Foto: tostphoto – stock.adobe.com

WLAN gegen mögliche Angriffe absichern

Erklärungen zur IT-Sicherheitsrichtlinie der KZBV – Teil 3

Vor dem Hintergrund der IT-Sicherheitsrichtlinie der KZBV hatten sich die bisherigen Artikel aus dieser Reihe mit der Datensicherung und der Netzwerksicherheit befasst. In zahlreichen Zahnarztpraxen werden allerdings auch Funknetzwerke, teilweise kombiniert mit traditioneller Verkabelung eingesetzt. Daher wird sich der heutige Artikel dem Thema WLAN widmen.

WLAN steht für Wireless Local Area Network, also für ein schnurloses lokales Netzwerk. Für den Einsatz eines WLAN in der Zahnarztpraxis oder in anderen Bereichen gibt es zwei grundlegende Ansätze. Einmal kann ein Router eine Verbindung zum Internet herstellen und ein sogenannter Access-Point stellt die Verbindung zum Router her. Häufiger wird aber zwischenzeitlich die zweite Variante eingesetzt, nämlich der WLAN-Router. Also ein Router, in den bereits der Access-Point integriert ist. Da die Einstellungen hinsichtlich des WLAN für beide Lösungen identisch sind, wird im Folgenden nur noch von WLAN-Routern gesprochen.

Foto: Hans Schenkel

Dr. Thomas H. Lenhard ist ein international anerkannter Experte für Informationstechnologie und Datenschutz. Er greift auf seinen umfangreichen Erfahrungsschatz aus drei Jahrzehnten Datenschutz und Datensicherheit zurück und ist u.a. als Datenschutzbeauftragter sowohl für die DGZMK als auch für die DGI umfassend tätig.

Im Zusammenhang mit der Sicherheit eines WLAN weist das Bundesamt für Sicherheit in der Informationstechnik (kurz: BSI) darauf hin, dass der Router unabhängig von der realisierten Variante in die Betrachtung zur Sicherheit eines WLAN einbezogen werden muss. Es wird vom BSI auch darauf verwiesen, dass in dem Zusammenhang immer wieder Versäumnisse den Weg bereiten für Angriffe Krimineller auf Router. Auf diese Versäumnisse und Gefahren wird daher noch später eingegangen.

Auf Aktualität achten. Grundsätzlich ist der stabilste und auch sicherste Weg ein Netzwerk aufzubauen, das Verlegen geeigneter Kabel und das Setzen entsprechender Anschlussdosen. Nicht jede Zahnärztin oder jeder Zahnarzt wird aber in der Lage sein, die gesamte IT-Verkabelung seiner Praxis neu zu planen, zu bauen oder entsprechend zu modernisieren. Teilweise finden sich daher, wie bereits in

einem früheren Artikel erwähnt, noch Verkabelungen, die zwar zum Zeitpunkt der Installation dem Stand der Technik entsprochen haben, inzwischen jedoch nicht mehr zeitgemäß sind. Jedenfalls gibt es mannigfache Gründe auf WLAN-Technologie zurückzugreifen.

Funkwellen enden nicht an Wänden oder Türen. Üblicherweise möchte man eine gute und stabile Verbindung auch bei Nutzung des WLAN sichergestellt wissen, was häufig auch mit dem Wunsch einer bestmöglichen „Ausleuchtung" der Praxis mittels Funkwellen einhergeht.

Die Möglichkeit des Empfangs von Netzsignalen außerhalb der Praxis eröffnet grundsätzlich allerdings auch destruktiven Zeitgenossen die Möglichkeit, das WLAN anzugreifen.

Absicherung gegen mögliche Angriffe. Daher ist es von elementarer Bedeutung, ein eingesetztes WLAN gegen mögliche Angriffe abzusichern. Der erste Schritt dazu ist der Einsatz eines professionellen Routers oder WLAN-Routers der mit einer Firewall ausgestattet ist. Da der Router die zentrale Schnittstelle zwischen Praxis und Internet darstellt, ist er ein bevorzugtes Ziel von Hackerangriffen. Soweit die Telefonie der Praxis ebenfalls über den Router abgewickelt wird, kann hier theoretisch nicht nur der gesamte Datenverkehr, einschließlich übermittelter Passwörter, sondern auch jedes geführte Telefonat „abgegriffen" oder aufgezeichnet werden.

Hinsichtlich der grundlegenden Funktionen eines Routers sollten daher die nachfolgenden Maßnahmen umgesetzt werden. Das Thema ist dabei so komplex, dass Sie, wenn Sie nicht zu den besonders IT-affinen Zeitgenossen zählen, günstigerweise den bei Ihnen eingesetzten IT-Service mit der Überprüfung des WLAN beauftragen. Auf der nächsten Seite dieses Artikels steht eine Checkliste für Sie bereit, mit der Sie selbst oder der von Ihnen beauftragte IT-Service eine Prüfung Ihres WLAN durchführen können.

In Bezug auf den Router selbst sollte Folgendes beachtet werden:

1. Der administrative Zugang zum Router über das Internet soll gesperrt werden. Allerdings wird in verschiedenen Quellen auch die Empfehlung ausgesprochen, dafür Sorge zu tragen, dass keinerlei Verbindungen zum Internet bestehen, solange an der Konfiguration eines Routers gearbeitet wird. Service-Tätigkeiten am Router sollten demnach grundsätzlich vor Ort durchgeführt werden. Auch wenn die Verbindung nur im internen Netz möglich ist, so wird häufig empfohlen, Router nur über verschlüsselte Verbindungen zu konfigurieren – also diese nur über das https-Protokoll anzusprechen.
2. Die vermutlich häufigsten Einbrüche in Router erfolgen über einen Administrator-Account, der für den Zugriff aus dem Internet freigeschaltet ist und dessen werksseitig vergebenes Passwort nicht geändert wurde. Dabei werden häufig Passwörter wie „admin" oder „1234" werksseitig vorgegeben.
   Auch wenn Maßnahme 1 beachtet wird, muss das werksseitige Passwort auf einem Router immer geändert werden. Dabei sollten die üblichen Vorgaben für Passworte berücksichtigt werden, dass nämlich sowohl Groß- und Kleinschreibung wie auch Sonderzeichen und Zahlen im Passwort präsent sind. Zusätzliche Sicherheit erhält man durch die Länge des Passworts. Da das Administratorpasswort des Routers sicherlich nicht jeden Tag gebraucht wird, ist es vertretbar, ein Passwort mit 16 Zeichen oder mehr zu verwenden.
3. Es muss sichergestellt sein, dass der Router regelmäßig aktualisiert wird. Einige Anbieter bieten bereits die Möglichkeit der automatischen Aktualisierung von Routern. Ansonsten müssen die Geräte regelmäßig darauf geprüft werden, ob sogenannte Firmware-Updates verfügbar sind.
4. Neuere Geräte bieten zum Teil einen Funktionsumfang, der in einer Praxis nicht unbedingt erforderlich ist. Alle Funktionalitäten, die nicht benötigt werden, sollten deaktiviert werden, damit die verwendeten Ports nicht zusätzliche Angriffsmöglichkeiten auf den Router bieten.

Veraltete Verschlüsselungsverfahren können schnell gehackt werden. Hinsichtlich der Funkverbindung zwischen Router/Access-Point und Endgerät ist das verwendete Kommunikationsprotokoll von wesentlicher Bedeutung für die Sicherheit. Viele WLAN-Router bieten noch veraltete Protokolle für die Kommunikation an. In einigen Quellen wird berichtet, dass WEP per se unsicher wäre und man zuweilen auch WPA überwinden könne. Diese Darstellungen sind stark untertrieben. Der „Hack" eines Systems, das mit WEP gesichert ist, dauert selbst mit umfassender Erläuterung vor Studenten nicht länger als zehn Minuten. Ohne Erläuterungen hat sich das Thema WEP für gewöhnlich in knapp zwei Minuten erledigt. WPA wird einem Angriff in aller Regel nicht länger als einen Arbeitstag standhalten können. Sollten Sie also noch eine dieser Verschlüsselungsverfahren im WLAN nutzen, so wäre jetzt der richtige Zeitpunkt einen Anruf beim IT-Betreuer zu tätigen und schnellstens für Abhilfe zu sorgen.

Umsteigen auf aktuelle Verschlüsselungsverfahren. Dem Stand der Technik dürften derzeit zwei neuere Protokolle entsprechen, nämlich WPA2 und WPA3. Die Verbreitung von WPA3 hält sich derzeit noch in Grenzen. Insbesondere sind bei Einsatz von WPA2 aber noch weitere Einstellungen zu berücksichtigen.

WPA2 sollte nur mit der Option „PSK" eingesetzt werden. Die Option steht für pre-shared key. Dabei muss der „key" von Hand in jedes Gerät eingegeben werden, das in das WLAN integriert werden soll. Auch hier sollte die Passwortkomplexität berücksichtigt werden und das Passwort sollte möglichst lang sein. Nicht umsonst bietet ein Router für diese Methode eine Passwortlänge von 64 Zeichen an. Davon sollte großzügig Gebrauch gemacht werden. Denken Sie daran: Die Passwortlänge bedeutet Sicherheit. Als Verschlüsselung sollte im Zusammenhang mit WPA2 AES gewählt werden. Darüber hinaus sollte die Funktion WPS deaktiviert werden.

Außerdem sollten Sie im WLAN-Router die Filterung nach MAC-Adressen aktivieren, damit nur zugelassene Rechner sich damit verbinden können. Bei der MAC-Adresse handelt es sich um eine Identifikationsnummer des Netzwerkadapters, die grundsätzlich weltweit einmalig sein sollte.

Schließlich sollte der WLAN-Router nach wenigen fehlerhaften Verbindungs-

versuchen einen Rechner für einen bestimmten Zeitraum sperren. Auf diese Weise wird ein Angriff so weit in die Länge gezogen, dass ein Einbruch von Hackern in das System innerhalb eines überschaubaren Zeitraums sehr unwahrscheinlich wird.

Angriffe erschweren. Wenn immer die gleichen Geräte mit Ihrem WLAN verbunden sind, können Sie IP-Adressen fest vergeben und DHCP deaktivieren.
Auch das kann Angriffe erschweren. Zwar wird häufig erwähnt, dass das Ausblenden der SID keinen Schutz vor Hackern bieten würde, jedoch erfordern einige gängige Hackertools die Angabe dieser SID, also des Netzwerknamens. Dieser kann zwar anderweitig ermittelt werden, jedoch spricht nichts dagegen, es Hackern so schwer wie möglich zu machen, ein Netzwerk anzugreifen.

Praxisnetz und Gäste-WLAN immer trennen. Eines sollten Sie übrigens in keinem Fall tun, nämlich Gäste oder Patienten über dasselbe WLAN, das für die Praxisverwaltung genutzt wird, einen Internetzugang zu ermöglichen. Praxisnetz und Gäste-WLAN sind stets zu trennen. In Zeiten von LTE und G5-Mobilfunk ist es in aller Regel ohnehin nicht mehr erforderlich, besondere WLAN-Zugänge zum Internet für Gäste oder Patienten vorzuhalten. Die meisten Nutzer mobiler Geräte können sich bereits direkt mit ausreichenden Übertragungskapazitäten zum Internet verbinden.

Schließlich sollten Sie, soweit es der Access-Point oder WLAN-Router Ihrer Praxis ermöglicht, die Zeiten eingrenzen, zu denen ein Gerät eine WLAN-Verbindung herstellen kann. Üblicherweise ist es nicht erforderlich, dass das WLAN z.B. nachts um 3 Uhr erreichbar ist.

Wie Sie den vorstehenden Ausführungen entnehmen konnten, ist es eine recht komplexe Aufgabe ein WLAN sicher einzurichten. Grundsätzlich sollte daher immer gelten, dass kein WLAN eingesetzt wird, wenn ein funktionierendes kabelbasiertes Netzwerk verfügbar ist. Selbst wenn ein Anschluss in einem Raum benötigt wird, der bislang nicht über Netzwerkkabel verfügt, bietet sich eine Verbindung über das Stromnetz an. Entsprechende Adapter sind vergleichsweise günstig zu bekommen und eignen sich derzeit schon für Übertragungsraten bis zu 1.200 Mbit/s.

Hilfe bei Fragen: Falls Sie Fragen zu Datenschutz oder Datensicherheit im Allgemeinen oder zu dem Artikel im Besonderen haben, können Sie sich gerne per Mail an den Autor wenden: dr.lenhard@it-planung.com Sie sollten lediglich als Betreff dann angeben: „Artikel in der ZZI“.

Ausblick: Im nächsten Artikel dieser Reihe wird das Thema deutlich weniger technisch sein. Sie erfahren in der nächsten Ausgabe der ZZI, worauf Sie beim Cloud-Computing achten müssen und wieso es derzeit problematisch sein kann, Daten in Cloud-Systemen außerhalb des EWR zu speichern.

→ **Dr. Thomas H. Lenhard**

CHECKLISTE WLAN-ROUTER

1. Ist der WLAN-Router für eine Praxis geeignet?
2. Ist der Administratorzugang zum WLAN-Router vom Internet aus gesperrt?
3. Wurden sämtliche Standardpasswörter des WLAN-Routers geändert und verfügt das Gerät über ein sicheres Passwort für den Administrator-Account (Klein- und Großbuchstaben, Sonderzeichen, Zahlen und mindestens 16 Zeichen Länge)?
4. Sind Verbindungen zur Nutzeroberfläche des WLAN-Routers nur verschlüsselt möglich?
5. Wird der WLAN-Router regelmäßig aktualisiert (Firmware-Updates)?
6. Sind nicht benötigte Funktionen im WLAN-Router deaktiviert?
7. Werden ausschließlich die Verschlüsselungsverfahren WPA2 oder WPA3 eingesetzt?
   7a. Soweit WPA2 eingesetzt wird, ist dann die Option PSK (pre-shared Key) gewählt und die Nutzung von AES aktiviert?
   7b. Soweit mit PSK gearbeitet wird, beinhaltet dann der pre-shared key sowohl Klein- wie auch Großbuchstaben, Sonderzeichen und Zahlen und ist wenigstens 32 Zeichen lang?
8. Ist die WPS-Funktion im WLAN-Router deaktiviert?
9. Soweit möglich: Ist die MAC-Filterung im WLAN-Router aktiviert?
10. Soweit möglich und zielführend: Ist DHCP (automatische Zuweisung von IP-Adressen) deaktiviert und sind feste IP-Nummer vergeben worden?
11. Soweit möglich: Ist die SID ausgeblendet?
    Anmerkung: Üblicherweise kann eine SID zur Herstellung einer Verbindung manuell eingegeben werden. Allerdings soll es Geräte geben, die sich nicht mit dem Netz verbinden lassen, wenn sie die SID nicht selbst finden.
12. Soweit möglich: Haben Sie im WLAN-Router Zeitfenster definiert, zu denen eine Verbindung per WLAN zum Router zulässig ist?
13. Ist es zutreffend, dass sich in Ihrer Praxis Patienten und Gäste nicht über das WLAN der Praxis ins Internet einwählen dürfen/können?
14. Gibt es Gründe dafür, dass das WLAN in Ihrer Praxis nicht durch Kabelverbindungen oder eine Netzwerkverbindung über das Stromnetz ersetzt werden können?

Falls Sie eine oder mehrere Fragen mit Nein beantwortet haben, besteht hinsichtlich der WLAN-Konfiguration Verbesserungspotenzial. Sollten Sie noch die Verschlüsselungsverfahren WEP oder WPA nutzen, wäre sogar ein sofortiges Handeln angebracht.