Medizinische Datenverarbeitung und Internet Datenschutz in der medizinischen Datenverarbeitung

Die Datenverarbeitung und die Kommunikation im Internet hat auch in den medizinischen Alltag Einzug gehalten. Problematisch ist dabei immer wieder die Verarbeitung von personen- und patientenbezogenen Daten in einem sogenannten Intranet bei gleichzeitiger Verwendung dieser Hardwarekomponenten, die auch den Zugang zum Internet ermöglichen. Diesem Themenkreis haben sich die Datenschutzbeauftragten der Länder angenommen. Der Sächsische Datenschutzbeauftragte hat darum gebeten, dass das Schreiben des Datenschutzbeauftragten des Landes Nordrhein-Westfalen vom 18. Februar 2002 der Sächsischen Ärzteschaft auf geeignete Weise zur Kenntnis gegeben wird. Der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen führt dazu Folgendes aus:

„Aufgrund verschiedener Anfragen und Beratungsersuchen hatte ich Veranlassung auf die bestehenden grundsätzlichen Bedenken zum Thema medizinische Datenverarbeitung und Internet einzugehen.
Die steigende Attraktivität des Internets führt in zunehmendem Maße dazu, dass auch Systeme, die medizinische Daten verarbeiten, einen Internetanschluss erhalten. Sei es, um das Internet als Kommunikationsnetz zum Austausch von patientenbezogenen Dokumenten zwischen Leistungserbringern auf Basis sogenannter Medizinnetze zu nutzen oder um das Informationsangebot des Internets dem medizinischen Personal zugänglich zu machen. Das Internet wurde allerdings als offenes System konzipiert. Sicherheitsüberlegungen spielten dabei keine oder nur eine untergeordnete Rolle. Patientendaten verarbeitende Systeme hingegen unterliegen wegen des hohen Schutzbedarfs der Daten entsprechend hohen Sicherheitsanforderungen und sind von ihrer Natur her als geschlossene Systeme zu betrachten.
Mit den Techniken der Verschlüsselung und der digitalen Signatur ist es zweifellos möglich, eine sichere Ende-zu-Ende Kommunikation via Internet zu realisieren. Insofern lässt sich im Internet ein „virtuell privates netz“ (VPN) aufbauen, sozusagen ein „Intranet im Internet“. Auf der reinen Kommunikationsebene ist ein solches VPN hinreichend sicher, was die Vertraulichkeit und Integrität der übermittelten Daten betrifft.
Was aber meist in die Sicherheitsbetrachtung nicht hinreichend mit einbezogen wird, sind die an das VPN angeschlossenen Endgeräte. Aber gerade auf diesen Endgeräten sind die medizinischen Daten gespeichert. Besteht nun die Möglichkeit, von diesen Endgeräten aus das „Intranet im Internet“ zu verlassen und beliebige Dienste und Teilnehmer des Internets „anzusprechen“, wird das sichere VPN gegenüber dem öffentlichen und unsicheren Internet geöffnet. Durch eine solche Öffnung ergeben sich durch die Unzulänglichkeiten der heutigen Internettechnologie nicht zu unterschätzende Risiken für die Vertraulichkeit, Integrität und Verfügbarkeit der auf den Endgeräten gespeicherten Daten.
Die Betreiber von Medizinnetzen versuchen zwar diesem Problem entgegenzuwirken, indem sie für das „Intranet im Internet“ ein zentrales, Firewall gesichertes Gateway zur Verfügung stellen. Damit reduziert man aber im Wesentlichen nur die Gefahren, die von Hackerangriffen verursacht werden, nicht jedoch die der Internettechnologie immanenten Risiken, die zum Beispiel von sogenannten aktiven Inhalten (wie ActiveX, JavaScript, Java-Applets) ausgehen können.
Ferner können verschlüsselte Informationen nicht durch die zentrale Firewall auf schadenverursachende Programmcodes (wie Viren, Trojaner, Würmer) überprüft werden. Somit wird diese Problematik auf die Endgeräte verlagert, da eine zentrale Firewall hier keinen Schutz bieten kann. In diesem Zusammenhang stellt sich die grundsätzliche Frage, ob Virenscanner überhaupt einen ausreichenden Schutz vor schadenverursachenden Programmcodes bieten können, da sie nur das abwehren können, was auch bekannt ist. Da aber täglich neue Formen solcher Programmcodes über das Internet verbreitet werden, müssen die Hersteller von Virenscannern auch ständig ihre Virendefinitionsdateien aktualisieren und die Nutzerinnen und Nutzer gleichfalls ihre Programme entsprechend updaten. In der Zeit zwischen dem Auftreten eines neuen Schadensprogramms bis zum Update des Virenschutzprogramms ist allerdings das jeweilige Datenverarbeitungssystem schutzlos, was in der medizinischen Datenverarbeitung nicht hingenommen werden kann. Ferner ist mittlerweile ein Angriff über HTTP bekannt. Um diesen Angriff zu unterbinden, müsste auf der Firewall das HTTP-Protokoll gesperrt werden. Damit wäre aber auch der WWW-Dienst nicht mehr nutzbar, was einem „Abschalten“ des Internetzugangs gleichkäme. Darüber hinaus kann auch durch eine zentrale Gateway nicht verhindert werden, dass einzelne Teilnehmerinnen und Teilnehmer eines Medizinnetzes auf ihren Endgeräten noch einen weiteren Internetzugang über einen öffentlichen Internetprovider installieren. Damit würden die Sicherheitsmechanismen des gesamten Medizinnetzes unterlaufen.
Als besonders problematisch sind allerdings Systeme zu bewerten, die ohne die Schutzmechanismen eines professionell betriebenen Medizinnetzes auskommen müssen und auf einen Standard-Internetanschluss zugreifen. Dies dürfte aber erfahrungsgemäß der Normalfall bei den niedergelassenen Ärztinnen und Ärzten sein. Es steht zu befürchten, dass die Patientendaten, die auf solchen Systemen

verarbeitet werden, ohne jeglichen Schutz sind. Damit ist deren Vertraulichkeit, Integrität und Verfügbarkeit in hohem Maße gefährdet.
An dieser Stelle kann ich nicht alle Sicherheitsrisiken und deren Auswirkungen im Detail darstellen. Meine grundsätzlichen Bedenken werden aber von Sicherheitsexperten geteilt. Da man heute leider noch keine umfassende technische Lösung hat, wird das Problem der Endgerätesicherheit aus kommerziellen Gründen allerdings meist verschwiegen. Insofern lässt man die Ärzteschaft im Unklaren über die Gefahren, denen sie sich unter Umständen aussetzen. Dies halte ich für sehr bedenklich, da letztlich die Ärztin und der Arzt verantwortlich für die Wahrung des Arzt-Patienten-Geheimnisses sind und sie auch die straf- und haftungsrechtlichen Folgen für solche offenkundigen Mängel tragen werden müssen.
Es ist deshalb nach meiner Auffassung dringend erforderlich, dass die Ärzteschaft über die mit der Internettechnologie verbundenen Gefahren umfassend aufgeklärt wird. Nur so können die Ärzte und Ärztinnen entscheiden, was sie für sich persönlich verantworten können und was nicht. Ich wäre Ihnen deshalb außerordentlich verbunden, wenn Sie die Mitglieder Ihrer Kammer über diese Gefahren ins Bild setzen würden mit dem Ziel, die bestehenden Datenschutzmängel im Hinblick auf die besonders schutzwürdigen Belange der betroffenen Patientinnen und Patienten, aber auch der betroffenen Ärztinnen und Ärzte unverzüglich abzustellen. ...“

Wir empfehlen Ihnen, sich mit dieser Problematik anhand Ihrer Ausstattung zu beschäftigen. Für die Sächsische Landesärztekammer dürfen wir Ihnen mitteilen, dass wir zwei getrennte Netze, nämlich ein Intranet für die Nutzung von Daten innerhalb der Sächsischen Landesärztekammer und ein Netz für den Zugang zum Internet, bei jeweils zwei getrennten Hardwarekomponenten installiert haben.

Assessor Michael Kratz, Datenschutzbeauftragter
der Sächsischen Landesärztekammer