Verlagsbeilage, August 2014

‹kes›
Die Zeitschrift für Informations-Sicherheit

special

Sonderdruck für TELEMED @
Kommunikationslösungen

Datenschutz und IT-Sicherheit in Arztpraxis und Klinik

SecuMedia

Komplettlösungen sichern Praxis-IT ab

Praxissysteme schützen, Patientendaten sichern

Cyberkriminalität und systematische Spionage sind mittlerweile leider ein Alltagsproblem. Alle zwei Sekunden wird weltweit ein Schadprogramm ins Netz gestellt. Alle 30 Sekunden wird eine Identität im Web gestohlen. Das Netz kennt keine Ländergrenzen. Die Komplexität der Viren und die Angriffe aus dem Internet nehmen dramatisch zu. Daher ist es heute wichtiger denn je, sich möglichst umfassend zu schützen.

Von Dirk Roeder, CGM Deutschland AG, Geschäftsbereich telemed

Gerade im Gesundheitswesen hat Datenschutz oberste Priorität. Grundsätzlich gilt die ärztliche Schweigepflicht gem. § 203 Strafgesetzbuch. Dies gilt auch für die Online-Übertragung von Sozialdaten/ Patientendaten sowie den Schutz der Praxis-EDV vor Zugriffen aus dem Internet. Die ärztliche Schweigepflicht ist von grundlegender Bedeutung für das Vertrauensverhältnis zwischen Arzt und Patient sowie der Wahrung von Patientengeheimnissen. Eine Verletzung dieser Grundlagen kann mit einer Geld- oder Freiheitsstrafe geahndet werden. Zur sicheren Online-Kommunikation sind vor allem das Bundesdatenschutzgesetz (BDSG) sowie die Datenschutzempfehlungen der Kassenärztlichen Bundesvereinigung (KBV) und der Bundesärztekammer (BÄK) richtungsweisend. Besondere Relevanz erfahren die Datenschutzvorschriften im Hinblick auf die ärztliche Dokumentationspflicht.

Datenschutzkonforme Übertragung von Patientendaten

Das Internet als Kommunikationsplattform in Praxen kann nicht mit dem Verhalten von Privatnutzern verglichen werden. Aus straf- und haftungsrechtlichen Gründen sind besondere Datenschutzvorkehrungen in der Praxis unumgänglich.

Den optimalen Schutz bietet die Daten- und E-Mail-Übertragung in einem geschlossenen Intranet wie zum Beispiel über die DSL, SDSL, VDSL, ISDN oder UMTS Vollzugänge von telemed. Hier erfolgt die Router-Einwahl der Praxis direkt in das Intranet, wo die Daten sicher und datenschutzkonform übertragen werden. Durch den Einsatz von zentralen Sicherheitsmechanismen wie Firewalls, Proxy-Server, Virenscanner, NAT ist die einzelne Praxis für Angreifer aus dem Internet nicht sichtbar.

Für den Zugriff ins Internet kann die Praxis zwischen drei telemed-Sicherheitszonen wählen:

— X-Zone
Die X-Zone bietet der Praxis den Zugriff auf Dienste der Kassenärztlichen Vereinigungen (KVen) beziehungsweise der Hausärztlichen Vertragsgemeinschaft (HzV) und der Kassenzahnärztlichen Vereinigungen (KZV) wie zum Beispiel die Online-Abrechnung und den eDMP-Versand. Weiter können telemed Mehrwertdienste wie der SMS-Versand, die gesicherte E-Mail-Übertragung, der Versand von eArztbriefen genutzt werden. Die Übertragung erfolgt hierbei geschützt im telemed-Intranet. Der Zugang zum Internet ist in dieser Sicherheitszone nicht möglich.

— S-Zone
Die S-Zone bietet den gleichen Leistungsumfang wie die X-Zone. Zusätzlich besteht hier die Möglichkeit, dedizierte, auf Sicherheit geprüfte fachliche Internetseiten aufzurufen (Whitelist). Zu diesen Seiten gehören zum Beispiel Seiten von Krankenkassen, Kassenärztlichen Vereinigungen, Arztinformationssystemherstellern, medizinische Inhalte.

— I-Zone
Auch die I-Zone bietet den Praxen die sichere Nutzung von Diensten der KVen beziehungsweise der HzVen und der KZVen sowie der telemed-Mehrwertdienste. Im Gegensatz zu den Varianten I und S hat der Teilnehmer hier jedoch die Möglichkeit, einen überwiegenden Teil aller Internetseiten aufzurufen, wobei potenziell gefährliche Webseiten gesperrt

sind (Blacklist). Die Blacklist wird seitens telemed permanent gepflegt und aktualisiert, was mehr Komfort und Sicherheit für die Praxen bedeutet.

Neben der Datenübertragung mittels Direkteinwahl in ein geschlossenes Intranet ist – zum Beispiel für Praxen, die bereits über einen herkömmlichen Online-Zugang verfügen – die Datenübertragung mittels eines Virtual Private Network (VPN) möglich. Hierbei erfolgt über einen bestehenden Online-Zugang der Praxis via Hardware- oder Software VPN die Einwahl in das Intranet, wo die sichere Datenübertragung erfolgt. Der Zugang ins Internet erfolgt dabei allerdings über den vorhandenen Provider und nicht über die Schutzmechanismen eines Intranets mit Direkteinwahl. Hierdurch besteht für die Praxis ein erhöhtes Risiko für Angriffe aus dem Internet über den vorhandenen Provider. Die Direkteinwahl über ein geschlossenes Intranet ist daher datenschutzrechtlich der Datenübertragung via VPN vorzuziehen.

KV-SafeNet

KV-SafeNet ist die hardwarebasierte, hochsichere Anbindungsvariante an das sogenannte „Sichere Netz der KVen“ (SNK), welche von den Landesdatenschützern zur Kommunikation von Sozial- und Patientendaten empfohlen wird. Auch hier ist die Anbindung per Direkteinwahl in ein Intranet als auch die Datenübertragung via VPN möglich. Über KV-SafeNet können unter anderem die seit dem ersten Quartal 2011 verpflichtende Online-Abrechnung sowie eDMP-Daten und eArztbriefe datenschutzkonform übertragen werden.

Zur Installation der KV-SafeNet-Zugänge in den Arztpraxen ist vor allem die Vor-Ort Unterstützung - auch im Supportfall - wichtig. Das Unternehmen telemed bietet Arztpraxen ein bundesweites KV-SafeNet geschultes und zertifiziertes Servicepartnernetz für Konfiguration, Installation und Wartung der Zugänge und Endgeräte direkt vor Ort.

Online-Rollout zur Erprobung der ersten Stufe der Telematik-Infrastruktur

Neben KV-SafeNet wird in Deutschland aktuell der sogenannte Online-Rollout der Telematik-Infrastruktur in zwei Testregionen (Nord-West und Süd-Ost) erprobt. Der Begriff „Telematik“ ist eine Kombination der Wörter „Telekommunikation“ und „Informatik“. Es handelt sich hierbei um die Vernetzung der IT-Systeme von Arztpraxen, Apotheken, Krankenhäusern und Krankenkassen und ermöglicht so einen systemübergreifenden Austausch von Informationen.

Die Telematik-Infrastruktur ist ein geschlossenes Netzwerk, zu dem man nur mit Heilberufsausweis und Gesundheitskarte Zutritt erlangt. Sie wird konzipiert und eingeführt von der „gesellschaft für Telematikanwendungen der Gesundheitskarte mbH“ (gematik), einer Organisation, die von den Spitzenverbänden der Leistungserbringer und Kostenträger des deutschen Gesundheitswesens gegründet wurde.

Zentrales Thema der Konzeption der Telematikinfrastruktur ist, dass sie bestehende Informationsgrenzen im Gesundheitswesen überwindet. Die ärztliche Schweigepflicht und das Recht auf informationelle Selbstbestimmung bleiben jederzeit gewahrt.

Aktuell wird die Online-Infrastruktur zur Vernetzung der Teilnehmer im Gesundheitswesen erprobt. Diese soll nach der eingehenden Erprobung mit umfassender Evaluation, die 2016 abgeschlossen sein soll, bundesweit ausgerollt werden.

KV-SafeNet dient der Anbindung der Leistungserbringer an das sichere Netz der Kassenärztlichen Vereinigungen (KVen)

Für die Testregion Nord-West erhielt im Dezember 2013 die CompuGroup Medical AG im Konsortium mit Strategy& und KoCo Connector von der gematik den Auftrag für den Online-Rollout zur Erprobung der ersten Stufe der Telematik-Infrastruktur in der Testregion Nord-West (Rheinland-Pfalz, Nordrhein-Westfalen, Schleswig-Holstein).

Der Geschäftsbereich telemed stellt in dieser Testregion insbesondere die Netzinfrastruktur bereit. Weiter wird der Support, basierend auf den bereits im Bereich KV-SafeNet bewährten Strukturen, gewährleistet. Ausschreibungsgegenstand für die Testregion war die Ausstattung der teilnehmenden Heilberufler (Ärzte, Zahnärzte, Psychotherapeutenpraxen und Krankenhäuser) mit allen für die Anbindung an die Telematikinfrastruktur notwendigen Komponenten und Diensten (bspw. Konnektoren von KoCo Connector, Kartenterminals von Ingenico Orga, VPN-Zugangsdienste) sowie deren Entwicklung, Aufbau und Betrieb.

Sichere Heimarbeit weltweit via USB-Stick oder App

Wichtig ist, dass alle Mehrwertdienste, die der Arzt bisher genutzt hat, in der Telematik-Infrastruktur und dem KV-SafeNet weiter

reibungslos funktionieren. Dies gilt insbesondere auch für die Heimarbeit, denn Arzt zu sein ist nicht nur Beruf, sondern Berufung. So arbeiten viele Ärzte auch nach Praxisschluss von zu Hause aus weiter oder möchten auf Schulungen, Fortbildungen und unterwegs jederzeit über den aktuellen Stand und wichtige Ereignisse in ihrer Praxis informiert sein.

Dies ist zum Beispiel über die telemed Mobile Praxis Center und Mobile Praxis Tablet möglich. Über eine beliebige Internetverbindung wird via USB-Stick (Desktop-PCs, Notebook) oder App (Tablet-PCs) auf die Arbeitsplatz-PCs der Praxis zugegriffen. Ein spezieller Dienst ermöglicht hierbei aus der Praxis eine gesicherte VPN-Verbindung zum zentralen Gateway im telemed-Netz. Der USB-Stick oder die App bauen im Gegenzug von extern ebenfalls eine passwortgeschützte VPN-Verbindung zum zentralen Gateway im telemed-Netz auf.

Über diese Verbindung wird remote auf das Arztinformationssystem in der Praxis zugegriffen. Dies ermöglicht dem Nutzer das Lesen und Ändern von Daten oder Einlesen elektronischer Gesundheitskarten direkt im Arztinformationssystem in der Praxis sowie das Drucken von Daten aus der Praxis auf dem externen Computer.

Zusätzlich bietet die Tablet Variante via App dem Teilnehmer eine Touch-Steuerung seines Praxis-PCs. Auch die im täglichen Einsatz viel genutzten Funktionstasten und Shortcuts kann er nutzen, denn diese sind in der virtuellen Tastatur hinterlegt.

Viren- und Malware-Schutz für Praxis-PCs

Ein besonderes Augenmerk ist auf den Virenschutz der Praxis PCs zu legen. Alle einschlägigen Datenschutzempfehlungen im Gesundheitswesen, wie die der KBV und BÄK sowie die „Sicherheitsanforderungen für SafeNet-Arbeitsplätze“, raten den Praxen dringend zur Installation einer lokalen Virenschutzsoftware.

Aufgrund der aktuellen Bedrohungslage ist es sinnvoll, Virenschutzlösungen einzusetzen, die neben den lokalen Virendefinitionen auch auf eine Cloud-Prüfung zurückgreifen. So ist zum Beispiel mit dem telemed Protect Virenschutz jeder Teilnehmer im Gesundheitswesen optimal geschützt. Neben einem umfassenden Antiviren-Schutz, einer Personal-Firewall sowie Anti-Malware-, E-Mail- und Download-Schutz zeichnet sich telemed Protect vor allem durch seinen Echtzeit-Schutz durch Zugriff auf ein zentrales, permanent gemanagtes Bedrohungsverzeichnis aus.

Der telemed Protect Virenschutz lässt sich einfach installieren bei gleichzeitig minimiertem Ressourcenverbrauch der Arbeitsplatz PCs in der Praxis. Optimierte Update-Technologien sorgen für einen geringen Bandbreitenbedarf. Optional können aktiv Informationen über einen Virenbefall abgerufen werden. Ebenso können standardisierte oder spezielle Reports, wie zum Beispiel Statusreports oder Erkennungsreports, angezeigt werden. All dies spart in der täglichen Praxisarbeit Zeit und Geld – und sichert wertvolle Daten.

Als Ergänzung zum lokalen Virenschutz bietet zum Beispiel das Produkt „telemed Protect Center“ zusätzlich einen zentralen Online-Virenscanner für Browserinhalte. Dieses erkennt und entfernt Viren, bevor diese auf den Praxisarbeitsplatz gelangen. Der durch telemed zentral im Intranet gemanagte Schutz benötigt keine gesonderte Installation und verbraucht keinerlei Ressourcen der Arbeitsplatz PCs.

Schutzschild für die Praxis

Seit Februar 2013 gelten die neuen Paragrafen 630a bis 630g des Bürgerlichen Gesetzbuches, die die Rechte der Patienten und ihre Position im Gesundheitssystem stärken. Für die behandelnden Ärzte bringt das vor allem mehr Pflichten: Auch die elektronische Dokumentation in der Praxis muss veränderungsfest sein. Das heißt, Löschungen oder Änderungen müssen jederzeit nachvollzogen werden können, und das Original muss erhalten bleiben. Durch die strengeren Vorgaben gewinnen rechtskonforme Praxissysteme und der Schutz vor Datenmissbrauch stark an Bedeutung.

Die standardisierte Lösung CGM MEDGUARD zum Beispiel macht die Praxis zur gesicherten Umgebung: Nach der Installation von Hard- und Software ist sie gegen böswillige Hacker-Angriffe abgeschirmt, verfügt über einen gesicherten Online-Zugang und Patientendaten sowie Dokumente werden qualifiziert elektronisch signiert und somit zuverlässig vor Manipulation und Datendiebstahl geschützt. ■

Sie haben noch weitere Fragen?

Dann wenden Sie sich bitte an Ihren Vertriebs- und Servicepartner oder direkt an telemed:

Telefon: 0261-80002007
Fax: 0261-80002029
E-Mail: info@telemed.de

Weitere Informationen finden Sie auch unter: ***www.telemed.de***