# Wenn der Bildschirm Totenköpfe zeigt

## Hackerangriffe auf Praxis-Webseiten – und was Sie dagegen unternehmen müssen

Medical-Tribune-Recherche

**WIESBADEN – Die Praxiswebsite besser vor Hackerangriffen schützen? Ach was, denken Sie, wer interessiert sich denn schon für meine Seite. Doch das Risiko für Angriffe ist nicht zu unterschätzen. Beugen Sie vor!**

Irgendwann ist es soweit: Sie wollen auf Ihre Website gehen und sehen Texte oder Bilder, die Sie nie eingestellt haben, wie z.B. einen Totenkopf oder die Meldung „You are hacked". Oder Sie rufen Ihre Praxiswebsite auf und werden auf eine fremde – und dubios erscheinende – Site weitergeleitet. Auch möglich: Ein (verärgerter) Besucher, beschwert sich über eine Viruswarnung seines Browsers oder seiner Antivirensoftware, nachdem er die Praxiswebseite aufgerufen hat. Vielleicht ist der Virus tatsächlich auf Ihrem Rechner, vielleicht hat der Virus seines Rechners aber auch Ihre Website infiziert, weil Ihr Antivirenprogramm nicht auf dem neuesten Stand ist. Besonders kritisch wird es, wenn Ihr Webhoster Sie darüber informiert, dass er Ihre Website abgeschaltet hat, weil Sie massenhaft Spam-Mails verschicken oder Schadprogramme verbreiten.

### Auch „Normal-Sterbliche" sind nicht sicher vor Hackern!

Klingt nicht gut? Ist es auch nicht. Wahrscheinlich fragen Sie sich in solchen Fällen zunächst, wer es auf Sie abgesehen hat. War das ein verärgerter Patient, ein neidischer Kollege oder wollen ein paar Jugendliche ihre Fähigkeiten testen, sogenannte Skript Kiddies? In der Regel trifft nichts davon zu, erklärt Dr. Christine Trutt-Ibing, eine Medizinerin, die seit 2009 im Anschluss an ihre mehrjährige Praxiserfahrung Internetlösungen für Niedergelassene entwickelt. „Die meisten Hackerangriffe erfolgen heute automatisiert aus dem Internet. Dabei checken kleine Computerprogramme zig-tausende Websites auf mögliche Schwachstellen wie z.B. zu kurze oder zu einfache Passwörter ab," erklärt sie. Möglich sei auch, dass sich die Botprogramme Sicherheitslücken in einem der CMS-Systeme wie WordPress, Joomla™, Typo 3 und Drupal suchen, die sie dann zielgerichtet für Hackerangriffe nutzen. Dass es hier nicht um Sonderfälle geht, die nichts mit uns „Sterblichen" zu tun haben, zeigt zum Beispiel der Vorfall im November 2016, als über 900 000 Kunden der Deutschen Telekom keine Internetverbindung mehr hatten. Viele waren sogar vom der IP-basiertem Telefon- und TV-Nutzung abgeschnitten. Ursache war ein weltweiter Hackerangriff, der eine bestimmte Sicherheitslücke in den betroffenen Router genutzt hatte, um diese als Botnetz für koordinierte Angriffe auf andere Systeme zu verwenden.

Dr. Christine Trutt_Ibing im Interview: Nicht jeder Angriff stört direkt die Funktion der Website – Handlungsbedarf besteht trotzdem!

**Layar-App herunterladen, Bild scannen und Interview starten**

### Hacker suchen Schwachstellen in den Systemen

### Erste Handlung: Website vom Netz nehmen

Erfolgt ein Angriff auf Ihre Praxiswebsite, sitzen die Auftraggeber also wahrscheinlich im Ausland und haben es gar nicht speziell auf Sie abgesehen: Die gehackten Seiten werden für kriminelle Zwecke eingesetzt, z.B. als Verteiler für Schad-Programme wie Computerviren oder Trojanern oder auch als Spamverteiler, die unbemerkt Phishing-Mails in die digitale Welt hinausschicken, um z.B. Bankzugangsdaten abzufischen.

Andere Botnets, die sich aus diesen gehackten Seiten zusammensetzen, helfen kriminellen Gruppen, an sensible Nutzerdaten heranzukommen, die sie entweder direkt gewinnbringend einsetzen oder im Darknet zu Geld machen.

Um weiteren Schaden zu verhindern, rät Dr. Christine Trutt-Ibing, sollten Sie, wenn ein Angriff erfolgt ist, sofort Ihre Website aus dem Netz nehmen (lassen). Danach muss analysiert werden, wie der Angriff erfolgte und vor allem, wann die Website gehackt wurde. Das Wissen um das Datum brauchen Sie, denn die Website muss aus einer Sicherungskopie hochgeladen werden, die vor dem Hackerangriff erstellt wurde – denn manche Viren „schlafen" zunächst für eine bestimmte Zeit, bevor sie aktiv werden. Laden Sie eine zu junge Sicherung hoch, besteht die Gefahr, dass diese den Virus bereits in sich birgt.

Außerdem wichtig ist ein Update auf die neueste Programmversion – das gilt insbesondere auch für eingesetzten Erweiterungen! Unabdingbar ist zudem die Änderung aller Passwörter (Logins, FTP). Am besten wenden Sie sich dazu an die Agentur, die Ihre Website betreut, oder an einen entsprechend spezialisierten Dienstleister.

### Drei Regeln helfen, das Schlimmste zu verhindern

Hundertprozentig schützen vor einem Hackerangriff kann man sich leider nicht. Auch Firmen mit eigenen IT-Abteilungen sind davor nicht gefeit. Um jedoch im Fall der Fälle den Schaden so gering wie möglich zu halten, gibt es drei goldene Regeln, um die Sicherheit zu erhöhen, sagt Dr. Christine Trutt-Ibing:

- Verwenden Sie sichere Passwörter
- Halten Sie Ihr Programm immer auf dem aktuellen Stand
- Fertigen Sie regelmäßig Sicherungskopien an

*Anouschka Wasner*

### Zum Schutz Ihrer Patienten

Dass Ihre Praxishomepage zu einem Teil des weltweiten Schadverbreitersystems werden kann, ist ein Problem. Ihre Patientendaten sind davon in der Regel aber nicht direkt betroffen, zumal die Website meist nicht auf dem Praxisserver liegt. Aber Achtung: Werden über die Praxishomepage Terminanfragen, Rezeptbestellungen oder E-Mail-Verkehr mit Patienten abgewickelt, liefern Sie im Fall eines Falles mit der Homepage auch medizinische Daten an die Hacker aus! Eine gesetzliche Eindeutigkeit gibt es hierzu nicht. Sicher ist: Wer Daten seiner Patienten auf welchem Weg auch immer über das Internet schickt, sollte sich dieses Risikos und der damit verbundenen Verantwortung bewusst sein. Und: Weisen Sie Ihre Patienten darauf hin, dass normale Mails mitgelesen werden können wie eine Postkarte – womit sich eigentlich jede (unverschlüsselte) Kommunikation über das Netz verbietet.

# Homepage ohne Datenschutzerklärung? Hier droht Abmahnung!

## Für quasi alle Praxis-Websites relevant: Wer personenbezogene Daten erhebt, ist seinen Besuchern eine Erklärung schuldig

Fortbildung der KV Hessen

**FRANKFURT – „Eine Datenschutzerklärung benötigt heute fast jede moderne Praxiswebsite", sagt Dr. Christine Trutt-Ibing, eine Medizinerin, die sich auf Internetlösungen spezialisiert hat. „Das wissen nur leider die Wenigsten."**

Das Wissen darum, dass jede Homepage ein Impressum braucht, ist heute ein Selbstläufer. Wann dagegen eine Datenschutzerklärung auf der Praxishomepage notwenig ist, ist für die meisten wahrscheinlich noch nicht mal als Frage ein Thema.

### Welche Daten werden von Ihren Besuchern erhoben?

Ziel einer solchen Datenschutzerklärung ist es, den User darüber aufzuklären, welche personenbezogenen Daten auf der betreffenden Website erhoben werden, wie mit diesen umgegangen wird und ob und in welcher Form Daten an Dritte weitergegeben werden. Benötigt wird die Datenschutzerklärung also von jeder Seite, die Daten erhebt.

Dann sind Sie ja aus dem Schneider? Wahrscheinlich nicht. Personenbezogene Daten werden viel häufiger erhoben, als wir glauben, erklärt Dr. Christine Trutt-Ibing auf einer Fortbildung der KV Hessen zum Thema Social Media, und macht es konkret, wann die Erklärung auf jeden Fall auf der Seite zu finden sein muss:

- ... wenn Sie Formulare auf der Website verwenden – dazu gehört auch das klassische Kontaktformular oder Bestellformulare für Rezepte und Überweisungen.
- ... wenn Sie eine Karte von Google Maps oder OpenStreetMap auf der Website verwenden, auf denen Sie die Lage Ihrer Praxis ersichtlich machen.
- ... Wenn Sie Videos von YouTube oder anderen Videoplattformen auf ihrer Praxishomepage eingebunden haben.
- ... wenn Sie Cookies verwenden (das macht heute fast jede Seite – fragen Sie Ihren IT-Service dazu!).
- ... wenn Sie ein Programm zur Auswertung der Besuche auf Ihrer Seite im Einsatz haben, also zum Beispiel Google Analytics oder Piwik.
- ... wenn Sie Social Buttons auf Ihrer Website haben, also eine Direktverlinkung zu z.B. Facebook oder Google Plus.

Die Pflicht, eine Datenschutzerklärung auf der Webseite einzubinden, ergibt sich übrigens aus § 13 des Telemediengetzes (TMG). Danach muss der User zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die etwaige Weitergabe von Daten an Staaten außerhalb der EU informiert werden.

### Geben Sie Besucherdaten an Dritte weiter?

Da die Unterrichtung zu Beginn des Nutzungsvorgangs auf Webseiten etwas schwierig ist, ist die gleichzeitige Unterrichtung ausreichend. Deswegen muss die Information aber jederzeit abrufbar sein – es bietet sich also an, die Datenschutzerklärung wie das Impressum über einen eigenen Reiter anklickbar zu machen.

Und was muss eine Datenschutzerklärung enthalten? Grundsätzlich geht es dabei zum Beispiel um die Fragen:

- Welche Art personenbezogener Daten werden erhoben?
- Warum werden diese Daten erhoben und was geschieht damit?
- Werden die Daten an Dritte weitergegeben, und wenn ja, unter welchen Umständen?
- Wie wird mit eventuellen Beschwerden umgegangen?

Da jede Website letztlich individuell aufgebaut ist und unterschiedliche Angebote enthält, empfiehlt die Expertin Dr. Trutt-Ibing bei anspruchsvollen Seiten den Besuch beim Anwalt oder in einfachen Fällen auch die Hilfestellung eines der Datenschutz-Muster-Generators, die kostenlos im Internet angeboten werden, auch von Rechtsanwälten.

Übrigens: Seitenbetreiber ohne korrekte Datenschutzerklärung riskieren seit 2016 auch Abmahnungen.

*Anouschka Wasner*