Management &
Krankenhaus
Zeitung für Entscheider im Gesundheitswesen

GIT VERLAG
Sonderdruck aus Management & Krankenhaus, August 2012, 31. Jahrgang, S. 24

WLAN – die Krux zwischen Datenschutz und Prozessoptimierung

Ob Patienten-Internet oder Notepad für den Arzt … WLAN ist Klinikalltag. Doch der Einsatz ist nicht ohne Fallstricke.

Stefanie Schneider, Mittbach

Seit Einführung der Diagnosis Related Groups (DRGs) wird ein leistungsorientiertes, pauschaliertes Vergütungssystem in Kliniken verwendet. So kann eine Klinik mittels WLAN ihre Prozesse stark verbessern. Das ermöglicht schnelle, schlanke und effiziente Prozesse. Lutz Hausmann, Geschäftsführer der Securepoint GmbH, Lüneburg, weiß hierzu mehr.

M & K: *Warum braucht eine Klinik ein WLAN?*

Lutz Hausmann: Ein wesentlicher Bestandteil zur Verbesserung der Leistungsfähigkeit im Krankenhaus ist die nahtlose Vernetzung über mehrere Standorte oder Räumlichkeiten hinweg, die durch WLAN-Infrastrukturen (Wireless LAN) leicht erreicht werden kann. Werden zudem die Patientendaten im Rahmen einer mobilen Visite und digitalen Patientenakte möglichst in Echtzeit im KIS erfasst und verarbeitet sowie WLAN-fähige medizinische Diagnosegeräte, etwa Röntgengeräte, Waagen etc., eingebunden, lassen sich Prozesse hinsichtlich Dauer und Effizienz erheblich verbessern und die Behandlung des Patienten beschleunigen.

Internet für Patienten ist kein Thema?

Hausmann: Doch, das ist sogar ein sehr spannendes Angebot. Denn ein wichtiger Nebeneffekt der WLAN-Nutzung ist die Möglichkeit der einfachen Bereitstellung kostenloser oder kostenpflichtiger Patienten-Mehrwert-Dienste, wie man es im Hotel gewöhnt ist, z. B. Internet-Anwendungen wie Web-Surfen, E-Mails schreiben oder TV und Video-on-Demand.

Sind WLANs große Herausforderungen für die IT-Abteilung?

Hausmann: Nicht zwangsläufig. Für den Einsatz von WLAN-Infrastrukturen in Kliniken und Praxen werden Managementsysteme zur sicheren Verwaltung der unterschiedlichen Anwendungen wie die mobile Patienten-Visite oder Patienten-Mehrwert-Dienste benötigt. Diese sog. Network Access Controller (NAC) wie die Securepoint-NAC-Systeme übernehmen die Aufgaben der Trennung von Netzen und Kommunikation über virtuelle LANs (VLAN). Damit sind klinisches Personal und Patienten vor den Gefahren des Internets geschützt und die Klinik kann den gesetzlichen Anforderungen an Sicherheit und den Nachweispflichten als Betreiber solcher Dienste nachkommen.

Könnten Sie das Prinzip dieser Netztrennung genauer erläutern?

Hausmann: Der gleichzeitige Betrieb mehrerer virtueller WLAN-Netze (VLAN) mit eigenen Kennungen (SSID) und eigenen Sicherheitsstufen ermöglicht die sicherheitsrelevante Separierung der Datenverbindungen in Patienten- und Mitarbeiternetze. Ebenfalls

ist zu beachten, dass nur Access Points verwendet werden, die für die Verwendung in diesen Bereichen zertifiziert sind. Das Zertifikat EN 60601-1-2 bescheinigt diesen Access Points die elektromagnetische Verträglichkeit (EMV), die für den Einsatz in medizinischen Einrichtungen notwendig ist. Denn es muss sichergestellt sein, dass medizinische Diagnosegeräte nicht beeinträchtigt werden, nicht unnötiger Elektrosmog entsteht und die Messergebnisse jederzeit zuverlässig bleiben.

Also ist die WLAN-Integration eher ein Sicherheitsthema, denn ein technisches?

Hausmann: Die Übertragung von Patientendaten mittels Funkwellen in einem WLAN über Access Points beinhaltet ein Grundproblem: Funkstrahlung breitet sich in alle Richtungen

aus, und meistens strahlen die WLAN-Funkstrahlen sogar weiter, als es der Betreiber möchte. Ein potentieller Angreifer muss sich nur in der Nähe des WLAN befinden, um Zugriff auf dessen Signale und damit auf die übertragenen Daten zu erhalten. Daraus resultiert die Folgerung, dass ein WLAN gegen Missbrauch geschützt werden muss. Das gilt generell, und besonders im Klinikumfeld mit den hochsensiblen Patientendaten.

Wie schützt eine Klinik ihr WLAN und ihre Daten?

Hausmann: Dies kann nur durch die Methoden der Kryptografie geschehen, da eine Authentifizierung durch MAC- oder IP-Adressen leicht zu umgehen ist. Der aktuelle Standard IEEE 802.11i verwendet als Verschlüsselungsmethode das Wi-Fi-Protected-Access-2 (WPA2)-Protokoll. WPA2 ist die Implementierung eines Sicherheitsstandards für Funknetzwerke nach den WLAN-Standards IEEE 802.11a, b, g und n und basiert auf dem Advanced Encryption Standard (AES). Er stellt den Nachfolger von WPA dar, das wiederum auf dem mittlerweile als unsicher geltenden Wired Equivalent Privacy (WEP) basiert. WPA2 implementiert die grundlegenden Funktionen des neuen Sicherheitsstandards IEEE 802.11i. Die Network Access Controller von Securepoint unterstützen diese Technologien vollständig.

Kann man bei so heiklen Daten in Sachen Sicherheit der Technik vertrauen?

Hausmann: Ja, das soll aber nicht leichtfertig geschehen. Der behandelnde Arzt hat die Verantwortung für die Sicherheit der ihm anvertrauten Patientendaten. Die technischen Lösungen kann er in der Regel nicht beurteilen und ist auf die Hersteller und Entscheidungsträger angewiesen. Viele Lösungen auf dem Markt verhalten sich im Hinblick auf die besonderen Anforderungen im Gesundheitswesen nicht gesetzes-konform und verursachen unter Umständen erhebliche Kosten, Ärger und haben rechtliche Konsequenzen. Dem Klinik-Management ist ebenfalls oft nicht bewusst, dass die Verwendung solcher Systeme die Sicherheit der Patientendaten beeinträchtigt. Ebenso wissen viele Ärzte nicht, dass die Verantwortung, und damit die Haftbarkeit, für die Sicherheit der Patientendaten nicht allein bei der Klinikdirektion oder den Chefärzten liegt, sondern zu großen Teilen auch beim behandelnden Arzt selbst.

Ist die Verantwortung des Arztes für die Daten rechtlich geregelt?

Hausmann: Ja, in mehrerer Hinsicht. Lassen Sie mich ein paar Beispiele nennen: In § 9 Abs. 1 MBO wird vorgeschrieben, dass der Arzt über das, was ihm in seiner Eigenschaft als Arzt anvertraut worden ist, zu schweigen hat. Dieses Satzungsrecht wird durch § 203 Abs. 1 des Strafgesetzbuches (StGB) bestätigt. Danach wird jeder Arzt, der unbefugt ein fremdes, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis offenbart, das ihm als Arzt anvertraut oder sonst bekannt gegeben worden ist, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Standesrechtlich kann die Verletzung der ärztlichen Schweigepflicht sogar zum Widerruf der ärztlichen Approbation führen.

Wer also nicht sicherstellt, dass Daten digital abhörsicher übertragen werden, handelt fahrlässig. Darüber hinaus regelt das Datenschutzgesetz, dass die bei der Behandlung anfallenden Patientendaten nur digital erfasst und bearbeitet werden dürfen, wenn der Patient schriftlich eingewilligt hat. Laut Bundesdatenschutzgesetz sind Daten im Gesundheitswesen sogar als besonders schützenswert anzusehen. Für die Übermittlung der Patientendaten mittels digitaler Methoden (E-Mail, WLAN etc.) ist daher ein entsprechender Schutz anzuwenden. Und eben ganz wichtig: Für die Einhaltung der betreffenden Datenschutzgesetze ist die Stelle und die Person verantwortlich, bei der die personenbezogenen Daten erhoben und digital gespeichert bzw. verarbeitet werden, und damit der behandelnde Arzt und die Klinik.

Sind surfende Patienten nicht ein großes Sicherheit-Risiko?

Hausmann: Die Separierung der Netze über die Network Access Controller reduziert dieses Risiko. Aber die Entscheidung, den Patienten Internet-Zugang über WLANs zu gewähren, zieht rechtliche Konsequenzen für die Klinik nach sich. Werden den Patienten zusätzlich Mehrwert-Dienste, wie eine Internet-Nutzung, angeboten, kommen weitere gesetzliche Nachweispflichten auf die medizinische Einrichtung als Betreiber zu, wenn Patienten oder Mitarbeiter Gesetzesverstöße begehen.

So findet das Urheberrechtsgesetz (UrhG) Anwendung, wenn illegale Downloads durchgeführt werden, beispielsweise bei Musikdateien. Auch die Anti-Terror-Gesetze sind zu berücksichtigen, wenn ein Missbrauch der IT-Infrastruktur im Bereich Terror und Kriminalität nachgewiesen werden kann. Als Provider von Zugangsdiensten für Patienten findet im Weiteren das Telekommunikationsgesetz (TKG) und die Richtlinie zur Vorratsdatenspeicherung in der Rechtsprechung Anwendung, da alle Anbieter von öffentlichen Telekommunikationsdiensten hier verpflichtet werden. Jedoch bieten sich auch große Chancen, da sich hierdurch zusätzliche Einnahmequellen für das Krankenhaus ergeben und für Patienten, ähnlich wie in einem Hotel, ein besserer Servcie geboten wird.

Und dennoch lohnt sich das Risiko WLAN?

Hausmann: Die Optimierung von Geschäftsprozessen in Kliniken durch die mobile IT-Infrastruktur gehört heute zu den wichtigen Voraussetzungen, um zukunftssicher aufgestellt zu sein. Wichtig ist allerdings, Netzwerkprodukte wie NACs einzusetzen, welche die besonderen Sicherheits- und Gesetzesvorschriften im Klinikumfeld beachten, und als Arzt sich bewusst zu sein, dass sich die Verantwortung dafür nicht komplett an die IT delegieren lässt.

| www.securepoint.de |

Zur Person

Lutz Hausmann, 48, leitet als geschäftsführender Gesellschafter seit 1998 die Securepoint GmbH, ein führendes Software-Unternehmen der IT-Security-Branche in Europa. Das inhabergeführte, unabhängige Unternehmen beschäftigt über 60 Mitarbeiter. Der studierte Informatiker Hausmann ist seit 2011 auch geschäftsführender Gesellschafter der Medical-IT-Services GmbH & Co. KG, die sich mit IT-Security in Arzt-Praxen und dem Klinik-Umfeld widmet. Medical-IT-Services ist ein von den Kassenärztlichen Vereinigungen bundesweit zertifizierter Provider für KV-SafeNet und bietet Arzt-Praxen und Kliniken u.a. ein Sicherheitspaket für KV-SafeNet und D2D-Kommunikation.