BUNDESÄRZTEKAMMER
KASSENÄRZTLICHE BUNDESVEREINIGUNG

Bekanntmachungen

Technische Anlage

Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis

Abkürzungsverzeichnis

AES	=	Advanced Encryption Standard
BSI	=	Bundesamt für Sicherheit in der Informationstechnik
DES	=	Data Encryption Standard
DMZ	=	Demilitarized Zone
DSL	=	Digital Subscriber Line
ISDN	=	Integrated Services Digital Network
IT	=	Informationstechnologie Information Technology
LAN	=	Local Area Network
NAT	=	Network Address Translation
OSI	=	Open Systems Interconnection Reference Model
PDA	=	Personal Digital Assistant
SSL	=	Secure Sockets Layer
TLS	=	Transport Layer Security
VoIP	=	Voice over IP
VPN	=	Virtual Private Network
WEP	=	Wired Equivalent Privacy
WLAN	=	Wireless LocalAreaNetwork
WPA/WPA2	=	Wi-Fi Protected Access

1 Einleitung

Die Etablierung und Aufrechterhaltung eines angemessenen IT-Sicherheitsstandes in der ärztlichen Praxis stellt sich aufgrund der stetig steigenden Komplexität der zum Einsatz kommenden IT-Infrastrukturen, wie auch dem stark gewachsenen Bedürfnis der Ärzte zum Einsatz von elektronischer Datenkommunikation, zunehmend als schwierig dar.

Dabei spielen fehlende Ressourcen aufgrund knapper Budgets in der ambulanten Versorgung wie auch die breite Auswahl an Sicherheitsprodukten eine wesentliche Rolle.

Diese Technische Anlage zu den „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ (1) soll einen kompakten und weitgehend allgemein verständlichen Überblick über die zu tätigenden IT-Sicherheitsmaßnahmen in den Arztpraxen geben.

1.1 Zielgruppe und Umgang mit dem Dokument

Das vorliegende Dokument richtet sich an jeden Arzt, in dessen Praxis mit Hilfe informationstechnologischer Werkzeuge Patientendaten verarbeitet werden. Aufgrund des durchgehend erhöhten Schutzbedarfs der Daten und Systeme sind weiterreichende organisatorische wie auch technische Sicherheitsmaßnahmen erforderlich.

Alle organisatorischen Maßnahmen sind auch für den technischen Laien verständlich, deren Kenntnis ist daher unerlässlich. Das Dokument bemüht sich um eine allgemein verständliche Darstellung der Sachverhalte.

Da die Umsetzung der hier beschriebenen technischen Maßnahmen an vielen Stellen Fachwissen erfordert, welches nicht zu den typischen Kompetenzen von Ärzten gehört, sollte die Umsetzung durch einen entsprechend erfahrenen IT-Dienstleister erfolgen und dies vom beauftragten Dienstleister dem Arzt gegenüber auch bestätigt werden. Das vorliegende Dokument richtet sich also auch an den vom Arzt jeweils beauftragten IT-Dienstleister und sollte diesem vorgelegt werden. Falls es z. B. aufgrund eines Einbruchs in den IT-Systemen des Arztes zu einem Schaden und einer Gerichtsverhandlung kommen sollte, könnte der Arzt so darlegen, dass er seinen Sorgfaltspflichten ausreichend nachgekommen ist. Selbstverständlich kann ein technisch versierter Arzt auch selbst IT-Sicherheitsmaßnahmen treffen, deren korrekte Umsetzung er dann aber auch eigenverantwortlich vertreten muss.

Die Mitarbeiter einer Arztpraxis sollten ihre Ansprechpartner des IT-Dienstleisters kennen. Dies dient hinsichtlich des Supports dazu, um schnelle und umfassende Hilfe zu erhalten und verhindert die vertrauliche Weitergabe von Informationen (Passwörter etc.) an unberechtigte Dritte.

1.2 Sicherheitsempfehlungen des BSI auf der Basis von IT-Grundschutz

Im Rahmen der Einführung und Gewährleistung von effizienten und effektiven IT-Sicherheitsmaßnahmen müssen eine Vielzahl von Prozessen betrachtet werden. Bei der Umsetzung unterstützen die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) (5) in Verbindung mit dem BSI-Standard 100-2, die Vorgehensweise nach IT-Grundschutz. Darin enthalten sind IT-Hinweise, Lösungsansätze für IT-Sicherheitskonzeptionen, praktische Umsetzungshilfen sowie diverse Hilfsmittel wie Checklisten, Muster und Beispiele zu den IT-Grundschutz-Katalogen (6).

Die Hinweise auf Regelungen der IT-Grundschutz-Kataloge vom Bundesamt für Sicherheit in der Informationstechnik (BSI) müssen beachtet werden. Bei Unklarheiten sollten die IT-Grundschutz-Kataloge des BSI zur Problemlösung hinzugezogen werden.

In der Technischen Anlage befinden sich Auszüge aus den IT-Grundschutz-Katalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) (5) und aus dem Leitfaden IT-Sicherheit (2).

2 Nutzung vorhandener Schutzmechanismen

Viele der heute in Arztpraxen eingesetzten Programme verfügen über eine Vielzahl hervorragender Schutzmechanismen. Aufgrund falscher Konfiguration oder aus Unkenntnis der vorhandenen Möglichkeiten zur Absicherung können Schwachstellen in IT-Systemen in der Arztpraxis resultieren.

Auch in modernen Praxisverwaltungssystemen sind zum Schutz der Patientendaten Sicherheitsmechanismen wie Passwortschutz oder Verschlüsselung integriert. Diese sind unbedingt zu nutzen und in ihrer höchsten Schutzstufe zu betreiben.

2.1 Umgang mit Passwörtern

Die meisten Zugangsschutzverfahren werden durch Passwortabfragen realisiert. Durch zu kurze, leicht erratbare Kennwörter ist es für unbefugte Dritte problemlos möglich, Einbrüche in IT-Systeme zu vollziehen. Durch systematisches Ausspähen, Probieren oder Raten gelangen Angreifer erfolgreich an Passwörter. Weiterhin macht es die sprichwörtliche Aufbewahrung des Passwortes unter der Tastatur oder in der Schreibtischschublade Unbefugten besonders leicht, an vertrauliche Informationen zu gelangen.

2.1.1 Qualitätsanforderungen an ein Passwort

Ein Passwort sollte bestimmten Qualitätsanforderungen genügen, um sich vor Hackerwerkzeugen (z. B. vollautomatisierte Abfrage von Zeichenkombinationen) zu schützen. Ein Passwort sollte länger als sieben Zeichen sein, nicht in Wörterbüchern vorkommen sowie nicht aus Namen oder persönlichen Daten (z. B. Geburtsdatum) bestehen. Des Weiteren sollten auch Sonderzeichen (z. B. $, #, ?, *, &) und/oder Ziffern enthalten sein. Bei der Verwendung von Sonderzeichen und Ziffern sollten gängige Varianten, wie beispielsweise das Anhängen einfacher Ziffern oder Sonderzeichen am Anfang oder Ende, vermieden werden.

Passwörter müssen unverzüglich geändert werden, wenn der Verdacht besteht, dass jemand unbefugt Kenntnis erlangt hat. Darüber hinaus ist eine regelmäßige Erneuerung ratsam, um das Risiko zu reduzieren, dass jemand unbemerkt Kenntnis vom Passwort erlangt hat. Die Anforderung, Passwörter regelmäßig zu erneuern, verleitet allerdings dazu, diese offenkundig an vermeintlich sicheren Orten (z. B. unter der Schreibtischauflage) aufzubewahren. Ist eine Aufbewahrung erforderlich (z. B. weil das Passwort selten verwendet und deshalb leicht vergessen wird), sollte sie sicher erfolgen, z. B. in einem verschlossenen Umschlag im Tresor oder abschließbaren Schrank.

2.1.2 Voreinstellungen und Leer-Passwörter

Die Einstellung von Standardpasswörtern in Accounts von Softwareprodukten ist allgemein bekannt. Hacker versuchen zunächst sich über diese Standardpasswörter Zugang zu verschaffen. Bei Neuinstallationen von Softwareprodukten sollten stets die Handbücher nach voreingestellten Passwörtern gesichtet und diese umgehend geändert werden.

Weiterhin sollte vom Hersteller zugesichert werden, dass sich keine sog. „Backdoors“ (nicht dokumentierte Administrationszugänge) für den Supportfall in der Software befinden.

Für Experten Bei der Installation von Betriebssystemen müssen die standardmäßigen Einstellungen überprüft werden. Hierbei wird dringend empfohlen die Optionen „Speicherung von Passwörtern“ zu deaktivieren.

2.2 Schutz von Arbeitsplatzrechnern

Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

Jedes gängige Betriebssystem bietet die Möglichkeit, Tastatur und Bildschirm nach einer gewissen Wartezeit oder sofort zu sperren. Die Entsperrung erfolgt dann erst nach Eingabe eines korrekten Passwortes. Neben der sofortigen manuellen Sperrung können auch Bildschirmschoner benutzt werden, um unbefugte Dritte bei vorübergehender Abwesenheit des rechtmäßigen Benutzers den Zugang zu dessen PC zu erschweren (z. B. PC in der Nähe des Wartezimmers einer Arztpraxis). Die automatische Aktivierung der Sperre sollte nicht zu schnell erfolgen, um eine Störung des Benutzers nach kurzen Arbeitspausen zu vermeiden. Ein häufig angewandter Zeitpunkt ist fünf Minuten nach der letzten Benutzereingabe (2).

Weiterhin sollte im Rahmen der Aufbauorganisation der Arztpraxis darauf geachtet werden, dass ein getrennter Aufnahme- und Wartebereich zum Schutz der Patientendaten besteht. Es sollte z. B. sichergestellt werden, dass Patienten, z. B. im Empfangsbereich, aber auch in den einzelnen Behandlungsräumen, nicht ungewollt Zugang zu fremden Patientendaten erlangen. Die IT-Infrastruktur sollte in der Arztpraxis nicht frei zugänglich für die Patienten sein.

2.3 Einsatz von Viren-Schutzprogrammen

Auf den in der Arztpraxis verwendeten Rechnern sind aktuelle Virenschutzprogramme unverzichtbar. Über Datenträger oder Netze wie Internet, Intranet sowie über das interne Netz einer Arztpraxis, können Computerviren verbreitet werden. Der Einsatz von Virenschutzprogrammen ist auch für Rechner ohne Internetanschluss oder Netzanbindung verpflichtend.

Virenschutzprogramme bieten allerdings nur dann effektiven Schutz, wenn sie auf dem neuesten Stand gehalten werden. So genannte Updates (Aktualisierungen) sind daher regelmäßig erforderlich. Für IT-Systeme, die aus Sicherheitsgründen keine direkte Verbindung mit den Systemen des Anbieters des Virenschutzprogramms haben, muss (möglichst vom IT-Dienstleister) eine Aktualisierung über einen Datenträger (z. B. USB-Stick, welcher die erforderlichen Dateien von einem „Internet-Rechner“ zugespielt bekommt) durchgeführt werden.

Achtung: *Selbst wenn Virenschutzprogramme immer auf dem neuesten Stand sind, bieten sie keinen absoluten Schutz vor Computerviren, Würmern und anderen Schadprogrammen. Es muss davon ausgegangen werden, dass ein Computersystem neuen Viren zumindest solange ausgesetzt ist, bis geeignete Virensignaturen von den Herstellern der Schutzprogramme zur Verfügung gestellt werden können (2).*

2.4 Mindestmaß der Datenzugriffsmöglichkeiten

Für Experten Betreffend der Datenzugriffsrechte sollte darauf geachtet werden, dass jeder Benutzer des Computersystems (einschließlich Administrator) ausschließlich Zugriffe bzw. Ausführrechte auf die seinem Tätigkeitsfeld entsprechenden Datenbestände und Programme hat. Insbesondere Programme, welche Verwendung bei der Systemadministration finden, sollten auf die jeweiligen Mitarbeiter beschränkt sein, welche diese für Ihre Arbeit benötigen. Die vergebenen Zugriffsrechte sollten in regelmäßigen Abständen auf Aktualität bezüglich der jeweiligen Tätigkeitsfelder überprüft werden.

2.5 Beschränkung der Arbeit mit Administratorrechten

Für Experten Viele Benutzer arbeiten unwissentlich oder wissentlich in der Rolle eines Administrators, die praktisch keinen Einschränkungen unterliegt und alle Systemprivilegien beinhaltet. Dadurch erhöht sich das Risiko im Falle einer erfolgreichen Übernahme der Administratorrolle durch unbefugte Dritte oder insbesondere durch ein Virus. Arbeitet der Benutzer hingegen mit eingeschränkten Systemrechten, kann in der Regel auch ein Schadprogramm (z. B. Virus) keine sicherheitskritischen Manipulationen am System vornehmen. Daher sollte für die tägliche Arbeit ein eingeschränktes Benutzerkonto mit den nötigsten Rechten verwendet werden. Nur bei Softwareinstallationen oder Konfigurationsänderungen am System ist eine Arbeit mit Administratorrechten sinnvoll (2). Selbstverständlich dürfen Software-Installationen und Änderungen der Systemkonfiguration nur fachkundigen Personen vorbehalten sein. Nur absolut notwendige Software sollte auf einem Rechner, der Patientendaten verarbeitet, installiert werden.

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Zu diesem Zweck sollten die berechtigten Personen über Zugriffskontrollmechanismen (z. B. Passwörter) legitimiert werden (siehe Kapitel 2.1).

2.6 Begrenzung von Programmprivilegien

Für Experten Neben der Rechtevergabe an einzelne Benutzer verfügen ausführbare Programme über bestimmte Zugriffsrechte und Systemprivilegien. Ein Benutzer vererbt in vielen Fällen die eigenen Berechtigungen an das gestartete Programm. Im Rahmen eines Angriffs und der Zweckentwendung des Programms durch den Angreifer, verfügt dieser somit über die vererbten Rechte des Benutzers. Programm-Berechtigungen sollten eingehend geprüft und nur mit Rechten ausgestattet werden, welche eine fehlerfreie Anwendung dieser garantieren.

2.7 Anpassung der Standardeinstellungen

Für Experten Viele Betriebssysteme und Softwareapplikationen sind vom Hersteller häufig mit Standardpasswörtern und Standard-Benutzer-Accounts vorkonfiguriert. Um Missbrauch zu vermeiden, müssen diese deaktiviert werden. Auch ist häufig die Programm- oder Systemkonfiguration noch nicht mit sicheren Vorgaben vorbelegt. Ein „frisch“ installiertes und noch nicht an die eigenen (Sicherheits-)Bedürfnisse angepasstes System sollte deshalb nie im produktiven Betrieb (bspw. in der Arztpraxis) genutzt werden! Betriebssysteme besonders exponierter Rechner sowie wichtige Server müssen „gehärtet“ werden. Das bedeutet in der IT-Sicherheit die Entfernung aller Softwarebestandteile und Funktionen, die zur Erfüllung der vorgesehenen Aufgabe durch das Programm nicht zwingend notwendig sind. Dadurch sinkt das Risiko, dass ein Angreifer durch den Missbrauch eines ungenutzten Programms Administrator-Privilegien auf dem System erlangt, die „Angriffsfläche“ des Systems wird reduziert (2).

2.8 Beachtung der Handbücher

Die zu einem System gelieferten Produktdokumentationen sollten aufmerksam gelesen werden. Oft werden Warnhinweise des Herstellers übersehen, wodurch dann später Probleme auftreten: Inkompatibilitäten, Systemabstürze oder unentdeckte Schwachstellen. Insbesondere die in Handbüchern in der Regel enthaltenen Hinweise für die sichere Konfiguration und den Betrieb sollten unbedingt befolgt werden.

2.9 Nutzung von Chipkarten

Chipkarten sind sichere Träger von kryptographischen Schlüsseln. Bei Vorliegen der notwendigen Sicherheitszertifizierungen für die Chipkarte bieten sie einen effektiven Schutz der Schlüssel, da diese nicht von der Karte ausgelesen werden können. Kann ein Sicherheitsmechanismus auf den Schutz eines kryptographischen Schlüssels durch eine Chipkarte zurückgeführt werden, ist der Nachweis seiner Sicherheit und Effizienz einfach.

Chipkarten werden für die Ver-/Entschlüsselung von Daten, der Authentisierung des Inhabers gegenüber elektronischen Diensten und die (ggf. sog. qualifizierte, d. h. rechtsgültige) elektronische Signatur eingesetzt. Aufgrund der beschriebenen Funktionen sind Chipkarten und die dazugehörigen geheimen PINs vom Eigentümer (z. B. Arzt) insbesondere vor Verlust oder den Zugriff durch Dritte zu schützen. Detaillierte Hinweise dazu liefert der Aussteller der Chipkarte in seiner Dokumentation.

Es wird empfohlen, Daten für den Transport über potentiell unsichere Netzwerke mit dem öffentlichen Schlüssel der Chipkarte des Empfängers zu verschlüsseln (sog. Hybridverschlüsselung mit asymmetrischer Kryptographie). Dies gilt z. B. für den Versand von medizinischen Daten per E-Mail in einem Intranet oder über andere Kommunikationsprotokolle und Anwendungen, wie z. B. Anwendungen für elektronische Patientenakten. Auch die Authentisierung des Arztes z. B. gegenüber einem medizinischen Web-Portal in einem Intranet sollte über eine Chipkarte erfolgen. Bisher übliche Verfahren mit Username und Passwort können bei weitem nicht die Sicherheit einer Chipkarte bieten.

Werden private/geheime kryptographische Schlüssel nicht auf eine sicherheitszertifizierte Chipkarte sondern als sog. Soft-Keys auf der Festplatte abgelegt, sind sie grundsätzlich Angriffen ausgesetzt. So kann ein spezialisierter Schadcode den Schlüssel samt ggf. erforderlichem Passwort stehlen und sowohl medizinische Daten entschlüsseln und dem Angreifer zuleiten als auch mit der Identität des Arztes auf elektronische Dienste (z. B. Webportale) mit Patientendaten zugreifen. Dies würde eine folgenschwere Kompromittierung der entsprechenden Dienste bedeuten.

3 Nutzung von Internet und Intranet

Die höchste Sicherheit ist gegeben, wenn keine Nutzung von Intra- sowie Internet in der Arztpraxis besteht. Bei der Nutzung von Intra- und Internet sollten reglementierende Maßnahmen getroffen werden. Umso offener ein Netz gestaltet ist, desto umfangreichere Sicherheitsvorkehrungen müssen getroffen werden, um die Sicherheit von Patientendaten zu gewährleisten.

Die in der Rahmenrichtlinie der Kassenärztlichen Vereinigungen „KV-SafeNet“ beschriebenen Bedingungen können als Beispiel für eine gesicherte Anbindung der teilnehmenden Ärzte zu den jeweiligen Diensteanbietern aufgeführt werden. Die geforderten Sicherheitsanforderungen können durch den IT-Dienstleister gewährleistet und somit eine gesicherte Anbindung zur Verfügung gestellt werden (3).

3.1 Allgemeine Hinweise

3.1.1 Virenschutz

Für Experten Virenschutzprogramme müssen so konfiguriert werden, dass sie Datenträger und Netze (Intranet, Internet) überwachen. Des Weiteren müssen auch Rechner ohne Anbindung an Netze über Virenschutzprogramme verfügen, um eine versehentliche Virenverschleppung auf das vernetzte System zu vermeiden.

Es wird dringend empfohlen, die Virenschutzprogramme stets auf dem aktuellen Stand zu halten (bei Bedarf mit Offline-Prozeduren, Kap. 2.3), da aufgrund sich schnell ausbreitender neuer Viren auch eine Anpassung des Virenscanners nötig ist, um den Schutz weiterhin zu gewährleisten.

Ausführbare Dateien, Skripte, heruntergeladene Dateien etc. sollten in regelmäßigen Abständen überprüft werden. Vor einer Tages- oder Monatssicherung empfiehlt sich ein vollständiges Durchsuchen aller Dateien.

3.1.2 Empfehlungen bei Sicherheitsvorfällen

Um bei Verdacht von begründeten Sicherheitsproblemen (z. B. Virenbefall) effizient agieren zu können, sollte ein Konzept vorliegen. Dies kann so gestaltet sein, dass eine externe Firma bei Bedarf beauftragt wird, weitere Maßnahmen einzuleiten. Wichtig ist, dass der infizierte/angegriffene Rechner vom Netz genommen wird und nicht in Kontakt mit Patientendaten kommt.

Besteht der Verdacht, dass aufgrund von Virenbefall oder eines anderen Sicherheitsvorfalls Patientendaten kompromittiert wurden, wird dringend empfohlen, den betroffenen Rechner nicht mehr zu verwenden, bis geklärt werden kann, ob evtl. eine Analyse durch Ermittlungsbehörden notwendig ist. Dies kann insbesondere auch zur Entlastung des Arztes führen, weil dadurch nachgewiesen werden kann, dass er mit der Technik sorgfältig umgegangen ist. Die tägliche Arbeit kann in der Zwischenzeit von einem anderen Rechner nach Aufspielen der letzten Datensicherung fortgesetzt werden.

3.1.3 Firewalls

3.1.3.1 Einführung

Die Zielsetzung einer Firewall ist die Regulierung und Absicherung des Datenverkehrs zwischen Netzsegmenten in verschiedenen Vertrauensstufen. Der klassische Einsatzzweck ist, den Übergang zwischen einem lokalen Netzwerk (LAN) (hohes Vertrauen) und dem Internet (kein Vertrauen) zu kontrollieren. Häufig kommt diese auch zwischen zwei oder mehreren organisationsinternen Netzen zum Einsatz, um dem unterschiedlichen Schutzbedarf der Zonen Rechnung zu tragen, z. B. Rechner, die in einem Kommunikationsnetzwerk mittels Firewall in einem DMZ abgeschottet werden.

Unterscheiden muss man zwischen der Hardware-Firewall (Netzwerk-Firewall) und der softwarebasierenden Personal-Firewall (Desktop-Firewall), die lokal auf dem zu schützenden Rechner installiert sind.

3.1.3.2 Anwendung und Einsatz in der Arztpraxis

Für Experten Informationen und Daten, welche in einem internen Netzwerk zur Verfügung stehen, sind einem überschaubarem Risiko ausgesetzt. Werden diese Netze oder ein Rechner jedoch über das Internet zu einem Intranet verbunden, wird dringend empfohlen ein speziell für diesen Zweck vorgesehenes (sog. dedi-

ziertes) Hardware-Gerät (z. B. Router) mit Firewall- und VPN-Funktionalität zu verwenden. Die sichere Anbindung ist jedoch nicht nur von der Hardware abhängig. Auch durch unsachgemäße Administration dieser Geräte kann eine Schwachstelle entstehen. Um eine sichere Anbindung zu gewährleisten, sind spezifische Kenntnisse über die Konfiguration der Geräte erforderlich, um die eigenen Daten gegenüber dem öffentlichen Netz zu schützen. Die Firewall ist mit den restriktivsten Regeln zu konfigurieren (z. B. keine pauschale Weiterleitung des gesamten ankommenden Datenverkehrs an einem Rechner, nur den nötigsten Datenverkehr zulassen). Weiterhin ist die Konfiguration durch eine geeignete Passwortvergabe, inklusive Call-Back oder Preshared Key Verfahren vor unbefugten Zugriffen zu schützen (3).

Der Arzt sollte sich von den Sicherheitsleistungen des Produktes überzeugen. Dazu sind Sicherheitszertifizierungen oder gute Referenzen hilfreich.

Die Konfiguration und Inbetriebnahme des Gerätes sollte von einem Experten vorgenommen werden. Wird die Konfiguration durch den Arzt oder das Praxispersonal selbstständig durchgeführt, ist die Überprüfung durch einen IT-Sicherheitsdienstleister dringend zu empfehlen, da sich in vielen Fällen gravierende Sicherheitslücken ergeben können. In einer Umgebung, in der IT-Systeme mit unterschiedlichem Schutzbedarf (z. B. Systeme mit Patientendaten und Systeme, die mit anderen Netzen kommunizieren), empfiehlt sich ein mehrstufiges Firewallkonzept, bei dem zusätzliche Filterelemente (bspw. Router) vor- oder nachgeschaltet werden. Ziel ist, die kritischen Systeme mit Patientendaten besonders zu schützen, indem sie in einer eigenen Sicherheitszone abgeschottet werden, in der nur definierte Kommunikationsverbindungen zugelassen werden.

Die Sicherung eines Netzes bzw. Teilnetzes sollte also stets über eine weitere Firewall erfolgen, darüber hinaus kann eine Verbindung zum „KV-SafeNet“ aufgebaut werden (3).

Bei einzelnen Rechnern bietet die Installation einer sog. Personal-Firewall oder der Betrieb mit einer aktivierten Windows-eigenen Firewall zumindest einen Basisschutz; Unix-artige Systeme (z. B. unter Linux oder Mac OS X) müssen mit aktivierten, eigenen Firewall-Mechanismen betrieben werden.

Des Weiteren kann in einem internen Netzwerk auch Software zur Integritätsüberprüfung (z. B. Tripwire oder AIDE) sicherheitskritischer Systeme zum Einsatz kommen. Diese Programme erkennen Inkonsistenzen und geben diese in Form eines Berichtes aus.

3.1.4 Beschränkung der Datenfreigaben und Dienste

Für Experten In vielen Fällen werden Serverdienste und Datenfreigaben in dem Netzwerk einer Arztpraxis bereitgestellt. Diese Serverdienste und Datenfreigaben könnten bei Bedarf für Zugriffe konfiguriert werden. Vertrauliche Daten sind damit von außen zugreifbar. Ihr Schutz hängt ausschließlich von zuverlässigen Authentisierungs- und Autorisierungsmechanismen ab. Sind diese jedoch falsch konfiguriert oder enthalten sie eine Schwachstelle, so geraten schutzbedürftige Informationen leicht in die falschen Hände. Daher sollte im Einzelfall stets geprüft werden, ob schutzbedürftige Daten überhaupt außerhalb des eigenen Systems bereitgestellt und verarbeitet werden müssen.

Alle Funktionen, Serverdienste und offene Kommunikationsports, die nach außen angeboten werden, erhöhen das Risiko einer möglichen Sicherheitslücke. Deshalb muss in jedem einzelnen Fall sorgfältig geprüft werden, ob es wirklich erforderlich ist, einen potentiellen „Problemkandidaten“ zu aktivieren und nach außen anzubieten. Bei bestehenden Installationen sollte regelmäßig überprüft werden, ob einzelne Dienste oder Funktionen nicht schlicht aus Versehen oder Bequemlichkeit aktiviert sind, obwohl sie von niemandem benötigt werden. Sowohl die Konfiguration als auch die Wartung der Systeme erfordert besonderes IT-Fachwissen und sollte deshalb nur von einem IT-Dienstleister vorgenommen werden (2).

3.1.5 Schutz von Patientendaten vor Zugriffen aus Netzen

Rechner mit Patientendaten sollten niemals direkt mit dem Internet/Intranet verbunden sein. Sobald ein direkter Zugriff aus dem Internet/Intranet auf eine Festplatte mit sensitiven Daten gelingt und diese Daten in unverschlüsselter Form abgelegt wurden, lassen diese sich auslesen. Auch die Verschlüsselung von Daten bietet keinen hinreichenden Schutz, da die Daten für die reguläre Nutzung jeweils entschlüsselt werden müssen und dann der Zugriff wieder möglich ist. Der Einsatz einer Verschlüsselungssoftware für Patientendaten wird gleichwohl dringend empfohlen. Detaillierte Informationen entnehmen sie bitte dem Kapitel 5.

3.1.6 Umgang mit Web-Browsern und E-Mail-Programmen

Bei den gängigen Internetbrowsern können vier verschiedene Sicherheitsstufen (hoch, mittel, niedrig und sehr niedrig) eingestellt werden. Durch eine entsprechende Browsereinstellung kann z. B. die Ausführung von aktiven Inhalten unterbunden werden. Es wird die Stufe „hoch“ empfohlen. Bei der Stufe „hoch“ können bestimmte Arbeiten nicht durchgeführt werden. Ist die Nutzung der Stufe „mittel“ erforderlich, sind weitergehende Sicherheitsmaßnahmen erforderlich. Insbesondere dürfen dann nur bekannte vertrauenswürdige Webseiten besucht werden.

Im Web-Browser sollten jedoch nur die aktiven Inhalte bzw. Skriptsprachen und Multimedia-PlugIns zugelassen werden, die für die Arbeit wirklich unverzichtbar sind. Besonders riskante Skriptsprachen sollten in jedem Fall deaktiviert werden (2). Web-Browser und E-Mail-Programme sind die häufigsten Einfallstore für Infektionen mit Schadprogrammen. Sie sollten deshalb nicht auf Rechner mit Patientendaten, sondern auf einem dedizierten Rechner ohne direkten Zugriff auf Patientendaten betrieben werden.

Ist die Verwendung eines Browsers zwingend notwendig, weil z. B. Patientendaten mit einem Krankenhaus- oder Laborportal über das http-Protokoll kommuniziert werden, sollten nur die absolut notwendigen Web-Seiten aus diesem Rechner angesteuert werden. Eine Einschränkung der Seiten kann organisatorisch – oder besser technisch – durch eine Firewall erzwungen werden. Dies ist wichtig, weil Infektionen mit Schadcode häufig bereits allein durch den Besuch einer Webseite ausgelöst werden, z. B. über infizierte Bilder in Werbeeinblendungen. Dies kann sogar bei sonst vertrauenswürdigen Seiten passieren, etwa wenn der Web-Server unbemerkt infiziert wurde.

Weiterführende Informationen

Welche Skripte, Protokolle oder Zusatzprogramme Sie meiden sollten, kann sich mit neuen technischen Entwicklungen immer wieder ändern. Aktuelle Hinweise über riskante Techniken finden sich auf den Internetseiten des BSI. Zurzeit gelten ActiveX, Active Scripting und JavaScript als besonders gefährlich (2).

Von Schadfunktionen in Dateianhängen empfangener E-Mails geht eine große Gefahr aus, wenn diese ungewollt ausgeführt werden. Solche Anhänge dürfen nicht arglos ohne Überprüfung geöffnet werden. Die Verwendung eines Viren-Schutzprogramms ist Pflicht! In Zweifelsfällen ist eine Nachfrage des Empfängers

beim Absender vor dem Öffnen eines Anhangs ratsam. Bestimmte E-Mail-Programme öffnen und starten Anhänge ohne Rückfrage beim Anwender. Das automatische Öffnen von E-Mail-Anhängen kann durch Wahl eines E-Mail-Programms ohne diese Funktionalität bzw. durch geeignete Konfiguration (Deaktivierung) oder durch die Nutzung von Zusatzprogrammen technisch verhindert werden (2).

3.2 Internet

Um den passiven Schutz bei der Nutzung des Internet zu erhöhen, empfiehlt es sich, nur bekannte bzw. die notwendigsten Web-Seiten zu besuchen.

3.2.1 Nutzung eines dedizierten Internet-Rechners

Es wird empfohlen, für die Nutzung des Internets hinsichtlich medizinischer Recherchen, Online-Banking, Diskussionsplattformen usw. einen dedizierten Rechner zu verwenden, welcher über keinen direkten Zugriff auf Patientendaten oder einen anderen vernetzten Rechner mit Patientendaten verfügt. Aufgrund von Sicherheitslücken (z. B. Internet-Browser, E-Mail-Programme, siehe Kapitel 3.1.6) kann eine unbemerkte Kompromittierung des Rechners erfolgen. Somit empfiehlt es sich, einen Nutzeraccount mit eingeschränkten Rechten zur Internetnutzung einzurichten, um den Schaden so gering wie möglich zu halten. Heruntergeladene Dateien können hier auf Inhalt und Viren geprüft werden und, wenn unbedingt nötig, anschließend per Datenträger ins interne Netz weitertransportiert werden.

Für Experten Der exponierte Rechner sollte möglichst als „read-only"-System betrieben werden, so dass ein erfolgreicher Angriff/Virenbefall keinen dauerhaften Schaden anrichten kann. Hier ist ein Betrieb als Live-System denkbar das von CD/DVD gestartet werden kann.

Alternativ kann ein solches System auch als „virtuelle Maschine", z. B. mit kostenloser Virtualisierungssoftware (VMWare Server/Player, VirtualPC usw.) betrieben und bei jedem Start in den ursprünglichen Zustand zurückversetzt werden. Eine Infektion mit Schadsoftware würde dann beim nächsten Start quasi rückgängig gemacht werden.

Niemals sollte ein sicherheitsrelevanter Rechner direkt mit dem Internet verbunden werden; stets sollte die Verbindung zumindest über einen Router mit NAT-Funktionalität, besser durch eine Firewall, erfolgen. Grund dafür ist, dass ein direkt verbundener Rechner mit „offizieller" IP-Adresse direkten Angriffen ausgesetzt ist. Wird dagegen NAT verwendet, werden nur IP-Pakete dem Rechner zugestellt, die er selbst angefordert hat.

Müssen Patientendaten über das Internet (immer unter Einsatz von Transport-Verschlüsselung, z. B. SSL/TLS) kommuniziert werden, müssen diese bereits „stark verschlüsselt[1]" sein, bevor sie auf den „Internet-Rechner" gelangen (siehe Kapitel 3.3.3). Aufgrund des hohen Risikos wird von einer derartigen Kommunikation generell abgeraten.

Weiterführende Maßnahmen

Es ist empfehlenswert, Sicherheitsmaßnahmen technisch zu erzwingen, um zu unterbinden, dass Anwender durch Fehlbedienung oder in voller Absicht Sicherheitsmechanismen abschalten oder umgehen. Die Übertragung gefährlicher Skripte beim Surfen oder potentiell verdächtiger E-Mail-Anhänge kann durch zentrale Einstellungen an der Firewall bzw. Verwendung eines sog. Proxys unterbunden werden (2).

3.2.2 Internet mit gesichertem Kanal via VPN

Für Experten Wenn ein Netzwerk oder ein Rechner mit einem Intranet über das Internet verbunden wird, sollte ein spezielles, sicher konfiguriertes Hardware-Gerät (Router) mit Firewall- und VPN-Funktionalität verwendet werden. Der Einsatz eines für diesen Zweck abgesicherten und gehärteten Rechners ist auch möglich.

3.3 Intranet

3.3.1 Verbindung ins Intranet

Für die Verbindung ins Intranet sind folgende Methoden üblich und in der Regel auch sicher:

- Einsatz eines Hardware-Gerätes (VPS-Device). Das Gerät stellt eine abgesicherte verschlüsselte Verbindung zum VPN-Server („Einwahlserver") des Intranet-Providers und übernimmt auch die Authentifizierung der Verbindung. Solche Geräte sollten vom Intranet-Provider bereitgestellt werden, der auch die Verantwortung für die Sicherheit übernimmt.
- Direkte „Einwahl" im Intranet. Damit ist die Terminierung der Verbindung auf OSI-Schicht 2 direkt beim Provider gemeint. Typische Beispiele sind
  – ISDN-Einwahl über eine Nummer des Intranet-Providers
  – DSL-Verbindung beim Intranet-Provider.

Dringend abgeraten wird vom Einsatz eines Software-VPN-Clients für die Einwahl ins Intranet über das ungeschützte Internet, weil der Rechner mit dem VPN-Client in der Regel unzureichend gegen Angriffe aus dem Internet geschützt ist.

Auch für Rechner oder Teilnetze, die mit einem Intranet verbunden sind, sollten keine unnötigen Risiken eingegangen werden. Es wird empfohlen, sie als weniger vertrauenswürdig zu betrachten und Zugriffe auf die Systeme mit Patientendaten zu beschränken.

Für Experten Systeme mit Intranet-Anschluss sollten in einer eigenen Sicherheitszone betrieben werden (also als DMZ betrachtet werden) und über eine Firewall von den Patientendaten-Systemen getrennt werden. Die Policy für die Kommunikationsbeziehungen sollten so restriktiv wie möglich gestaltet werden: Am Besten sollte Datenverkehr nur von den internen Systemen auf die exponierten Systeme erlaubt sein.

Empfohlen wird die Einrichtung eines „Kommunikationsrechners", der mit dem Intranet verbunden ist und nur mittelbaren Zugriff auf Patientendaten hat, z. B. indem die zu versendenden Daten vom Patientendaten-System zuerst auf den Kommunikationsrechner exportiert werden. Praxisverwaltungssysteme sollten solche Kommunikationsbeziehungen unterstützen.

3.3.2 Kommunikation im geschützten Intranet

Zunehmend besteht die Anforderung, Patientendaten über das Internet im Rahmen von Projekten oder Portalen zu kommunizieren. Es wird dringend empfohlen, für solche Portale und die allgemeinen Kommunikationsvorgänge ein geschütztes Intranet zu verwenden.

Die Übermittlung bzw. der Empfang von Daten muss durch einen geschützten VPN-Tunnel gesichert sein. Der Aufbau darf erst nach einer gegenseitigen Authentifikation der Endpunkte erfolgen (3).

[1] Mit „starker Verschlüsselung" ist die Verschlüsselung mit vom BSI für den Schutzbedarf „hoch/sehr hoch" bzw. für med. Daten speziell zugelassenen Algorithmus und Schlüssellänge gemeint. Derzeit gelten z. B. AES ab 128 bit Schlüssellänge oder 3key-TripleDES mit 168 bit (symmetrisch), RSA mit 2048 bit Schlüssellänge oder ECDH mit 224 bit (asymmetrisch) als „stark genug" für medizinische Daten [4].

3.3.3 Kommunikation im ungeschützten Internet

Wenn die Kommunikation nicht über ein geschütztes Intranet erfolgen kann, sind alternative Sicherheitsmaßnahmen notwendig, die gewährleisten, dass die Patientendaten nicht unbefugten Personen zugänglich werden. Eine Absicherung der Übertragung z. B. über IPSec oder SSL ist hier nicht ausreichend. Die Daten sind deshalb vor der Übertragung durch moderne Kryptographie-Software zu verschlüsseln. Detaillierte Informationen entnehmen Sie bitte dem Kapitel 5 „Verschlüsselung".

3.3.4 Verbindung ins Internet über das Intranet

Für Experten Eine Verbindung ins Internet sollte über den gesicherten Proxy eines vertrauenswürdigen Providers hergestellt werden. Da in der Arztpraxis die Zugriffe auf Internet-Inhalte klar den fachlichen Aufgaben zugeordnet werden können, empfiehlt es sich, eine Positivliste der erreichbaren Adressen zu erstellen und somit den Besuch sicherheitsgefährdender Web-Seiten weitestgehend auszuschließen.

Technisch kann dies durch eine Filterung nach zugelassenen Internet-Adressen oder Domainnamen auf der Firewall geschehen.

Im Falle der Verwendung mehrerer thematisch getrennter Positivlisten ist es zweckmäßig, anstelle des Firewall-Filters jeweils eigene Proxys vorzusehen. Der Internet-Rechner sollte so konfiguriert werden, dass der Anwender ausschließlich über den ihm zugeordneten Proxy auf das Internet zugreifen kann. Ein Mehraufwand entsteht durch die Erstellung und Pflege der Positivlisten.

Aufgrund der in Kapitel 3.2.1 beschriebenen Problematik sollte für jede Verbindung ins ungeschützte Internet ein dedizierter Rechner verwendet werden, da Infektionen nicht ausgeschlossen werden können.

4 Kommunikationsnetzwerke

4.1 Local-Area-Network (LAN)

Die Local-Area-Network (LAN) Verkabelung der Arztpraxis muss durch den IT-Dienstleister/Arzt dokumentiert werden. Der Arzt muss sich überzeugen können, dass im Praxis-LAN keine Geräte angeschlossen werden, über die er keine Verfügungsgewalt hat und die den Datenverkehr der Praxis aufzeichnen können.

4.2 Wireless-Local-Area-Network (WLAN)

Der Einsatz von Wireless-Local-Area-Network (WLAN) in einer Praxis soll möglichst vermieden werden. Falls es dennoch notwendig ist, WLAN einzusetzen (z. B. weil sonst unverhältnismäßig teure bauliche Maßnahmen erforderlich wären), darf es nur mit Verschlüsselung betrieben werden, die dem aktuellen Stand der Technik entspricht. Derzeit wird eine Absicherung des WLAN mit WPA oder WPA2 empfohlen. Eine WEP-Absicherung ist nicht sicher und auch für ambitionierte Laien leicht zu kompromittieren.

4.3 Voice over IP (VoIP)

Der Einsatz von VoIP ist mit besonderen Gefahren verbunden. In vielen Fällen ist die Installation einer ungeprüften Software mit Zugang zum Internet notwendig, die mit besonderen Risiken verbunden ist. Außerdem können die Gesprächsinhalte leicht „abgehört" werden. Beim Einsatz von VoIP ohne Verschlüsselung muss man davon ausgehen, dass die Sprachdaten relativ einfach aufgezeichnet werden können. Die sog. Verkehrsdaten, also die Information, wer mit wem und wann kommuniziert hat, sind auch bei verschlüsselten Sprachdaten leichter als bei herkömmlicher Telefonie zu ermitteln. Auch nicht professionellen Angreifern ohne hoheitliche Befugnisse gelingt das Aufzeichnen der Sprach- und Verkehrsdaten von VoIP durch den Einsatz frei erhältlicher Softwaretools. Dies ist der Fall, wenn VoIP über das öffentliche Internet geleitet wird, in den meisten Fällen z. B. wenn Telefone an DSL-Modems/Router angeschlossen werden und über die öffentliche Internet-Verbindung verwenden.

Dies bedeutet nicht, dass VoIP unter allen Umständen unsicher ist. Setzt eine Telefongesellschaft VoIP über besonders abgesicherte IP-Netze (z. B. dedizierte Intranets für VoIP) ein, kann mit VoIP eine der herkömmlichen Telefonie gleichwertige Sicherheit erreicht werden. Der Arzt, der auf ein solches professionelles Angebot zurückgreifen möchte, sollte von der Telefongesellschaft bestätigen lassen, dass die Sicherheit gleichwertig oder besser als die herkömmlichen Telefonverbindungen ist.

5 Verschlüsselung

Beim Einsatz von Verschlüsselungstechnologien für den Schutz von Daten (z. B. bei der Datenübertragung) müssen geeignete Algorithmen und Schlüssellängen verwendet werden.

Es wird derzeit empfohlen, eine symmetrische Verschlüsselung nach dem Advanced Encryption Standard (AES) mit mindestens 128 bit Schlüssellänge (idealerweise AES-256) zu verwenden. Alternativ kann eine Verschlüsselung auf Basis des 3key-TripleDES (Triple Data Encryption Standard) mit 168 bit Schlüssellänge genutzt werden. Für Daten, die außerhalb der eigenen Infrastruktur gespeichert werden, muss AES-256 für die symmetrische Verschlüsselung verwendet werden. Näheres über Verschlüsselungsalgorithmen und Schlüssellängen ist in einer Technischen Richtlinie des BSI (BSI-TR-03116, http://www.bsi.de/literat/tr/tr03116/BSI-TR-03116.pdf) festgelegt.

Die Datenträger der in der Arztpraxis verwendeten Notebooks oder PDAs etc. mit Patientendaten, sind vollständig zu verschlüsseln, um bei Diebstahl einen Missbrauch sensibler Daten zu vermeiden. Des Weiteren können auch stationäre Rechner bei einem Einbruch gestohlen werden. Daher ist eine generelle Verschlüsselung, der auf einem Datenträger befindlichen Patientendaten der Arztpraxis, ausdrücklich zu empfehlen.

Der IT-Dienstleister bzw. PVS-Hersteller muss geeignete Prozeduren und Maßnahmen für das Schlüsselmanagement vorsehen, so dass einerseits die Sicherheit der Daten und andererseits deren Verfügbarkeit gewährleistet werden.

Der Einsatz von Chipkarten wird empfohlen, um den effektiven Schutz von kryptographischen Schlüsseln und somit auch der verschlüsselten Daten zu gewährleisten.

6 Datensicherung (Backup)

Sensitive Daten sowie Geschäftsdaten (z. B. Abrechnungen) müssen durch eine regelmäßige Datensicherung (Backup) gegen Verlust geschützt werden. Ein Verlust solcher Daten kann im Extremfall die berufliche Existenz gefährden.

Für die Anfertigung von Backups stehen zahlreiche Software- und Hardwarelösungen zur Verfügung. Es ist wichtig, dass ein Backup-Konzept erstellt und konsequent (am Besten automatisiert) angewendet wird, so dass Backups regelmäßig durchgeführt werden. Es ist außerdem wichtig, dass wirklich alle relevanten Daten vom eingerichteten Backup erfasst werden. Dies stellt insbesondere bei verteilten heterogenen Umgebungen (mehrere vernetzte Rechner mit verschiedenen Betriebssystemen) eine beson-

dere Herausforderung dar. Auch mobile Endgeräte wie Notebooks, unvernetzte Einzelplatzrechner und PDAs müssen in das Backup-Konzept einbezogen werden. Es sollte regelmäßig verifiziert werden, dass das Backup auch tatsächlich funktioniert und die Daten wieder erfolgreich eingespielt werden können.

Die Backup-Medien müssen unter Beachtung der gesetzlichen Vorschriften an einem sicheren Ort aufbewahrt werden. Der Aufbewahrungsort sollte zudem hinreichend gegen Elementarschäden wie Feuer, Wasser und Ähnliches geschützt sein.

Alle Anwender müssen wissen, welche Daten wann und wie lange gesichert werden. In der Regel werden nur bestimmte Verzeichnisse und Dateien gesichert, selten geschieht ein komplettes Backup (2).

Der Schutz der Backup-Medien ist für die Sicherheit der Patientendaten elementar. Am einfachsten gelangen Datendiebe über unzureichend abgesicherte Datensicherungen an sensitive Daten. Zumindest ein abschließbarer Schrank, besser ein Tresor, der auch Schutz vor Feuer bietet, sind erforderlich für die Aufbewahrung der Backup-Medien. Außerdem wird der Einsatz von Verschlüsselungen bei der Erstellung von Backups empfohlen, so dass auch entwendete Backup-Medien für Unbefugte nicht zugänglich sind.

7 Entsorgung und Reparatur von IT-Systemen und Datenträgern

Besonders wenn Computer bzw. einzelne Festplatten repariert oder weggeworfen werden, können Unbefugte (in der Regel auch noch auf defekten Datenträgern) vertrauliche Daten einsehen oder rekonstruieren. Servicetechniker sollten daher nie allein (ohne Aufsicht) an IT-Systemen oder TK-Anlagen arbeiten. Wenn Datenträger das Haus verlassen, müssen vorher alle Daten sorgfältig gelöscht werden (2).

Achtung:

Durch spezielle Software können gelöschte Dateien, welche auf herkömmliche Weise gelöscht wurden, ganz oder in Teilen lesbar wiederhergestellt werden. Sensitive und bedeutende Dateien müssen sicher durch Zusatzprogramme gelöscht werden.

8 Regelmäßige Sicherheits-Updates (Aktualisierungen)

Höchste Priorität bei Sicherheits-Updates haben angesichts der sich manchmal rasend schnell ausbreitenden neuen Viren die Virenschutzprogramme (siehe Kapitel 2.3). Updates von Web-Browsern, E-Mail-Programmen und Betriebssystemen sollten ebenfalls regelmäßig durchgeführt werden. Aber auch andere Anwendungssoftware (z. B. Praxisverwaltungssoftware) und bestimmte Hardware-Komponenten müssen regelmäßig gewartet werden.

Um IT-Systeme abzusichern, ist eine regelmäßige Informationsbeschaffung über neu aufgedeckte Schwachstellen und Hilfsmittel zu deren Beseitigung notwendig. Eigene Recherchen werden durch aktuelle Empfehlungen im Internet sowie Fachartikel erleichtert. In „neueren" Programmversionen (z. B. von Browsern) wurden sicherheitsrelevante Schwachstellen in der Regel vom Hersteller beseitigt. Dies erspart jedoch nicht eine individuelle Betrachtung, da neue Versionen in der Regel auch neue Funktionen und Fehler beinhalten, die andere Gefahren mit sich bringen.

Die Fülle ständig neu veröffentlichter Updates und Sicherheits-Patches macht zudem einen Auswahlprozess erforderlich. In der Regel können nicht alle installiert werden, insbesondere nicht im Rahmen einer Sofortmaßnahme. Daher sollte bereits im Vorfeld Einvernehmen darüber bestehen, nach welchen Auswahlkriterien bestimmt wird, welche Updates mit wie viel Zeitverzug installiert werden können bzw. müssen.

Selbst wenn der Systemverantwortliche wichtige Sicherheits-Updates nicht einspielt, bleibt deshalb weder automatisch das System stehen noch erfolgt umgehend ein bösartiger Hackerangriff. Das macht deutlich: Das Einspielen von Updates erfordert sehr viel Disziplin und muss von vornherein als Prozess verankert sein. Gerade bei Viren-Schutzprogrammen sollte das schnellstmögliche Einspielen von Updates zur Routine werden.

Zum Herunterladen von Updates ist in der Regel eine Internet-Verbindung erforderlich, was die Aktualisierung von IT-Systemen erschwert, die aus Sicherheitsgründen nicht ins Internet verbunden werden dürfen. IT-Dienstleister sollen für solche Systeme Prozeduren vorsehen, damit Updates für solche Rechner offline bereitgestellt werden können (z. B. Herunterladen auf einen „Internet-Rechner", Verteilung in die internen Systeme über einen USB-Stick, Automatisierung der Prozedur über ein Script). Besteht eine Verbindung über ein geschütztes Intranet, ist auch eine Aktualisierung über diese Verbindung möglich (2).

9 Schutz der IT-Systeme vor physikalischen Einflüssen

Nicht nur durch Fehlbedienung oder mutwillige Angriffe können einem IT-System Schäden zugefügt werden. Oftmals entstehen gravierende Schäden infolge physischer Einwirkung von Feuer, Wasser oder Strom. Viele Geräte dürfen nur unter bestimmten Klimabedingungen betrieben werden. Daher sollten besonders wichtige IT-Komponenten (Server, Sicherungsmedien, Router etc.) in ausreichend geschützten Räumen untergebracht werden. Zusätzlich sollten sie an eine unterbrechungsfreie Stromversorgung mit Überspannungsschutz angeschlossen sein. Nützliche Tipps zur Umsetzung erteilen beispielsweise die Feuerwehr sowie das Internet-Angebot des BSI (2).

10 Fernwartung

Beim Einsatz der Fernwartung müssen grundlegende Sicherheitsvorkehrungen getroffen werden, um der Datensicherheit genüge zu tun. Bei der Einwahl in die Fernwartungsaktivitäten muss eine Autorisierung mittels einem aktuell gültigen Passwort erfolgen. Grundsätzlich gilt, dass der Techniker ohne ein gültiges Passwort nicht auf den Praxisrechner zugreifen kann. Nach Beendigung einer Fernwartungssitzung sollte daher eine Änderung des Passwortes erfolgen, somit kann zu einem späteren Zeitpunkt der Techniker nicht ohne Autorisierung auf das System zugreifen.

Die Fernwartungsdaten zwischen dem Computer des Arztes und des Technikers dürfen nur verschlüsselt und über eine geschützte Verbindung (siehe Kapitel 3.3.2) übermittelt werden. Im Rahmen der Fernwartung sollte darauf geachtet werden, dass die Fernwartung ausdrücklich von der Arztpraxis freigegeben wird. Die Zugriffsrechte des Technikers müssen auf ein Minimum beschränkt werden.

In begründeten Notfällen (z. B. Systemstillstand) kann eine Wartung auf Basis der Echtdaten erfolgen. Grundsätzlich sollten jedoch Testdaten (Testpatienten) dem Fernwartungspersonal zur Verfügung gestellt werden.

Die Fernwartung muss protokolliert werden und vor Ort am Bildschirm durch den Praxisinhaber oder autorisiertes Personal überwacht werden. Weiterhin wird empfohlen, dass der Arzt oder dass Praxispersonal Mindestkenntnisse über die Praxis-EDV erwerben, um die Arbeit des Wartungstechnikers qualifiziert begleiten zu können. Anhand des Protokolls sollte jederzeit nachvollzogen werden, welche Veränderungen vorgenommen und auf welche Dateien zugegriffen wurde.

11 Elektronische Dokumentation und Archivierung

Die Anforderungen an die rechtssichere elektronische Behandlungsdokumentation von Ärzten sind sehr hoch. Der Nachweis, dass elektronisch erfasste Daten nicht nachträglich manipuliert wurden bzw. werden können, kann am sichersten durch den Einsatz von (qualifizierten) elektronischen Signaturen und Zeitstempeln erbracht werden.

Im Idealfall verfügt das PVS über ein Dokumenten-Management-System, welches die elektronische Dokumentation verwaltet. Dieses sollte mit qualifizierten elektronischen Signaturen (SigG) und qualifizierten Zeitstempeln arbeiten und auch die Anforderungen des Signaturgesetzes für das Übersignieren von Dokumenten beachten. Dabei sind PIN-Eingaben des Arztes auf ein minimales Maß zu halten, indem z. B. mehrere zusammenhängende Dokumente zusammengefasst werden oder – falls technisch möglich – sog. Stapelsignaturen ausgestellt werden. Eine vom SigG vorgesehene Übersignatur, d. h. das nachträgliche Anbringen eines qualifizierten Zeitstempels bevor die kryptographischen Algorithmen der ursprünglichen Signatur ungültig werden, sollte für den Arzt transparent und automatisiert erfolgen.

Die entsprechenden Technologien sind bereits seit Jahren verfügbar und beschrieben. Lösungen dafür müssen nicht unbedingt aufwändig sein. Ein minimaler Ansatz wäre beispielsweise die qualifizierte elektronische Signatur und die Einholung eines qualifizierten Zeitstempels (bei sicherer Netzanbindung) für die täglichen Backup-Dateien. Eine solche Minimallösung bietet allerdings nicht den Komfort eines geeigneten Dokumentenmanagement-Systems in Hinsicht auf die o. g. (voraussichtlich selten fällige) „Übersignatur".

Grundsätzlich sind auch andere Verfahren geeignet, die elektronische Behandlungsdokumentation so zu gestalten, dass der Nachweis, dass die Daten nicht nachträglich geändert wurden (bzw. geändert werden konnten), gelingen kann. Jedoch nur die qualifizierte elektronische Signatur ist vom Gesetzgeber der Schriftform gleichwertig gestellt worden und bietet somit eine rechtliche Sicherheit.

12 Literaturverzeichnis

1. Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Bundesärztekammer
2. Leitfaden IT-Sicherheit, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2007, http://www.bsi.bund.de/gshb/Leitfaden/index.htm
3. Rahmenrichtlinie der Kassenärztlichen Vereinigungen „KV-SafeNet" – Medizinische Netz-/Dienste-Infrastruktur, V2.1, Stand: 25. 5. 2007
4. Technische Richtlinie des BSI , BSI-TR-03116, http://www.bsi.de/literat/tr/tr03116/BSI-TR-03116.pdf, Stand: 23. 3. 2007
5. IT-Grundschutz-Kataloge, Bundesamt für Sicherheit in der Informationstechnik (BSI), http://www.bsi.bund.de/gshb/index.htm
6. Hilfsmittel für eine vereinfachte Anwendung der IT-Grundschutz-Vorgehensweise, Bundesamt für Sicherheit in der Informationstechnik (BSI)

http://www.bsi.bund.de/gshb/deutsch/hilfmi/hilfmi.htm

13 Glossar

Advanced Encryption Standard (AES)
Bei AES handelt es sich um ein symmetrischen Verschlüsselungsalgorithmus, welcher in vielen Produkten als Standard integriert ist. Er gilt momentan als sicher.

Backdoors
Hierbei handelt es sich um nicht dokumentierte Administrationszugänge in einer Software.

Data Encryption Standard (DES)
Der DES ist ein symmetrischer Verschlüsselungsalgorithmus. Die Sicherheit ist abhängig von der Schlüssellänge.

DMZ
Eine DMZ bezeichnet ein Netzwerk mit sicherheitstechnisch kontrollierten Zugriffmöglichkeiten auf die daran angeschlossenen Server.

Firewalling
Als Firewalling bezeichnet man den Prozess des Sicherns eines Netzwerks oder eines Teilnetzwerks mittels einer Firewall. Durch Firewalls werden vorher definierte Kommunikationsbeziehungen ermöglicht.

Lokal-Area-Network (LAN)
Lokale Netzwerke sind als feste Installation dort zu finden, wo mehrere Rechner über kleine Entfernungen an einem bestimmten Ort dauerhaft vernetzt werden.

Network Address Translation – NATing
NATing setzt die (meist privaten) IP-Adressen eines Netzes auf andere (meist öffentliche) IP-Adressen eines anderen Netzes. Somit ist es möglich einerseits mit mehreren Rechnern in einem LAN, einerseits die IP-Adresse des Internet-Access-Routers für den Internet-Zugang zu nutzen, und andererseits wird das LAN hinter der im Internet registrierten IP-Adresse des Routers verborgen.

Voice over IP (VoIP)
Unter Voice over IP (VoIP) versteht man das Telefonieren über Computernetzwerke, die nach Internet-Standards aufgebaut sind.

Wireless-Local Area-Network (WLAN)
Drahtlose lokale Netze sind Wireless-Local-Area-Network (WLAN)

Anlage – Checkliste

a) Nutzung vorhandener Schutzmechanismen

Ist der Aufnahmebereich von dem Warte- sowie Behandlungsbereich getrennt, sodass wartende Patienten/-innen keine Informationen über Dritte erlangen können?	☐
Wurden die Standardpasswörter bzw. Leerpasswörter nach Installation der Software geändert?	☐
Wurde die Standardeinstellung „Speicherung von Passwörtern“ nach der Installation des Betriebssystems deaktiviert?	☐
Ist der Zugang zum Praxiscomputer durch ein Passwort geschützt?	☐
Besitzt nur das befugte Personal Kenntnis von dem Passwort?	☐
Entspricht das Passwort dem aktuellen Sicherheitsstandard (siehe Kapitel 2.1.1)?	☐
Ist eine regelmäßige Erneuerung des Passwortes zur Risikominimierung vorgesehen?	☐
Ist das Passwort vor dem Zugriff unbefugter Dritter geschützt bzw. liegt es nicht an vermeintlich sicheren Orten (z. B. Schreibtischauflage)?	☐
Wird ein passwortgeschützter Bildschirmschoner mit kurzer Aktivierungszeit eingesetzt?	☐
Wird der Nutzer mit Administratorrechten nur für diese Aufgabe genutzt?	☐
Wurden nach der Installation des Betriebssystems oder der Software die entsprechenden Einstellungen zur Wahrung des Sicherheitsbedürfnisses getroffen?	☐
Wurde das Handbuch bei der Konfiguration sowie bei der Inbetriebnahme des Systems aufmerksam gelesen?	☐
Sind die Computer mit Viren-Schutzprogrammen ausgestattet?	☐
Besitzen die Computernutzer die für sie geeigneten Zugriffsrechte nach ihrem Tätigkeitsprofil – eingeschränktes Benutzerprofil?	☐
Wurden ausführbare Programme zur Risikominimierung mit dem Mindestmaß an Berechtigungen versehen?	☐
Werden Chipkarten zur Ver-/Entschlüsselung von Daten, sowie zur Authentisierung gegenüber elektronischen Diensten und zur elektronischen Signatur eingesetzt?	☐

b) Nutzung Internet und Intranet

Werden die Viren-Schutzprogramme regelmäßig aktualisiert?	☐
Ist Ihr Virenschutzprogramm zur Überwachung von Datenträgern als auch von Netzen konfiguriert?	☐
Gibt es regelmäßige Virenprüfungen?	☐

Liegt ein Konzept bei begründeten Sicherheitsproblemen (z. B. bei Virenbefall) vor, um effizient agieren zu können?	☐
Sind Ihre Rechner, die mit dem Internet verbunden sind, ausreichend geschützt?	☐
Wird ein Router mit Firewall- und VPN-Funktionalität verwendet?	☐
Wurde die Konfiguration des Routers/der Firewall etc. durch den Praxisinhaber oder das -personal durchgeführt?	☐
Wurden die durch den Praxisinhaber oder das -personal getätigten Einstellungen durch einen IT-Sicherheitsdienstleister überprüft?	☐
Wurde bei einzelnen Rechnern als Basisschutz die Personal Firewall aktiviert?	☐
Sind Beschränkungen von Datenfreigaben und Diensten mit zuverlässigen Authentisierungs- und Autorisierungsmechanismen versehen?	☐
Es ist kein direkter Zugriff aus dem Internet/Intranet auf einen Rechner mit Patientendaten möglich.	☐
Verwenden Sie einen Web-Browser oder E-Mail-Programme? Falls Sie einen Web-Browser verwenden: Wurden diesbezüglich weitergehende Sicherheitsmaßnahmen getroffen, um nur zulässige und dringend notwendige Scriptsprachen sowie Multimedia-PlugIns auszuführen?	☐
Nutzen Sie einen dedizierten Internetrechner hinsichtlich medizinischer Recherche, Online-Banking etc., welcher keinen Zugriff auf Patientendaten hat? Ist der Rechner gemäß Kapitel 3.2 der Technischen Anlage konfiguriert?	☐
Verwenden Sie Intranet in Ihrer Praxis? Ist die Verbindung gemäß Kapitel 3.3 der Technischen Anlage konfiguriert?	☐

c) Kommunikationsnetze

Verwenden Sie LAN in der Arztpraxis? Liegt eine Dokumentation der Verkabelung (LAN) in der Arztpraxis vor?	☐
Verwenden Sie WLAN in der Arztpraxis? Nutzen Sie zur Absicherung WPA oder WPA2?	☐
Verwenden Sie Voice over IP (VoIP)? Gewährleistet ihre Telefongesellschaft die gleichwertige Sicherheit zum herkömmlichen Telefonnetz?	☐

d) Verschlüsselung

Sind mobile Datenträger, welche Patientendaten enthalten, vollständig verschlüsselt?	☐
Sind Patientendaten auf stationären Rechner durch eine Verschlüsselung geschützt?	☐
Werden die empfohlenen Verschlüsselungstechnologien gemäß Kapitel 5 der Technischen Anlage eingesetzt?	☐
Ist ein Schlüsselmanagement integriert?	☐
Werden Chipkarten zur Ver-/Entschlüsselung von Daten sowie zur Authentisierung gegenüber elektronischen Diensten und zur elektronischen Signatur eingesetzt?	☐

e) Datensicherung

Führen Sie regelmäßige Datensicherungen durch?	☐
Werden die Datensicherungen geeignet aufbewahrt?	☐

f) Entsorgung und Reparatur von IT-Systemen und Datenträgern

Werden Maßnahmen getroffen, welche eine vollständige Löschung von Datenträgern sicherstellen (Zusatzprogramme)?	☐
Werden Servicetechniker bei Arbeiten an dem IT-System oder an der TK-Anlage beaufsichtigt?	☐

g) Sicherheits-Updates

Führen Sie folgende Updates regelmäßig durch bzw. spielen Sicherheits-Patches ein?	
● Betriebssystem	☐
● Virenschutzprogramme	☐
● Web-Browser	☐
● E-Mail-Programme	☐

h) Schutz der IT-Systeme vor physikalischen Einflüssen

Sind Ihre IT-Komponenten vor physikalischen Einwirkungen, wie Feuer, Wasser oder Strom, eingehend geschützt?	☐
Werden die IT-Komponenten unter den vorausgesetzten Klimabedingungen betrieben?	☐
Besteht eine unterbrechungsfreie Stromversorgung mit Überspannungsschutz?	☐

i) Fernwartung

Erfolgt eine Authentisierung bei der Einwahl zur Fernwartung mittels gültigem Passwort?	☐
Erfolgt die Freigabe zur Fernwartung nur durch die Praxis?	☐
Sind die Zugriffsrechte des Technikers auf ein Mindestmaß beschränkt?	☐
Erfolgt eine Aktualisierung des Passwortes nach jeder Fernwartungssitzung?	☐
Werden die Fernwartungsdaten zwischen dem Computer des Arztes und des Technikers verschlüsselt und über eine geschützte Verbindung übertragen?	☐
Werden Wartungsarbeiten bzw. Tests während der Wartung anhand von Testpatienten durchgeführt?	☐
Wird die Fernwartung protokolliert sowie vor Ort am Bildschirm durch sachkundiges autorisiertes Personal überwacht?	☐
Werden die Protokolle der Fernwartung archiviert?	☐

j) Elektronische Dokumentation und Archivierung

Werden Ihre zu archivierenden Dokumente mit einer qualifizierten elektronischen Signatur und Zeitstempeln versehen?	☐