KN PRAXISMANAGEMENT

Cyberkriminalität: Wer die Risiken kennt und damit umgehen kann, muss nichts fürchten

Ein Beitrag von Dr. Michael Visse, Kieferorthopäde aus Lingen.

Die Welt, in der wir heute leben, ist vernetzt. Internet und digitale Revolution haben in den zurückliegenden Jahren sehr viel verändert und ein Ende ist noch lange nicht abzusehen. Die rasante Entwicklung wird durch das mobile Internet noch katalysiert. Die Chancen, die sich hier für Praxen bieten, sind immens. Dass sich Patienten durch das Internet informieren und es auch zur Kommunikation verwenden, ist längst an der Tagesordnung. Diese Tatsache nutzen einige Praxen bereits und sind damit sehr erfolgreich.
Wie in den meisten Praxen, die das iie-System einsetzen, erfolgt auch in unserer Lingener Praxis das komplette Terminmanagement mit Terminbestätigung und Patienteninformation über Webbasierte Anwendung. Über die Schnittstelle ivoris connect ist alles mit der Praxis-Managementsoftware verbunden, was die Nutzung einfach und komfortabel macht. Viele Praxen stehen hier allerdings noch ganz am Anfang und haben wenig oder gar keine Erfahrungen mit dieser innovativen Möglichkeit der Patientenkommunikation gemacht. Dies wird sich mit Sicherheit kurz- oder mittelfristig ändern. Die Vorteile, die sich durch Web-basierte Dienstleitungen bieten, sind einfach zu groß, um sie zu ignorieren.

Karikaturen: © Burkhard Mohr

Durchdachtes Datenmanagement spart Geld und Nerven

Bei allen Vorteilen dürfen allerdings auch die Risiken nicht unterschätzt werden. Wir alle müssen uns darüber bewusst sein, dass wir keine IT-Expertise haben und uns als eher unerfahrene Nutzer mit Cyberkriminalität nicht auskennen. Das Internet abzu-

Fortsetzung auf Seite 17 KN

KN Fortsetzung von Seite 17

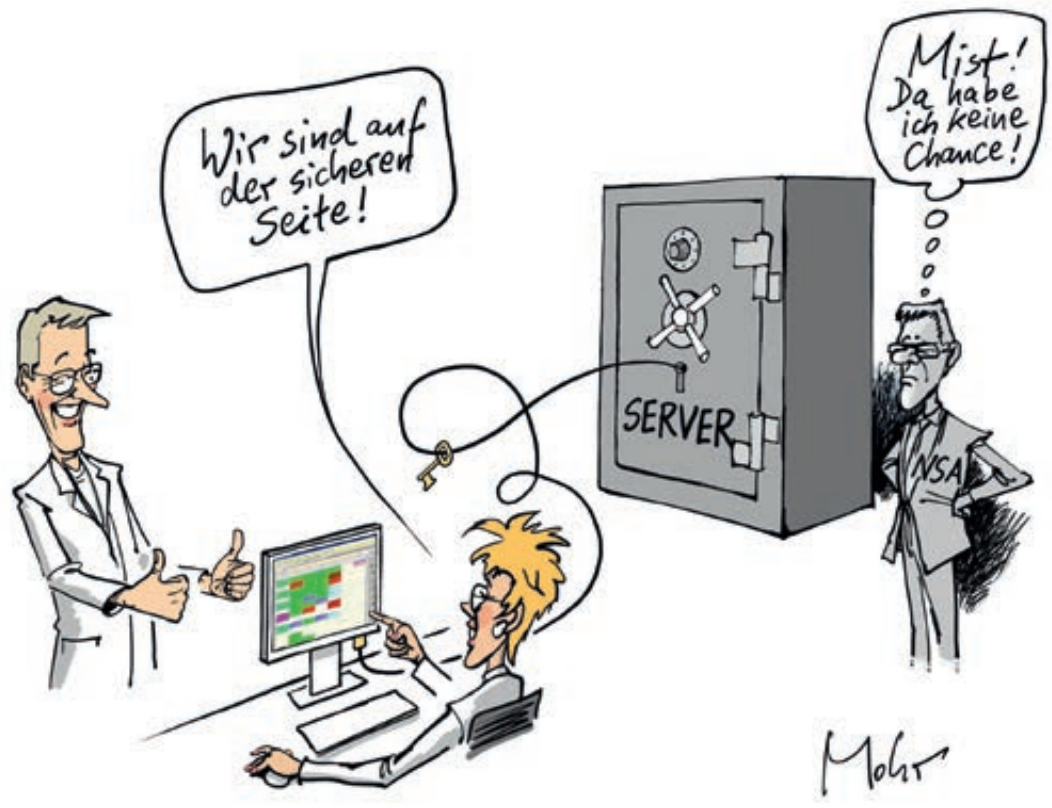
schalten und den Kopf in den Sand zu stecken ist jedoch kaum die richtige Lösung. Wer so handelt, hat von vornherein verloren, da er sich dem technologischen Fortschritt komplett verweigert. Wichtig ist, die Risiken zu kennen und damit umgehen zu können. Dazu braucht es Expertenrat und ein durchdachtes Datenmanagement. Die Einstellung, dass bislang nichts passiert ist und es schon weiterhin gutgehen wird, ist extrem gefährlich. Denn ist erst einmal ein Schaden entstanden, legt dieser den gesamten Praxisbetrieb lahm. Das ist nicht nur ärgerlich, sondern kann auch sehr teuer werden. Ein erfolgreicher Angriff auf Ihre Daten zieht zwangsläufig die Bereinigung des infizierten Systems sowie ggf. auch Neuanschaffungen nach sich. Den entstandenen Schaden zu beheben kostet also Geld, vor allem aber auch reichlich Energie und Nerven.

Häufige Formen von Cyberkriminalität

Vor allem drei Erscheinungsformen von Cyberkriminalität sind weit verbreitet:

- Identitätsdiebstahl/Phishing: Hierbei werden getarnte vertrauenserweckende E-Mails verschickt, bei denen der Empfänger aufgefordert wird, persönliche Informationen preiszugeben.
- Ransomware: Dabei werden kryptografische Verfahren verwendet, um Dateien und Dokumente auf infizierten Computern zu verschlüsseln. Für die Wiederherstellung des Zugriffs wird die Zahlung eines Lösegeldes (engl. ransom) gefordert.
- Botnetze: Davon spricht man, wenn viele – meist mehrere tausend – Rechnersysteme mit einem Schadcode infiziert und zusammengeschlossen wurden, um dann von Kriminellen zur Durchführung bestimmte Aktionen genutzt zu werden.

Tatsachenberichte von betroffenen Kollegen geben einen Eindruck, welche Schäden entstehen



können und mit welchem Aufwand die Behebung verbunden ist. Zunächst meine persönlichen Erfahrungen: Ich wurde Opfer einer Abofalle, einer verbreiteten Masche mit Klingeltönen. Wann und wie ich mir diesen Virus eingefangen habe, kann ich nicht mehr genau nachvollziehen. Identifiziert wurde das Ganze durch meinen Steuerberater, der feststellte, dass von meinem Konto monatlich zwischen 15 und 25 Euro für einen mir unbekannten Service abgebucht wurden. Nach meinem Verständnis wurde ich Opfer von Kriminellen, was der Abobetreiber natürlich ganz anders sah. Völlig unverständlich war für mich, dass mein Mobilfunkanbieter die Zahlungen für den dubiosen Drittanbieter eingezogen hat. Aus dieser höchst ärgerlichen Erfahrung habe ich gelernt und weiß heute, dass man sich davor ganz einfach schützen kann, indem man bei seinem Mobilfunk-Provider die Drittanbietersperre aktiviert. Damit kann diese von Cyberkriminellen nicht mittels Schadsoftware genutzt werden.

Nachfolgend der Erfahrungsbericht eines Kollegen: „Patientendaten sind das wertvollste Gut einer Praxis. Dessen ist man sich in aller Regel jedoch gar nicht bewusst und realisiert es erst dann, wenn sie plötzlich nicht mehr vorhanden sind. Ich spreche hier aus eigener leidvoller Erfahrung, denn meine Praxis wurde vor einiger Zeit Opfer eines so genannten Kryptovirus. Angehängt war dieser an eine völlig authentische und professionell gestaltete Bewerbung einer zahnmedizinischen Fachangestellten. Da sehr viele Zahnärzte und Kieferorthopäden auf der Suche nach qualifiziertem Personal sind, wird eine solche Mail natürlich geöffnet. Danach nimmt das Unheil seinen Lauf. Kurze Zeit später wird der Virus aktiv und verschlüsselt in wenigen Minuten alle Daten auf dem Server. Der Virus greift das komplette Netzwerk inklusive der Sicherungen an. So war es auch bei mir. Von einem Moment zum nächsten hatten wir auf nichts mehr Zugriff und ein Weiterarbeiten wurde unmöglich. Auf dem Server befand sich ein Datenlink mit einem Text, mit dem ich aufgefordert wurde, eine hohe vierstellige Summe zu zahlen, um die Datenverschlüsselung rückgängig zu machen.“ (Einen ausführlichen Erfahrungsbericht finden Interessierte unter blog.iie-systems.de)

Ein weiterer Kollege, der hier ebenfalls namentlich nicht genannt werden möchte, wurde Opfer eines Botnetzes: „Wir haben vor einiger Zeit plötzlich bemerkt, dass unsere Server sehr viel langsamer wurden, haben dem aber zunächst gar keine Bedeutung beigemessen. Dann wurden wir von einem Patienten informiert, dass er von uns eine E-Mail mit einer Rechnung im Anhang erhalten habe. Da wurden wir natürlich sofort hellhörig, denn wir versenden grundsätzlich keine Rechnungen per E-Mail. Wir haben sofort unseren Servicetechniker angesprochen und ihn gebeten, sich umgehend mit der Problematik auseinanderzusetzen. Durch seine Analyse fand er heraus, dass von unserem Account zigtausende Mails versendet wurden, deren Anhang vermutlich auch eine Schadsoftware enthielt, die sich dann auf den Rechnern der Empfänger installiert, sofern diese den Anhang öffnen. Das ist nicht nur sehr unangenehm, sondern für eine Praxis auch ein enormer Reputationsverlust, von den Nerven, die wir hier gelassen haben, ganz zu schweigen.“

Wie kann man sich wirkungsvoll schützen?

Damit Ihnen solche Erfahrungen erspart bleiben, möchte ich Sie für die Thematik Cyberkriminalität sensibilisieren und Ihnen konkrete Ratschläge geben, wie Sie sich schützen können:

- Halten Sie Ihre Software immer auf dem aktuellen Stand (regelmäßige Updates).
- Verzichten Sie keinesfalls auf eine Firewall und einen professionellen Virenscanner.
- Gehen Sie mit E-Mail-Anhängen und Nachrichten in sozialen Netzwerken sorgsam und überlegt um.
- Führen Sie eine Datensicherung nach protokolliertem Standard durch.
- Schützen Sie Ihre Hardware gegen Diebstahl und unbefugten Zugriff.

In unserer Praxis in Lingen sichern wir alle Daten in einem qualifizierten Rechenzentrum in Deutschland. So haben wir die Gewissheit, dass die Daten jederzeit rückgespielt werden können. Das gibt uns das gute Gefühl, in diesem Bereich völlig auf Nummer Sicher zu gehen.

Wer die Risiken beherrscht, kann die Chancen nutzen

Ich selbst möchte keine bösen Überraschungen erleben und überlasse bei den Praxisdaten daher nichts dem Zufall. Mein Rat: Beschäftigen Sie sich intensiv mit dem Thema Datensicherung und der sicheren Nutzung des Internets. Denken Sie nicht erst darüber nach, wenn ein Schaden bereits entstanden ist. Sprechen Sie Ihren Spezialisten vor Ort an und lassen Sie sich beraten. Die Investition in Datensicherheit ist eine mehr als sinnvolle Investition, die sich unbedingt lohnt.

Das Internet aus der Praxis zu verbannen ist freilich auch ein Weg, mit dem sich das Risiko minimieren lässt. Mittel- und langfristig führt dieser Weg jedoch in eine Sackgasse, aus der umzukehren nahezu unmöglich ist. Wer die Risiken beherrscht, hat die Möglichkeit, alle Chancen zu nutzen. Und die sind im Hinblick auf neue Informations- und Kommunikationstechnologie immens. Wer hier den Anschluss verpasst, wird zu den Verlierern der digitalen Revolution gehören. Wollen Sie sich wirklich in dieser Gruppe wiederfinden? KN

KN Kurzvita

Dr. Michael Visse
[Autoreninfo]

KN Adresse

Dr. Michael Visse
Fachzahnarzt für KFO
Gründer von iie-systems GmbH & Co. KG
Georgstraße 24
49809 Lingen
Tel.: 0591 57315
info@iie-systems.de
www.iie-systems.com