26. Nurgat ZA, Smythe M, Al-Jedai A et al.: Introduction of vincristine mini-bags and an assessment of the subsequent risk of extravasation. J Oncol Pharm Pract 2015; 21: 339–347.
27. Institute for Safe Medication Practices (ISMP): Targeted Medication Safety Best Practices for Hospitals: Frequently Asked Questions: http://www.ismp.org/Tools/BestPractices/faq/FAQ-BP1.pdf (zuletzt geprüft: 10. Januar 2018). Horsham, Oktober 2014.
28. Arzneimittelkommission der deutschen Ärzteschaft: Umstellung von einheitlichen „Luer-Konnektoren" auf spezifische Konnektoren für verschiedene Anwendungsbereiche, um Verwechslungen vorzubeugen. AkdÄ Drug Safety Mail 2017–03 vom 24. Januar 2017.
29. Aktionsbündnis Patientensicherheit e.V.: Hilfestellung zur Umstellung von Luer-Verbindern auf neue verwechslungssichere Verbinder: http://www.aps-ev.de/wp-content/uploads/2016/08/APS-HE_LUER-Verbinder_lang-1.pdf (letzter Zugriff: 10. Januar 2018). 1. Auflage; Berlin, Dezember 2016.
30. The Newcastle upon Tyne Hospitals NHS Foundation Trust: Intrathecal Cytotoxic Chemotherapy (ITC) Policy: http://www.newcastle-hospitals.org.uk/IntrathecalCytotoxicChemotherapyPolicy201712.pdf (letzter Zugriff: 20. Februar 2018). Version 4; 7. Dezember 2017.
31. National Cancer Control Programme: Guidance on the Safe Use of Intrathecal Chemotherapy in the Treatment of Cancer: https://www.hse.ie/eng/services/list/5/cancer/profinfo/medonc/safetyreview/itcguidance.pdf (letzter Zugriff: 20. Februar 2018). Oncology Medication Safety Review. Implementation Resources. Rec. 71 Intrathecal Policies. 2. Dezember 2016.
32. Clinical Oncological Society of Australia: Guidelines for the Safe Prescribing, Dispensing and Administration of Cancer Chemotherapy: https://www.cosa.org.au/media/1093/cosa_guidelines_safeprescribingchemo2008.pdf (letzter Zugriff: 20. Februar 2018). November 2008.
33. Arzneimittelkommission der deutschen Ärzteschaft: „Aus der UAW-Datenbank": Nebenwirkungen durch Medikationsfehler. Dtsch Arztebl 2016; 113: A 1948–1950.

Sie können sich unter www.akdae.de/Service/Newsletter für einen Newsletter der AkdÄ anmelden, der auf neue Risikoinformationen zu Arzneimitteln hinweist.

Arzneimittelkommission der deutschen Ärzteschaft, Herbert-Lewin-Platz 1, 10623 Berlin, Postfach 12 08 64, 10598 Berlin, Telefon: 0 30/40 04 56-5 00, Fax: 0 30/40 04 56-5 55, E-Mail: info@akdae.de, Internet: www.akdae.de

BUNDESÄRZTEKAMMER
KASSENÄRZTLICHE BUNDESVEREINIGUNG

Bekanntgaben

Technische Anlage

Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis[1]

In der Ausgabe 10/2018 des Deutschen Ärzteblattes sind die „Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis" veröffentlicht worden (http://daebl.de/YC26). Diese -von den gesetzlichen Anforderungen abgeleiteten- Hinweise und Empfehlungen sollen mit der Technischen Anlage1 in kompakter und weitgehend allgemein verständlicher Form überblicksartig um die ggf. zu tätigenden Sicherheitsmaßnahmen ergänzt und konkretisiert werden.

Die Technische Anlage im Internet:
http://daebl.de/MA27

[1] vorläufig überarbeitete und an die DSGVO angepasste Fassung

„5. Deutscher Kongress für Patientensicherheit bei medikamentöser Therapie"

18.–19. Oktober 2018, Berlin

Gefördert durch das Bundesministerium für Gesundheit, veranstaltet von der Arzneimittelkommission der deutschen Ärzteschaft.

Kongressort: Langenbeck-Virchow-Haus, Luisenstraße 58/59, 10117 Berlin

Die Hauptthemen sind:
- 10 Jahre Aktionsplan AMTS: Erfolge und Perspektiven
- Interprofessionelle Zusammenarbeit als Schlüssel zu mehr AMTS?
- Medikationsplan: Forschungsprojekte, Status quo und Ausblick
- Nebenwirkungen durch Medikationsfehler
- AMTS in der Pädiatrie und Geriatrie
- AMTS in Therapieleitlinien
- Innovationsfonds – Untersuchungen zur AMTS

Fortbildungspunkte sind bei der Ärzte- und der Apothekerkammer Berlin beantragt.

Weitere Informationen finden Sie unter:
http://www.patientensicherheit2018.de

32. Mediweek Davos, Sommerseminarwoche

2. bis 6. Juli 2018 im Kongresszentrum Davos, Schweiz

Weiter- und Fortbildungsseminare der Schweizerischen Gesellschaft für Innere Medizin (SGIM) 2018

Die zuständigen Ärztekammern anerkennen die Fortbildungspunkte. In Deutschland und Österreich praktizierende Ärzte erhalten die Bestätigung nach Vorlage der Bescheinigung.

Wissenschaftliche Gestaltung/Kongressleitung:
Prof. Dr. Edouard Battegay, Prof. Dr. Cornel Sieber, Prof. Dr. Thomas F. Lüscher, Dr. Christian Buol, Dr. Walter Kistler, Dr. Gerd Stuckmann

Programm:
Allgemeine Innere Medizin, Diabetologie, Hepatologie, Rheumatologie, Onkologie, Infektiologie, etc.

Anmeldung und Auskünfte:
Destination Davos Klosters, Davos Congress, Talstraße 41, CH-7270 Davos Platz
Telefon: +41 (0)81 415 21 60, Fax: +41 (0)81 415 21 69
www.mediweekdavos.ch, E-Mail: info@davoscongress.ch

BUNDESÄRZTEKAMMER
KASSENÄRZTLICHE BUNDESVEREINIGUNG

Bekanntgaben

Technische Anlage

Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis[1]

[1] vorläufig überarbeitete und an die DSGVO angepasste Fassung

Deutsches Ärzteblatt | 22.06.2018 | DOI: 10.3238/arztebl.2018.ds_ta01

1 Einleitung

Die Etablierung und Aufrechterhaltung eines angemessenen Informationssicherheitsstandes in der ärztlichen Praxis ist – wie in den „Hinweisen und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ ausgeführt wird – aus datenschutzrechtlichen, strafrechtlichen und haftungsrechtlichen Gründen erforderlich. Die Artikel 24, 25 und 32 der DSGVO stellen Anforderungen an die „Sicherheit der Verarbeitung“, den „Datenschutz durch Technikgestaltung“ und die „Verantwortung des für die Verarbeitung Verantwortlichen“. Zusätzlich werden in § 22 Abs. 2 BDSG weitere Maßnahmen beschrieben, die bei der Verarbeitung besonderer Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) zu beachten sind.

Diese Technische Anlage zu den „Hinweisen und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ versucht die oben genannten, zum Teil abstrakt gehaltenen gesetzlichen Anforderungen zu konkretisieren und einen kompakten und weitgehend allgemein verständlichen Überblick über die zu tätigenden Sicherheitsmaßnahmen zu geben. Dabei kommt dieser Technischen Anlage keine normative Wirkung zu, sondern sie soll über mögliche Risiken und entsprechende Sicherheitsmaßnahmen informieren und helfen, die oben genannten Anforderungen umzusetzen.

1.1 Zielgruppe und Umgang mit dem Dokument

Das vorliegende Dokument richtet sich an jeden Arzt[1], in dessen Praxis mit Hilfe informationstechnologischer Werkzeuge Patientendaten verarbeitet werden. Aufgrund des durchgehend erhöhten Schutzbedarfs der Gesundheitsdaten und der eingesetzten Systeme sind weitreichende organisatorische wie auch technische Sicherheitsmaßnahmen erforderlich. Alle organisatorischen Maßnahmen werden auch für den technischen Laien verständlich dargestellt. Das Dokument bemüht sich um eine allgemein verständliche Darstellung.

> **Hinweis:** Da die Umsetzung der hier beschriebenen technischen Maßnahmen an vielen Stellen IT-Fachwissen erfordert, sollte die Umsetzung durch einen entsprechend erfahrenen Dienstleister erfolgen und dies vom beauftragten Dienstleister dem Arzt gegenüber auch bestätigt werden. Das vorliegende Dokument und die mit „**Hinweis**“ gekennzeichneten Passagen richten sich also auch an den vom Arzt jeweils beauftragten Dienstleister und sollten diesem vorgelegt werden. Die Beauftragung eines professionellen Dienstleisters wird empfohlen. Dabei ist bei der Auswahl des geeigneten Dienstleisters auf dessen Kompetenz sowie dessen Zuverlässigkeit zu achten. Beide Gesichtspunkte werden idealerweise durch ein Zertifikat nachgewiesen.

Die Mitarbeiter einer Praxis sollten ihre Ansprechpartner des Dienstleisters kennen. Dies dient hinsichtlich des Supports dazu, 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 muss eine Vielzahl von Prozessen betrachtet werden. Bei der Umsetzung kann das IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik (BSI) [5] in Verbindung mit dem BSI-Standard 200–2, die Vorgehensweise nach IT-Grundschutz unterstützen. Darin enthalten sind 47 „elementare Gefährdungen“ der Informationssicherheit von „Feuer“ bis „Schädliche Seiteneffekte IT-gestützter Angriffe“, modulare Bausteine eines Informationssicherheitmanagementsystems, Anforderungen und weiterführende Informationen sowie praktische Umsetzungshinweise. Die Hinweise auf Regelungen des IT-Grundschutz-Kompendiums des BSI sollten beachtet werden. Sie könnten bei der konkreten Problemlösung herangezogen werden.

Die Technische Anlage enthält vorrangig Auszüge aus dem IT-Grundschutz-Kompendium des 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. Aus falscher Konfiguration oder aus Unkenntnis der vorhandenen Möglichkeiten zur Absicherung können Schwachstellen in IT-Systemen in der Praxis 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 zu erratende 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.

Abkürzungsverzeichnis
AES = Advanced Encryption Standard
BSI = Bundesamt für Sicherheit in der Informationstechnik
DMZ = Demilitarized Zone
DSGVO = Datenschutzgrundverordnung
ISMS = Informationssicherheitsmanagementsystem
IT = Informationstechnologie/ Information Technology
LAN = Local Area Network
MAC = Media Access Control
NAT = Network Address Translation
OSI = Open Systems Interconnection
SSL = Secure Sockets Layer
TI = Telematikinfrastruktur
TLS = Transport Layer Security
UPnP = Universal Plug and Play
VoIP = Voice over IP
VPN = Virtual Private Network
WEP = Wired Equivalent Privacy
WLAN = Wireless Local Area Network
WPA2 = Wi-Fi Protected Access

[2] Berufs-, Funktions- und Personenbezeichnungen wurden unter dem Aspekt der Verständlichkeit dieses Textes verwendet. Eine geschlechtsspezifische Differenzierung ist nicht beabsichtigt.

Weiterhin macht es die sprichwörtliche Aufbewahrung des Passwortes unter der Tastatur oder in der Schreibtischschublade Unbefugten besonders leicht, an vertrauliche Informationen zu gelangen. Für jedes Zugangsschutzverfahren sollte ein separates Passwort gewählt werden.

2.1.1 Qualitätsanforderungen an ein Passwort

Ein Passwort sollte bestimmten Qualitätsanforderungen genügen, um sich vor Hackerwerkzeugen (z. B. vollautomatisiertes Ausprobieren von bekannten Zeichenkombinationen) zu schützen. Ein Passwort sollte mindestens acht Zeichen lang 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, für verschiedene Anwendungen und Dienste dieselben Passwörter zu benutzen. Sicherer ist es, die Passwörter für verschiedene Anwendungen und Dienste nach einem einheitlichen Schema zu erzeugen oder Programme für das Passwortmanagement einzusetzen, die zufällige Passwörter generieren und verwenden. Ist eine Aufbewahrung von Passwörtern erforderlich (z. B. weil es selten verwendet und deshalb leicht vergessen wird), sollten Sie diese z. B. in einem verschlossenen Umschlag im Tresor oder einem abschließbaren Schrank hinterlegen.

Häufige fehlgeschlagene Anmeldeversuche sollten zu zeitlichen Sperrungen des Zugangs führen, um das Durchprobieren von Passwörtern zu verhindern. Alternativ kann auch das betroffene Benutzerkonto gesperrt werden. Passworteingabefelder dürfen die eingegebenen Zeichen standardmäßig nicht im Klartext darstellen. Eine Trennung privat genutzter Passwörter und geschäftlich genutzter Passwörter ist dringend angeraten.

> **Hinweis:** Achten Sie bei der Beschaffung von Produkten auf die entsprechen Funktionalitäten bezüglich dem Schutz von Benutzerkonten.

2.1.2 Voreinstellungen und Leer-Passwörter

Die Einstellung von Standardpasswörtern in Benutzerkonten von Software- und Hardwareprodukten ist allgemein bekannt. Hacker versuchen zunächst sich über diese Standardpasswörter Zugang zu verschaffen. Bei Neuinstallationen von Produkten sollten stets die Handbücher nach voreingestellten Passwörtern gesichtet und diese umgehend geändert werden. Beachten Sie auch die Standardpasswörter von Geräten wie zum Beispiel Druckern, Netzwerkgeräten und weiterer Peripherie.

> **Hinweis:** Bei der Installation von Softwareprodukten müssen die standardmäßigen Einstellungen überprüft werden. Hierbei wird dringend empfohlen, die Option „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 bei Bedarf zu sperren. Die Entsperrung erfolgt dann erst nach Eingabe eines korrekten Passwortes. Neben der sofortigen manuellen Sperrung bei Bedarf können auch Bildschirmschoner bzw. die Energieoptionen des Betriebssystems benutzt werden, um unbefugten Dritten bei vorübergehender Abwesenheit des rechtmäßigen Benutzers den Zugang zu dessen PC zu erschweren (z. B. PC im Behandlungszimmer einer Praxis). Die automatische Aktivierung der Sperre sollte individuell eingestellt werden, um eine Störung des Benutzers nach kurzen Arbeitspausen zu vermeiden.

Weiterhin sollte in der Praxis darauf geachtet werden, dass ein getrennter Aufnahme- und Wartebereich zum Schutz der Patientendaten besteht. Es sollte z. B. sichergestellt werden, dass Patienten im Empfangsbereich, aber auch in den einzelnen Behandlungsräumen, nicht ungewollt Kenntnis von fremden Patientendaten erlangen. Die IT-Infrastruktur sollte in der Praxis nicht frei zugänglich für die Patienten sein. Jeder Zugriffsversuch, sowohl erfolgreich als auch erfolglos, sollte automatisiert im System protokolliert werden. Im Einzelfall ist eine Meldung des Vorfalls an die zuständige Datenschutzaufsicht und eine Benachrichtigung des Betroffenen erforderlich (siehe [1], Abschnitt 3.10.).

> **Hinweis:** Sperren Sie ihren Arbeitsplatzrechner, wenn dieser nicht besetzt ist bzw. der Patient allein im Behandlungsraum verbleibt. Aktivieren Sie zusätzlich die automatische Sperrung. Der Einsatz von Blickschutzfolien auf Monitoren kann, insbesondere in beengten Räumlichkeiten, vor neugierigen Blicken schützen.
>
> Dies gilt ebenfalls für die Anzeige von personenbezogenen Daten auf weiteren medizinischen Geräten z. B. EKG-Geräten.

2.3 Einsatz von Viren-Schutzprogrammen

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

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 Dienstleister) eine Aktualisierung über einen Datenträger (z. B. USB-Stick, welcher die erforderlichen Dateien von einem „Internet-Rechner“ zugespielt bekommt) durchgeführt werden. Alternativ gibt es Lösungen am Markt, die solche Aktualisierungen automatisiert aus dem abgesicherten Bereich (mittels Pull-Verfahren) von Systemen im unsicheren Internetbereich kopieren und einrichten.

> **Hinweis:** 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].

Deutsches Ärzteblatt | 22.06.2018 | DOI: 10.3238/arztebl.2018.ds_ta01

2.4 Begrenzung der Datenzugriffsmöglichkeiten

Die Delegation von Benutzerrechten eines Arztes an das Praxispersonal sollte immer nach dem Prinzip der minimalen Berechtigungsvergabe erfolgen und nachvollziehbar dokumentiert werden.

Hinsichtlich der Datenzugriffsrechte sollte darauf geachtet werden, dass jeder Benutzer des Computersystems (einschließlich Administrator) ausschließlich Zugriffs- bzw. Ausführungsrechte auf die für seine Tätigkeit entsprechend erforderlichen Datenbestände und Programme hat. Insbesondere Programme, welche Verwendung bei der Systemadministration finden, sollten auf die jeweiligen Benutzer 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

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 durch einen Virus. Arbeitet der Benutzer hingegen mit eingeschränkten Systemrechten, kann in der Regel auch ein Schadprogramm 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 Softwareinstallationen 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 Abschnitt 2.1).

2.6 Begrenzung von Programmprivilegien

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 Zweckentfremdung 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. Diese Entscheidungen sind zu dokumentieren, regelmäßig zu überprüfen und ggf. anzupassen.

2.7 Anpassung der Standardeinstellungen

Viele Betriebssysteme sowie Softwareapplikationen und Hardwarekomponenten sind vom Hersteller häufig mit Standardpasswörtern und Standard-Benutzerkonten 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 Praxis) 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 wie: 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 können sichere Träger von kryptographischen Schlüsseln sein. 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 einfacher.

Chipkarten werden für die Ver-/ Entschlüsselung von Daten, der Authentisierung des Inhabers gegenüber elektronischen Diensten und die (ggf. sog. qualifizierte, d. h. der handschriftlichen Unterschrift gleichgestellte) elektronische Signatur eingesetzt. Aufgrund der beschriebenen Funktionen sind Chipkarten und die dazugehörigen geheimen PINs vom Inhaber (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 Netze mit dem öffentlichen Schlüssel der Chipkarte des Empfängers zu verschlüsseln. Dies gilt z. B. für den Versand von medizinischen Daten per E-Mail 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 sollte über eine Chipkarte erfolgen. Bisher übliche Verfahren mit Benutzername 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 Patientendaten bedeuten.

3 Nutzung von Internet, Intranet und Gesundheitsnetzen

Theoretisch wäre die höchste Sicherheit für das Praxisverwaltungssystem gegeben, wenn dieses nicht an Gesundheitsnetze

und vor allem nicht an das Internet angebunden wäre, d. h. wenn das Praxisverwaltungssystem offline betrieben würde. Praktisch benötigen die Systeme aber zumindest regelmäßige Updates. Bei der unbestreitbar sinnvollen Nutzung von Gesundheitsnetzen zum Austausch von Patientendaten aber auch bei der ergänzenden Nutzung von Intranet und Internet müssen reglementierende Maßnahmen getroffen werden. Umso offener ein Netz gestaltet ist, desto umfangreichere Sicherheitsvorkehrungen müssen getroffen werden, um die Sicherheit von Patientendaten zu gewährleisten.

Der Gesetzgeber hat die Spitzenverbände des deutschen Gesundheitswesens in § 291a Abs. 7 SGB V damit beauftragt, ein sicheres und weitgehend geschlossenes digitales Gesundheitsnetz – die sogenannte Telematikinfrastruktur (TI) – in Deutschland aufzubauen. In § 291a Abs. 7 S. 3 SGB V ist geregelt, dass die TI über die Anwendungen der elektronischen Gesundheitskarte hinaus für weitere Anwendungen des Gesundheitswesens z. B. eigene Netze der Leistungserbringer genutzt werden kann. Darüber hinaus sehen die Spezifikationen einen sogenannten „Sicheren Internetservice“ (SIS) für einen Zugang in das Internet vor.

Die TI und die Netze der Leistungserbringer werden in diesem Dokument als „Gesundheitsnetz“ bezeichnet. Zu den weiteren Anforderungen an die Gesundheitsnetze siehe auch Abschnitt 3.3.2.

3.1 Allgemeine Hinweise

3.1.1 Virenschutz

Virenschutzprogramme müssen so konfiguriert werden, dass sie Datenträger und Netze (Gesundheitsnetz, Intranet und Internet) überwachen. Des Weiteren sollten 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. Jegliche Dateien von Dritten, die heruntergeladen oder z. B. per E-Mail empfangen wurden, sollten immer vor dem Öffnen überprüft werden. Vor einem Backup empfiehlt sich ein vollständiges Überprüfen aller Dateien durch den Virenscanner.

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 weiterhin 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. Sollte sich der Sicherheitsvorfall bestätigen, so ist dies gegebenenfalls bei der zuständigen Aufsichtsbehörde zu melden und ggf. der Betroffene zu benachrichtigen (siehe [1], Abschnitt 3.10.).

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 einer „Demilitarized Zone“ (DMZ) abgeschottet werden. Unterscheiden muss man zwischen der Hardware-Firewall (Netzwerk-Firewall) und der softwarebasierten Personal-Firewall (Desktop-Firewall), die lokal auf dem zu schützenden Rechner installiert sind.

3.1.3.2 Anwendung und Einsatz in der Praxis

Hinweis: 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 mit einem Gesundheitsnetz verbunden, wird dringend empfohlen, ein speziell für diesen Zweck vorgesehenes sog. dediziertes 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 automatischen Portfreigaben über UPnP). Weiterhin ist die Konfiguration durch geeignete 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 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) betrieben werden, 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, mit der nur definierte Kommunikationsverbindungen zugelassen werden. Die Sicherung eines Netzes bzw. Teilnetzes sollte also stets über eine weitere Firewall erfolgen. 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.

Deutsches Ärzteblatt | 22.06.2018 | DOI: 10.3238/arztebl.2018.ds_ta01

Des Weiteren kann auch Software zur Integritätsüberprüfung sicherheitskritischer Systeme zum Einsatz kommen. Diese Programme erkennen Inkonsistenzen und geben diese in Form eines Berichtes aus.

3.1.4 Beschränkung der Dateifreigaben und Dienste

In vielen Fällen werden Serverdienste und Dateifreigaben in dem Netzwerk einer Praxis bereitgestellt. Diese Serverdienste und Dateifreigaben könnten bei Bedarf für Zugriffe konfiguriert werden. Damit ließe sich von außen auf vertrauliche Daten zugreifen. 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 offenen 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, eine Dateifreigabe 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 worden sind, obwohl sie von niemandem benötigt werden. Sowohl die Konfiguration als auch die Wartung der Systeme erfordern besonderes IT-Fachwissen und sollten deshalb nur von einem Dienstleister vorgenommen werden [2].

3.1.5 Schutz von Patientendaten vor Zugriffen aus dem Internet

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

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

Im Web-Browser sollten 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, sollten nur die absolut notwendigen Web-Seiten von diesem Rechner aus 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 auf diesem Wege sogar bei sonst vertrauenswürdigen Seiten passieren.

> **Hinweis:** Verzichten Sie auf die Verwendung des unverschlüsselten HTTP-Protokolls und achten Sie darauf, dass auch Web-Browser und E-Mail-Programme stets mit aktuellen Updates versorgt sind.

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, JavaScript und Flash als besonders gefährlich [2].

Von Schadfunktionen in Dateianhängen empfangener E-Mails geht eine große Gefahr aus, wenn diese ungewollt ausgeführt werden. 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 Internets 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 für medizinische Recherchen, Online-Banking, Soziale Netzwerke, Online-Shopping 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 Abschnitt 3.1.6) kann eine unbemerkte Kompromittierung des Rechners erfolgen. Auch hierfür empfiehlt es sich, ein Benutzerkonto mit eingeschränkten Rechten zur Internetnutzung einzurichten, um den Schaden so gering wie möglich zu halten(siehe Abschnitt 2.5 Beschränkung der Arbeit mit Administratorrechten). Heruntergeladene Dateien können hier auf Inhalt und Viren geprüft werden und, wenn unbedingt nötig, anschließend per Datenträger ins interne Netz weitertransportiert werden.

> **Hinweis:** Der dedizierte 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 einer CD/DVD oder einem USB-Stick gestartet werden kann.

Alternativ kann ein solches System auch als „virtuelle Maschine", z. B. mit (kostenlos verfügbarer) Virtualisierungssoftware 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. Die Verbindung sollte stets zumindest über einen Router mit NAT-und Firewall-Funktionalität erfolgen.

Sollen Patientendaten über das Internet (immer unter Einsatz einer Transport-Verschlüsselung „TLS“) übertragen werden, müssen diese „stark verschlüsselt[2]“ sein, bevor sie auf den „Internet-Rechner“ gelangen (siehe Abschnitt 3.3.3).

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 im Internet oder beim Öffnen potentiell verdächtiger E-Mail-Anhänge kann durch zentrale Einstellungen an der Firewall bzw. Verwendung eines sog. Proxy-Servers unterbunden werden [2].

3.2.2 Internet mit gesichertem Kanal via VPN

Hinweis: Wenn ein Netzwerk oder ein Rechner mit einem Gesundheitsnetz 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 Gesundheitsnetze

3.3.1 Verbindung ins Gesundheitsnetz

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

- Einsatz eines Hardware-Gerätes (VPN-Device). Das Gerät stellt eine abgesicherte verschlüsselte Verbindung zum VPN-Server („Einwahlserver“) des Gesundheitsnetz-Zugangsdienst-Providers her und übernimmt auch die Authentifizierung der Verbindung. Solche Geräte sollten vom Gesundheitsnetz-Zugangsdienst-Provider bereitgestellt werden, der auch die Verantwortung für die Sicherheit übernimmt.
- Einsatz eines Software-VPN-Clients aus dem Praxisnetz in das Gesundheitsnetz mit einem zweiten Authentifizierungsfaktor. Hierbei wird eine abgesicherte verschlüsselte Verbindung zum VPN-Server aufgebaut und mittels eines zweiten Faktors die Manipulation der Authentizität bzw. der unbeobachtete Missbrauch von Praxisgeräten zum Zugang in das Gesundheitsnetz zusätzlich erschwert.

Dringend abgeraten wird vom Einsatz eines einfachen Software-VPN-Clients (ohne zweiten Faktor) für die Einwahl in das Praxisnetz 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 Gesundheitsnetz 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.

> **Hinweis:** Systeme mit Gesundheitsnetz-Anschluss sollten in einer eigenen Sicherheitszone betrieben (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.

[3]Mit „starker Verschlüsselung“ ist die Verschlüsselung mit vom BSI für den Schutzbedarf „hoch/sehr hoch“ bzw. für med. Daten speziell zugelassener Algorithmus und Schlüssellänge gemeint. Derzeit gelten z. B. AES ab 256 Bit Schlüssellänge (symmetrisch), RSA mit ab 2048 Bit Schlüssellänge oder ECIES mit 250 Bit (asymmetrisch) als „stark genug“ für medizinische Daten [4].

Empfohlen wird die Einrichtung eines „Kommunikationsrechners“, der mit dem Gesundheitsnetz 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 Gesundheitsnetz

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 Gesundheitsnetz 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].

Wenn die Kommunikation nicht über ein geschütztes Gesundheitsnetz 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 TLS ist hier nicht ausreichend. Die Daten sind deshalb vor der Übertragung durch moderne Kryptographie-Software zu verschlüsseln. Detaillierte Informationen entnehmen Sie bitte dem Abschnitt 5 „Verschlüsselung“.

3.3.3 Verbindung ins Internet über das Gesundheitsnetz

Eine Verbindung ins Internet sollte über den gesicherten Proxy-Server eines vertrauenswürdigen Providers hergestellt werden, z. B. SIS. Da in der Praxis 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 Abschnitt 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 Verkabelung des Local-Area-Network (LAN) der Praxis muss durch den Dienstleister/ Arzt dokumentiert werden. Der Arzt muss sich überzeugen können, dass im Praxis-LAN keine Geräte angeschlossen wurden, 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 WPA2 empfohlen. Eine WEP oder WPA Absicherung ist nicht sicher und auch für ambitionierte Laien leicht zu kompromittieren. Darüber hinaus sollten sowohl der WLAN-Router als auch die WLAN Clients jeweils auf dem aktuellsten Stand gehalten und Sicherheitspatches[3] zeitnah eingespielt werden. Der Zugang zum WLAN sollte auf bekannte Clients (identifizierbar über die MAC-Adresse) beschränkt werden.

4.3 Voice over IP (VoIP) und Videotelefonie über das Internet

In den letzten Jahren hat sich Telefonie über VoIP (also über technische Internet-Protokolle) weit verbreitet und verdrängt mittlerweile die klassische Telefonie über dedizierte Telefonleitungen. Viele etablierte Telefongesellschaften bieten inzwischen bei Neuverträgen sogar nur noch VoIP-Anschlüsse an.

Diese etablierten Telefongesellschaften müssen gemäß § 109 des Telekommunikationsgesetzes (TKG) Maßnahmen, zum Schutz der übermittelten personenbezogenen Daten auf dem aktuellen Stand der Technik treffen. Bei Anbietern, welche bei der Bundesnetzagentur registriert sind[4], kann davon ausgegangen werden, dass die Vertraulichkeit der Kommunikation nach dem Stand der Technik gewahrt ist. Eventuelle Sicherheitsauflagen des Anbieters müssen dabei eingehalten werden. Insbesondere müssen evtl. vom Anbieter mitgeteilte Zugangsdaten für VoIP geheim gehalten werden.

Anders sind internetbasierte Telefonie- oder Videotelefonie-Dienstleistungen zu bewerten, deren Anbieter nicht bei der Bundesnetzagentur registriert sind. In diesem Fall muss vom Anbieter verbindlich zugesichert werden, dass die Vertraulichkeit der Kommunikation technisch hinreichend gewährleistet ist. Bei Bedarf muss der Anwender selbst für eine effektive Verschlüsselung sorgen, falls diese technisch möglich ist.

Nicht empfohlen wird die Kommunikation von Patientendaten mit Hilfe von (Video-)Telefonie über VoIP, wenn diese mit Hilfe von Software auf einem gewöhnlichen Rechner in der Praxis, der direkt mit dem Internet verbunden ist, realisiert wird.

4.4 Vernetzung in der Praxis durch das Stromnetz (Powerline)

Es ist möglich, eine Vernetzung in der Praxis über das Stromnetz mit Hilfe sogenannter Powerline-Adapter zu realisieren. Vorteil einer solchen Vernetzung ist, dass keine weiteren Datenleitungen verlegt werden müssen. Nachteil einer solchen Vernetzung ist, dass sich die Datensignale auch in das Stromnetz von benachbarten Wohnungen oder Gebäuden ausbreiten können, so dass der Netzwerkverkehr abgehört oder manipuliert werden kann. Eine effektive und sichere Filterung am Stromzähler kann nicht vorausgesetzt werden. Eine Vernetzung über das Stromnetz wird aus diesem Grund grundsätzlich nicht empfohlen. Ist aus bautechnischen Gründen eine Vernetzung über LAN-Kabel nicht möglich, kann die Vernetzung über das Stromnetz nur mit besonderen Sicherheitsmaßnahmen erwogen werden. Es muss sichergestellt werden, dass die Powerline-Adapter verschlüsselt kommunizieren. Die Verschlüsselung mit einem werkseitigen Default-Schlüssel ist in der Regel nicht sicher. Ein individueller Schlüssel muss nach der Dokumentation des Herstellers in allen Powerline-Adaptern generiert und eingestellt werden. Es wird empfohlen, die korrekte Funktion der Verschlüsselung regelmäßig zu prüfen und den Schlüssel regelmäßig zu ändern. Darüber hinaus sind die Empfehlungen des BSI (BSI-TR-02102 [4]) bezüglich der Algorithmen und Schlüssellängen zu beachten.

5 Verschlüsselung

5.1 Allgemeine Hinweise

Beim Einsatz von Verschlüsselungstechnologien für den Schutz von Daten (z. B. bei der Datenübertragung) müssen geeignete Algorithmen und Schlüssellängen verwendet werden. Es wird derzeit für die langfristige Sicherheit von verschlüsselten Daten empfohlen, eine symmetrische Verschlüsselung nach dem AES mit mindestens 256 Bit Schlüssellänge zu verwenden. Für Daten, die außerhalb der eigenen Infrastruktur gespeichert werden, muss mindestens AES-256 für die symmetrische Verschlüsselung verwendet werden. Näheres über Verschlüsselungsalgorithmen und Schlüssellängen ist in der Technischen Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI (BSI-TR-02102 [4]) festgelegt. Für „Kryptographische Vorgaben für Projekte der Bundesregierung – Teil 1: Telematikinfrastruktur“ gilt die Technische Richtlinie BSI-TR-03116–1 [8] des BSI. In dieser werden entsprechende Empfehlungen je nach Anwendungsbereich (z. B. Verschlüsselung von Patientendaten, Signatur usw. für die TI) gegeben.

Die Datenträger der in der Praxis verwendeten Notebooks oder mobilen Geräte usw. 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 Praxis ausdrücklich zu empfehlen.

> **Hinweis:** Der 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.

5.2 Auslagerung der Speicherung der medizinischen Dokumentation (Datensicherung) und Datenverarbeitung an externe Firmen

Die externe Verarbeitung (u. a. Speicherung, Archivierung, etc.) von Patientendaten außerhalb des eigenen Praxisverwaltungssystems ist nur unter sehr engen rechtlichen Vorgaben (vgl. § 203 Abs. 3 S. 2 StGB und ggf. Artikel 28 DSGVO) zulässig. Die externe Verarbeitung ist mittels vertraglicher Vereinbarungen und technischer Vorgaben weitgehend einzuschränken. Der Dienstleister muss zudem ggf. zur Geheimhaltung verpflichtet werden (§ 203 Abs. 4 Nr. 1 StGB, siehe [1] Abschnitt 2.4.3.) und muss technische und organisatorische Maßnahmen ergreifen, um personenbezogene Patientendaten und das Patientengeheimnis zu schützen. Der Dienstleister sollte beispielsweise medizinische Daten getrennt von anderen Datenarten speichern, um den Beschlagnahmeschutz gem. § 97 Abs. 2 StPO zu gewährleisten. Die Übertragung der medizinischen Daten zu dem Dienstleister sollte verschlüsselt und integritätsgeschützt erfolgen. Beide Endpunkte der Kommunikation (d. h. Praxis und Dienstleister) sollten sich gegenseitig authentifizieren. Der Dienstleister sollte vertrauenswürdig sein und über ein funktionierendes IT-Sicherheitsmana-

[4] Z. B. gegen die KRACK Attacke https://www.heise.de/select/ct/2017/23/1510344956316080
[5] Link (Abruf am 23.01.2018): https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Datenschutz/datenschutz-node.html

gement verfügen. Um dies zu beurteilen sind Zertifizierungen hilfreich, wie z. B. nach der internationalen Norm ISO/IEC 27001, oder nach der internationalen Norm ISO/IEC 27001 auf der Basis von BSI-Grundschutz.

Folgende Betriebsarten der externen Datenverarbeitung und -archivierung finden hierbei besondere Beachtung:

- Die Auslagerung der Datenverarbeitung außerhalb der Praxis: Dies ist der Fall, wenn das Computerprogramm des PVS bei einem externen Dienstleister („in der Cloud"), außerhalb der Praxis betrieben wird. Damit wäre der Zugang des Dienstleisters zu den Patientendaten potentiell technisch möglich.
- Die Auslagerung der Datenhaltung außerhalb der Praxis: Dies ist der Fall, wenn das PVS in der Praxis betrieben wird, die Daten allerdings extern gespeichert werden. Selbst bei der Verwendung einer sicheren verschlüsselten Speicherung wäre dies mit dem Risiko einer verminderten Verfügbarkeit verbunden (z. B. Unterbrechung der Netzleitung, technischer Defekt, Insolvenz des Dienstleisters).

Eine externe Datenhaltung älterer Datenbestände z. B. zu Archivierungszwecken ist mit zusätzlichen Sicherheitsmaßnahmen (organisatorische und technische Redundanz, Notfallkonzepte) möglich, die das Risiko einer verminderten Verfügbarkeit ausschließen.

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 besondere Herausforderung dar. Auch mobile Endgeräte wie Notebooks und nicht vernetzte Einzelplatzrechner 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 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].

> **Hinweis:** Dieser Abschnitt ist im Zusammenhang mit dem Verzeichnis der Verarbeitungstätigkeiten (siehe [1], Abschnitt 3.7.) zu berücksichtigen.

Der Schutz der Backup-Medien ist für die Sicherheit der Patientendaten elementar. Am einfachsten gelangen Datendiebe über unzureichend abgesicherte Datensicherungen an Patientendaten. 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 und somit das gleiche Schutzniveau der Datenhaltung wie auf den Festplatten der Praxisrechner (siehe Abschnitt 5) erreicht wird. Es wird empfohlen, die Schreibrechte auf das Backup-System stark einzuschränken und so zu wählen, dass die Backupdaten auch bei einer Kompromittierung durch Schadsoftware (z. B. Cryptotrojaner) nicht mit verschlüsselt werden können und damit unbrauchbar werden.

Werden die Backup-Medien außerhalb der eigenen Infrastruktur bei einem Dienstleister gespeichert, so ist eine Verschlüsselung nach Absatz 5 erforderlich.

7 Entsorgung und Reparatur von IT-Systemen und Datenträgern

Besonders wenn Computer bzw. einzelne Festplatten und sonstige Datenträger (z. B. USB-Sticks) 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].

> **Hinweis:** Durch spezielle Software können gelöschte Dateien, welche auf herkömmliche Weise gelöscht wurden, ganz oder in Teilen lesbar wiederhergestellt werden. Durch Zusatzprogramme lassen sich solche Dateien durch mehrfaches Überschreiben sicher löschen. Alternativ können Datenträger auch physisch zerstört werden.

8 Regelmäßige Sicherheits-Updates (Aktualisierungen)

Höchste Priorität bei Sicherheits-Updates haben angesichts der sich manchmal rasend schnell ausbreitenden neuen Viren die Virenschutzprogramme (siehe Abschnitt 2.3). Das Einspielen von Updates von Web-Browsern, E-Mail-Programmen und Betriebssystemen muss ebenfalls regelmäßig und am besten automatisch durchgeführt werden. Aber auch andere Anwendungssoftware (z. B. Praxisverwaltungssoftware sowie Tools und Laufzeitumgebungen) und bestimmte Hardware-Komponenten müssen regelmäßig gewartet und aktualisiert werden.

Um IT-Systeme abzusichern, ist eine regelmäßige Informationsbeschaffung über neu aufgedeckte Schwachstellen und Hilfsmittel zur Beseitigung der Schwachstellen 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 Patches installiert werden, insbesondere nicht im Rahmen einer Sofortmaßnahme. Daher sollte bereits im Vorfeld festgelegt werden, 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.

Deutsches Ärzteblatt | 22.06.2018 | DOI: 10.3238/arztebl.2018.ds_ta01

Hinweis: 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. 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 Gesundheitsnetz, 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 Überspannung. 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 sowie organisatorische Maßnahmen getroffen werden, um der Datensicherheit genüge zu tun. Bei der Einwahl in das Praxissystem mittels Fernwartung muss eine Autorisierung mittels eines aktuell gültigen Passworts erfolgen. Der Techniker sollte ohne ein gültiges Passwort nicht auf den Praxisrechner zugreifen können. 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 kann. Alternativ bieten viele Fernwartungslösungen die Nutzung von Einmalpasswörtern je Nutzung an.

Die Fernwartungsdaten zwischen dem Computer des Arztes und des Technikers dürfen nur verschlüsselt und über eine geschützte Verbindung (siehe Abschnitt 3.3.2) übermittelt werden. Die Zugriffsrechte des Technikers müssen auf ein Minimum beschränkt 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 das Praxispersonal Mindestkenntnisse über die Praxis-IT erwerben, um die Arbeit des Wartungstechnikers qualifiziert begleiten zu können. Anhand des Protokolls sollte jederzeit nachvollzogen werden, welche Veränderungen vorgenommen wurden und auf welche Dateien zugegriffen wurde.

11 Elektronische Dokumentation und Archivierung

Die elektronische Dokumentation wird in § 630f BGB nur allgemein geregelt.

Im Fall der elektronisch geführten Patientenakte ist durch den Einsatz einer geeigneten Softwarekonstruktion sicherzustellen, dass nachträgliche Änderungen automatisch kenntlich gemacht werden (vgl. [1], Abschnitt 4.2.). Aus Sicht des Anwenders ist es geboten, ein Praxisverwaltungssystem einzusetzen, welches über eine entsprechende Funktionalität verfügt. Alternativen zur Verwendung einer IT gestützten Änderungsdokumentation, die gleichermaßen rechtssicher sind, sind aus dem Gesetz nicht ableitbar. Dennoch sollen an dieser Stelle Vorgehensweisen dargestellt werden, die die Position des Benutzers in einem Haftungsprozess möglicherweise verbessern können.

Der Mangel, der durch technische Maßnahmen ausgeglichen werden soll, ist das Löschen, Ersetzen oder Verändern des ursprünglichen Inhalts der Patientenakte sowie die mögliche Änderung des Zeitpunkts eines Eintrags.

Folgende Maßnahmen können hierzu geeignet sein:

- Häufige, am besten tägliche Datensicherung der hinzugefügten Daten (technisch: sog. inkrementelles Backup). Vorausgesetzt ist, dass es ein vollständiges Datenbackup gab. Zu verwenden sind nicht-veränderbare Speichermedien.
- Die Datenträger müssen sicher aufbewahrt werden. Durch Backuplösungen kann jedoch die vom Gesetzgeber beabsichtigte Manipulationssicherheit nicht vollständig erreicht werden, da Änderungen zwischen zwei Sicherungen nicht erfasst werden.
- Integritätssicherung der innerhalb eines Tages hinzugefügten Daten mit einer qualifizierten elektronischen Signatur oder einem qualifizierten elektronischen Zeitstempel Der Vorteil dieses Verfahrens ist, dass die tägliche Datensicherung auch mit Speichermedien, die eine nachträgliche Veränderung zulassen (Festplatte, Band, externer Dienstleister), erfolgen kann. Wird ein qualifizierter Zeitstempel verwendet, kann außerdem der Zeitpunkt, zu dem die Daten vorgelegen haben, zweifelsfrei nachgewiesen werden. Das Problem der fehlenden Lückenlosigkeit zwischen den Sicherungen besteht aber weiterhin.

Durch die zuvor aufgeführten Maßnahmen wird keine lückenlose bzw. rechtssichere Dokumentation gewährleistet. Aus diesem Grund können weitere Maßnahmen ergriffen werden. Hierbei wird zugrunde gelegt, dass nachträgliche Änderungen der Patientenakte in der Regel nicht sehr häufig vorkommen.

Erkundigen Sie sich bei Ihrem Dienstleister über verfügbare Produkte und den Umfang der angebotenen Lösungen.

Für die rechtssichere langfristige Erstellung elektronischer Dokumente müssen insbesondere die Vorgaben der eIDAS Verordnung und des Vertrauensdienstegesetz (VDG) beachtet werden. Dies können PVS- oder Archivsoftware-Hersteller z. B. durch die Umsetzung der Technischen Richtlinie BSI-TR-03125 [7] („Beweiswerterhaltung kryptographisch signierter Dokumente", BSI-TR-ESOR) sicherstellen. Die PVS- oder Archivsoftware-Hersteller sollten Aussagen dazu treffen können, wie ihre Softwareprodukte die rechtssichere langfristige Archivierung sicherstellen und welche Zertifizierungen die Softwarelösung vorweisen kann.

12 Ersetzendes Scannen

Sollen einkommende Papierdokumente (z. B. Arztbriefe von Kollegen) eingescannt werden, um diese elektronisch zu verwalten und das Original zu vernichten, wird dieser Vorgang als „Ersetzendes Scannen" bezeichnet. Aus technischer Sicht empfiehlt die Richtlinie BSI-TR-03138 [6] (BSI-TR-RESISCAN) des BSI

technische Maßnahmen für das Ersetzende Scannen. Diese Richtlinie beschreibt, welche Maßnahmen durchgeführt werden müssen, damit der Beweiswert des elektronisch erfassten Dokuments (Scanprodukt) möglichst nah an den des Originaldokuments angenähert wird. Zitat aus der Richtlinie: „Ziel ist es, die mit einer Vernichtung des Originaldokuments stets einhergehende Verringerung des Beweiswerts für den jeweiligen Anwender durch einen an das Original möglichst weit angenäherten Beweiswert des – in einem nachweisbar ordnungsgemäßen Prozess erstellten – Scanproduktes selbst auszugleichen, zu minimieren oder sichtbar zu machen."

Hinweis: Die Technische Richtlinie [6] des BSI definiert das Ersetzende Scannen als den „Vorgang des elektronischen Erfassens von Papierdokumenten mit dem Ziel der elektronischen Weiterverarbeitung und Aufbewahrung des hierbei entstehenden elektronischen Abbildes (Scanprodukt) und der späteren Vernichtung des papiergebundenen Originals".

Die rechtliche Anwendbarkeit der Technischen Richtlinie [6] für die ärztliche Dokumentation in der Patientenakte ist nach Ansicht des BSI gegenwärtig nur für Röntgenbilder und diesbezügliche Aufzeichnungen ausdrücklich geregelt. Für sonstige Papierdokumente der Patientenakte existiert keine gesetzliche Bestimmung, die es gestattet oder verbietet, die Originaldokumente nach dem Scannen zu vernichten (Anlage R, Abschnitt R.1.2.4, S. 21 der Technischen Richtlinie). Ärzte, die beabsichtigen, Papierdokumente nach der Digitalisierung zu vernichten, müssen diese unklare Rechtslage berücksichtigen und sich ggfs. beraten lassen. Wird ein sehr hoher Beweiswert der Scanprodukte angestrebt, wären die „zusätzlichen Maßnahmen bei sehr hohen Integritätsanforderungen" der Richtlinie zu berücksichtigen (Gliederungspunkt 4.3.3 der Technischen Richtlinie).

Etwas differenzierter sind die von TR-RESISCAN empfohlenen Maßnahmen zur Vertraulichkeit und Verfügbarkeit zu betrachten. Die Richtlinie trifft hierzu unter anderem folgende Aussage: „Die Vertraulichkeitsanforderungen haben keinen Einfluss auf den Beweiswert des Scanprodukts"[5]. Gescannte Dokumente werden Teil der elektronischen Dokumentation in der Praxis. Zur Sicherstellung der Vertraulichkeit und Verfügbarkeit wird daher die Einhaltung derselben Maßnahmen empfohlen, die auch sonst für die elektronische Dokumentation in der Praxis vorgesehen sind und in der vorliegenden Technischen Anlage beschrieben sind.

13 Umgang mit externen Speichermedien

Es gibt zunehmend Angebote der Industrie für elektronische Patientenakten auf externen Speichermedien (z. B. USB-Sticks). Diese sollen – nach der Vorstellung der Industrieanbieter – in der Praxis angeschlossen werden, um Daten auszulesen oder neue Daten darauf zu speichern. Von außen ist nicht erkennbar, ob sich auf externen Speichermedien Schadsoftware befindet, die – sogar durch bloßes Stecken – den Rechner des Arztes infizieren und z. B. Patientendaten löschen, manipulieren oder stehlen kann.

Auch wenn einige externe Speichermedien spezielle Sicherheitsmechanismen gegen Schadsoftware implementieren, kann in der Regel ein sicheres externes Speichermedium eines renommierten Anbieters nicht von einer Fälschung unterschieden werden.

Die Nutzung eines fremden externen Speichermediums ist einer Kommunikation mit einem unsicheren externen Netz (Internet) gleichzusetzen. Es gelten demnach die gleichen Voraussetzungen, wie für die Anbindung eines Praxisrechners an ein unsicheres Netz (Internet).

Fremde Speichermedien dürfen nicht direkt mit einem Patientendaten führenden System verbunden werden. Die Nutzung fremder Speichermedien darf nur an einem Rechner oder einer speziellen Hardwarekomponente geschehen, welche speziell im Voraus gehärtet wurde und Sicherheitsmechanismen zur Abwehr von Angriffen implementiert. Ein Mindestmaß an Sicherheit bietet zudem die regelmäßige Aktualisierung des Betriebssystems mit Updates in Kombination mit einer aktuellen Anti-Viren-Software.

14 Maßnahmen bei Einsatz von Chipkarten-Terminals und Konnektoren

Für das Einlesen der elektronischen Gesundheitskarte werden unter anderem Chipkarten-Terminals und im Zusammenspiel mit der TI so genannte Konnektoren eingesetzt. Es dürfen nur von der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) zugelassene Komponenten verwendet werden. Die Kartenterminals und Konnektoren können teilweise auch für die Erstellung und Prüfung von qualifizierten elektronischen Signaturen sowie für weitere Anwendungen, bspw. im sicheren Netz der KVen (SNK), eingesetzt werden. Die Empfehlungen und Auflagen der Hersteller der jeweiligen Produkte sollten für den sicheren Einsatz in der Praxis berücksichtigt werden. Vor der Beschaffung der notwendigen Komponenten sind neben der Zulassung der gematik auch der Funktionsumfang der Komponenten und die Art der Zulassung zu beachten. Die Zulassung eines Gerätes z. B. für den Online Produktivbetrieb (OPB) bedeutet nicht automatisch, dass es den Funktionsumfang und die Zulassung für eine spätere Stufe beinhaltet. Im Zweifel gibt die gematik Auskunft über den notwendigen Funktionsumfang, unterschiedliche Releases und entsprechend zugelassene Komponenten.

15 Weiterführende Hinweise

Die Kassenärztliche Bundesvereinigung bietet auf ihrer Internetseite eine einfache anonyme Selbsteinschätzung bezüglich der Informationssicherheit der Praxis unter „Mein PraxisCheck Informationssicherheit" http://www.kbv.de/html/6485.php an.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet eine Internetpräsenz mit aktuellen Sicherheitshinweisen und allgemeinen Empfehlungen für die Informationssicherheit unter https://www.bsi-fuer-buerger.de an.

Das BSI und der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (bitkom) bieten unter https://www.allianz-fuer-cybersicherheit.de aktuelle und valide Informationen zu Gefährdungen im Cyber-Raum.

Die oder der Bundesbeauftragte für Datenschutz und Informationsfreiheit veröffentlicht unter https://www.bfdi.bund.de Informationen zur Datenschutzgrundverordnung, Kurzpapiere zur Interpretation des neuen Datenschutzrechts, sowie weitere Arbeits-

[6] Zitat aus BSI-TR-RESISCAN Anlage R Kap. R.1.2.4 Tab. 8 Fußnote 26

Deutsches Ärzteblatt | 22.06.2018 | DOI: 10.3238/arztebl.2018.ds_ta01

hilfen wie Muster zum Verzeichnis der Verarbeitungstätigkeiten. Die Landesbeauftragten für Datenschutz und Informationsfreiheit bieten auf ihren Internetseiten ähnliche Informationen (und ggf. landesdatenschutzspezifische Besonderheiten) an.

Die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) gibt Auskunft über Datenschutz und Informationssicherheit in der Telematikinfrastruktur (TI) https://www.gematik.de. Dies umfasst auch die dezentralen Komponenten wie elektronische Gesundheitskarte (eGK), den elektronischen Heilberufsausweis (HBA), den „Praxisausweis" (SMC-B) sowie den Konnektor und Kartenlesegeräte.

16 Literaturverzeichnis

1. Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Bundesärztekammer/ Kassenärztliche Bundesvereinigung; 2018
2. Leitfaden IT-Sicherheit, Bundesamt für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.html, Stand: 17.02.2012
3. Richtlinie der Kassenärztlichen Vereinigungen „Sicheres Netz der KVen – KV-SafeNet", V3.2, Stand: 31. 7. 2015
4. Technische Richtlinie des BSI , BSI-TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html, Stand: 22.01.2018
5. IT-Grundschutz-Kompendium, Bundesamt für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html, Stand 2018
6. Technische Richtlinie des BSI , BSI-TR-03138 Ersetzendes Scannen (RESISCAN), https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03138/index_htm.html, Stand: 02.03.2017
7. Technische Richtlinie des BSI , BSI-TR-03125 Beweiswerterhaltung kryptographisch signierter Dokumente; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_V1_2_1.pdf?__blob=publicationFile&v=2, Stand: 27.02.2018
8. Technische Richtlinie des BSI , BSI TR-03116–1 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 1: Telematikinfrastruktur, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03116/index_htm.html, Stand: 2015

17 Glossar

Advanced Encryption Standard (AES)
Bei AES handelt es sich um einen symmetrischen Verschlüsselungsalgorithmus, welcher in vielen Produkten als Standard integriert ist. Er gilt momentan als sicher, falls die Schlüssellänge ausreichend lang gewählt wird und ein sicheres Padding-Verfahren verwendet wird.

Backdoors
Hierbei handelt es sich um nicht dokumentierte (Administrations-) Zugänge in einer Software.

BSI
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist der zentrale IT-Sicherheitsdienstleister des Bundes. Das BSI untersucht und bewertet bestehende Sicherheitsrisiken und schätzt die Auswirkungen neuer Entwicklungen ab. Auf dieser Grundlage bietet es Dienstleistungen in den vier Kernbereichen Information, Beratung, Entwicklung und Zertifizierung an.

DMZ
Eine DMZ bezeichnet ein Netzwerksegment, das zwischen dem ungesicherten Netz (z. B. dem Internet) und dem vertrauenswürdigen lokalen Netz durch Firewalls abgetrennt ist. Dies ermöglicht zum Einen sicherheitstechnisch kontrollierte Zugriffmöglichkeiten auf interne Ressource auf die daran angeschlossenen Server, zum anderen schützt es das lokale Netz vor unberechtigten Zugriffen.

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

Gesundheitsnetz
In dieser Technischen Anlage wird unter einem Gesundheitsnetz ein Netz für das Gesundheitswesens verstanden, das auf Internettechnologie aufbaut, aber logisch vom Internet getrennt, und somit sicherer als dieses ist.

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.

SIS – Sicherer Internetservice
Ein durch eine Application-Level-Gateway-Paketfilter-Struktur geschützter Zugang zum Internet. Ein Mehrwertdienst, der von einigen VPN-Zugangsdienstanbietern bereitgestellt wird.

Voice over IP (VoIP)
Unter Voice over IP (VoIP) versteht man das Telefonieren über Computernetzwerke, die auf den Internet-Standards aufbauen.

VPN
Mit VPN wird ein virtuelles privates Kommunikationsnetz bezeichnet. Dabei verwendet ein VPN ein bestehendes physisches Kommunikationsnetz wie das Internet, etabliert aber durch das VPN-Protokoll ein verschlüsseltes Netz.

Wireless-Local Area-Network (WLAN)
Drahtlose lokale Netze die auf Standards der IEEE-802.11-Familie aufsetzen sind Wireless-Local-Area-Network (WLAN).