facebook postet in Echtzeit direkt auf dem Smartphone-Display als Push-Benachrichtigung des Patienten sichtbar.

© Christos Georghiou / Fotolia

Ärzte, die ihren Patienten weitere interessante Zusatzfunktionen – etwa eine Terminvergabe via App – bieten möchten, können solche Erweiterungsmodule in einem eigens dafür angelegten Appstore erwerben. Ärzte können ihre Patienten so über freie Termine informieren und Patienten können mit wenigen Klicks Termine vereinbaren. Das entlastet das Praxisteam organisatorisch und Patienten profitieren von flexiblerer Terminvergabe.

Die App ist verfügbar unter:
http://www.tobit.com/chayns

Quelle: Fink & Fuchs Public Relations AG

Neuer Masterstudiengang an der Uni Chemnitz

Spezialisten rund um das Thema Älterwerden

Mit Beginn des Wintersemesters 2013/2014 bietet das Institut für Weiterbildung GmbH an der TU Chemnitz den berufsbegleitenden Masterstudiengang Klinische Gerontopsychologie an, der die damit verbundenen neuen Herausforderungen an das Gesundheitswesen systematisch aufgreift und daraus ein Ausbildungskonzept aufgebaut hat. „Bislang fehlt es an spezialisierten Psychologen in diesem Bereich. Dies liegt unter anderem daran, dass bisher kein Studiengang existiert, der die speziellen klinisch-psychologischen Herausforderungen des Älterwerdens in diesem breiten Umfang abdeckt", sagt der Studiengangsleiter Prof. Stephan Mühlig.

In dem Fernstudiengang Klinische Gerontopsychologie werden Grundlagen sowie spezielle klinische Kompetenzen für die psychologische Betreuung und Behandlung älterer Menschen mit ihren spezifischen physischen, psychischen und sozialen Bedingungen vermittelt. Die Studenten sollen ein grundlegendes Verständnis für deren besondere körperliche, emotionale und soziale Probleme, ihre gesundheitlichen und funktionalen Einschränkungen, ihre altersspezifischen Bedürfnisse und Wünsche, aber auch ihre Kapazitäten und Ressourcen gewinnen.

Der Fernstudiengang ist innerhalb von sechs Semestern berufsbegleitend zu absolvieren. Er richtet sich an Interessenten mit einem Hochschulabschluss in Psychologie und verwandten Fächern, wie Pädagogik, Sozialpädagogik, Pflegewissenschaften, Gesundheitswissenschaften/Public Health sowie an Berufstätige im Gesundheitssektor (zum Beispiel Berater, Sozialarbeiter, Alten- oder Krankenpfleger). Über die Zulassung entscheidet im Einzelfall der Prüfungsausschuss. Eine mangelnde Einschlägigkeit des ersten Hochschulabschlusses kann durch eine mehrjährige Tätigkeit im Bereich Gerontologie kompensiert werden. Weitere Infos unter: www.tuced.de

Quelle: Technische Universität Chemnitz