

# Datenschutz in der Praxis

## Sicherheit der IT in medizinischen Versorgungszentren

Evren Eren

Der steigende Bedarf sowie zunehmende intersektorale Versorgungsstrukturen stellen neue Ansprüche an Organisation und Sicherheit der Informationstechnik (IT) in Krankenhäusern und medizinischen Versorgungszentren (MVZ). Während aber Krankenhäuser über einen relativ hohen IT-Standard verfügen, hinken die meisten MVZ dem State of the Art teilweise weit hinterher. Fortschrittliche MVZ sind bestrebt, ihre Arbeitsabläufe durch IT zu unterstützen, und vernetzen sich zunehmend mit Krankenhäusern, anderen MVZ und teilweise auch Arztpraxen. Hier bedingt der Schutzbedarf von Informationen, insbesondere patientenbezogener Daten, eine nachhaltige Absicherung von Systemen und den Aufbau notwendiger IT-Infrastrukturen.

Im Gesundheitswesen ist eine qualitätsgesicherte Verfügbarkeit und Verarbeitung von Informationen essenziell, nicht zuletzt durch die stetig zunehmende Digitalisierung. Der Einsatz von IT wird heute vorrangig durch die gesetzlichen und betrieblichen Notwendigkeiten bestimmt. Innovative MVZ ersetzen ihre alten Systeme durch neue und effiziente. Das Gros hat jedoch veraltete Systeme im Einsatz und kann kaum noch die gesetzlichen Auflagen erfüllen. Insbesondere in puncto Sicherheit besteht ein immenser Nachholbedarf. Aber auch die „Early Adopter“ sollten IT-Sicherheitsstrukturen nicht nebenläufig in Eigenregie einführen. Eine nachhaltige Umsetzung muss eigenverantwortlich und rechtlich vertreten werden können. Dabei sollte klar zwischen technischer und organisatorischer IT-Sicherheit differenziert werden, wobei beide Welten aufeinander genau abgestimmt sein müssen.

### Technische IT-Sicherheit

Für die technische IT-Sicherheit, die vorrangig der Stabilität der Operativsysteme und dem Schutz der betrieblichen Daten vor Verlust, Datenspionage oder Sabotage dient, sind die für die Sicherheit bekannten Faktoren Vertraulichkeit, Authentizität, Integrität und Verfügbarkeit ausschlaggebend. Hierzu werden konventionelle Verfahren und Methoden wie elektronische Signatur, Verschlüsselung, Authentifizierung und Autorisierung angewandt. In MVZ ergeben sich im Wesentlichen folgende Schwachstellen:

#### *Kommunikation intern und extern*

Bei der Netzsicherheit sollte zwischen intern und extern unterschieden werden. Auch die Größe des Netzes, die darin enthaltenen Rechnersysteme und somit auch deren Anwendungen sind entscheidend. Das Netz ist Träger

und Medium von Systemen und Anwendungen und erlaubt die Verteilung von Daten sowie die Kommunikation innerhalb sowie mit anderen Netzen oder Systemen.

Ein großes internes Netz sollte je nach Dimension und Struktur in Teilnetze fragmentiert und voneinander getrennt und kontrolliert betrieben werden. Eine Trennung kann physisch, aber auch logisch erfolgen: Erstere mit Hilfe von Netzkomponenten (Switches, Router usw.), Letztere mittels VLAN-Switches. Einfach ausgedrückt lautet die zentrale Fragestellung: „Wer oder was darf was, womit und wofür?“ Dies betrifft Anwender, Anwendungen und Systeme gleichermaßen. Beispielsweise sollten Praxis-PCs physisch keine sicherheitskritischen Daten enthalten, wenn sie auch eine Verbindung zum Internet haben. PCs oder Notebooks sollten in der Regel komplett vom Praxisnetz getrennt sein. Falls das nicht möglich ist, müssen auf ihnen sicherheitskritische Daten unbedingt verschlüsselt werden.

MVZ kommunizieren typischerweise mit Arztpraxen, anderen MVZ und Krankenhäusern. In der Regel werden dabei Befunde und Gutachten, also patientenrelevante Daten, ausgetauscht. Während dabei oft noch per Fax kommuniziert wird, haben einige MVZ bereits auf E-Mail-Transfer umgestellt. Aufgrund der Vertraulichkeit der Informationen sollte dieser aber größtenteils verschlüsselt erfolgen.

Einige MVZ setzen zur Vernetzung virtuelle private Netze (VPN) oder einfache Tunnel ein und erweitern damit das interne Netz (Intranet). In diesem Zusammenhang sollten die Aspekte Verfügbarkeit, Skalierbarkeit, Quality of Service, Netzmanagement sowie Migrationsfähigkeit Beachtung finden.

#### *Dokumentation und Sicherung*

Ein MVZ stellt vielfältige Anforderungen an die Dokumentation von Vor-

gängen, das Speichern von Informationen unterschiedlichster Art und in diversen Formaten, die sowohl zentral, aber auch verteilt und fragmentiert vorliegen können und kommuniziert werden müssen. Dabei ist eine Absicherung durch Verschlüsselung, Authentizität sowie Integritätsprüfung wichtig. Datenintegrität ist ein essenzieller Punkt in der Informationssicherheit, da Veränderung und Manipulation nachvollziehbar sein müssen. Die Sicherheitsrisiken für digitale Archive werden derzeit noch wenig beachtet. Nachlässigkeit oder aber Datendiebstahl, Missbrauch von Zugangsrechten sind unterschätzte Gefahren. IT-Sicherheitskonzepte sollten dieses Thema als integralen Bestandteil der Security Policy aufnehmen. Sensible Daten müssen mittels geeigneter Programme vor Verlust gesichert werden. Dies erfordert einen regelmäßigen und automatisierten Backup. Selbstverständlich sollten Backups auch regelmäßig verifiziert werden. Die Verifikation enthält dabei den Vergleich und die Prüfung der Daten sowie ihr erfolgreiches Zurückspielen. Die „Technische Richtlinie zur vertrauenswürdigen Langzeitspeicherung (TR-VELS)“ des BSI ist hierfür eine gute Orientierung.

### *Sicherheit und Schutz von Daten und Systemen*

In medizinischen IT-Systemen und -Anwendungen existieren Standards, die bereits Sicherheitsfunktionen implementieren. Hierzu zählen z.B. HL7 und Dicom (siehe *Textkasten*).

Die Verschlüsselung von sensiblen bzw. sicherheitskritischen Daten wie Patienten-, Abrechnungs- und Sozialdaten ist unabdingbar, um ihren Missbrauch ausschließen zu können. Zudem müssen Patientendaten oder andere vertrauliche Informationen vom System generell vor Einsichtnahme, Kopie und Übermittlung geschützt werden. Entsprechende Authentifizierungs- und Autorisierungsmechanismen müssen sie vor unberechtigtem Zugriff schützen.

Die Zugriffslogik kann variieren. In der Regel hat das behandelnde Personal Zugriff auf die Patientendaten. Dies ist die klassische behandlungs- bzw. pati-

entenbezogene Logik mit entsprechend hohem organisatorischen Aufwand, weshalb aus pragmatischen Gründen z.B. in Krankenhäusern zu meist mit Gruppen-Accounts je Station gearbeitet wird. Berechtigungsstrukturen mit Zugriffen je behandelndem Personal lassen sich dabei natürlich nicht abbilden. Eigentlich sollte der Zugriff nur auf Daten gestattet sein, die zur Erfüllung des Behandlungsauftrags notwendig sind. Gruppen-Accounts haben den Nachteil, dass die Zugriffsregelung nicht mehr funktioniert, wenn Personal rotiert oder ausscheidet. Dieser hohe administrative Aufwand ist nicht praktikabel. Außerdem ist eine Befristung von einzelnen Zugriffsrechten nicht möglich. Eine Zugriffslogik mit stärkerer Bindung an den Behandlungspfad bzw. -kontext ist sinnvoll, jedoch ohne ein komplettes Ablösen der beschriebe-

### **HL7 und Dicom**

Der *HL7-Standard* (High Level 7) dient dem Datenaustausch rund um Patienteninformationen, Leistungen und Befunde. Obgleich er *der* Standard für die Kommunikation ist, ist sein Einsatz inhomogen, z.B. wird er kaum von niedergelassenen Ärzten genutzt. Befunde aus Krankenhäusern liegen damit nicht elektronisch vor. Solche Medienbrüche führen unweigerlich zu Sicherheitslücken. Da im HL7-Standard Sicherheitsfunktionen implementiert sind, können z.B. Nachrichten per S/MIME abgesichert oder als Klartext über TLS (SSL) übertragen werden. Es wird jedoch lediglich die Nachrichtenauthentizität berücksichtigt.

*Dicom* (Digital Imaging and Communication in Medicine) ist ein Datenformat, das sich international als Standard für die Übermittlung von medizinischem Bildmaterial etabliert hat. Die Datensicherheit wird hierbei durch drei Sicherheitserweiterungen gewährleistet: Absicherung der Kommunikation per TLS, Verschlüsselung einzelner Datenfelder zur Sicherung der Vertraulichkeit von Patientenidentifikationsdaten sowie ein proprietäres Signaturdatenformat.

nen rollenbasierten bzw. stations-/abteilungsbezogenen durch die behandlungs-/patientenorientierte Logik. In diesem Kontext ermöglicht die elektronische Fallakte die diagnosebezogene Kommunikation von Daten zwischen Gesundheitsdienstleistern. Mit ihr sind Sicherheitsmechanismen wie Pseudonymisierung, Berechtigungsmanagement und Verschlüsselung sowie Einflussnahme des Patienten für die Autorisierung zur Einsichtnahme und Verarbeitung möglich, die den Auflagen des Datenschutzes genügen können. So können Behandlungsdokumente in Praxisverwaltungssoftware (PVS) und Krankenhausinformationssystemen (KIS) dezentral gespeichert werden. Der Patient entscheidet, wer neben dem behandelnden Arzt zusätzlich Zugriff auf seine Daten haben darf. Bei der Fallakte wird kein Vollzugriff gewährt. Es werden nur die für den Behandlungsfall notwendigen Daten freigegeben. Auf intersektoralen Behandlungspfaden ließe sich über rollenbasierte Strukturen eine Logik abbilden, welche an einer Behandlung beteiligte Instanz was sehen „darf“ und „kann“.

### *Elektronische Signatur*

In der medizinischen Dokumentation spielt die elektronische Signatur eine wichtige Rolle. Mittlerweile existieren einige Lösungen für die langfristige elektronische Archivierung elektronisch signierter Dokumente. Signierte Dokumente werden mit zusätzlichen Parametern wie Zertifikat und Zeitstempel versehen, die eine Überprüfung des Dokumentes oder der Signatur erlauben. Es wird empfohlen, die sog. qualifizierte elektronische Signatur einzusetzen, die von einem Zertifizierungsdienst ausgestellt wird. Dies erfordert eine entsprechende PKI (Public Key Infrastructure), und i.d.R. sind Smartcards zur Signaturerstellung nötig. Elektronische Arztbriefe, die als Textdokumente vorliegen, können so in ein pdf-Dokument konvertiert und elektronisch signiert werden.

Während der Zugriff auf eine Papierakte einfach geregelt ist, stellt ihr elektronisches Pendant erhebliche Anforderungen an die Zugriffsregelung. Sie existiert in der Regel nicht mehr

einfach und ist durch elektronische Vervielfältigung (Kopie und Transport) örtlich nicht eindeutig. Die fortschreitende Entwicklung zur integrierten und systemübergreifenden Patientenakte verstärkt die Risiken hinsichtlich des Datenschutzes. Die ärztliche Dokumentationspflicht stellt durch die Digitalisierung der konventionellen Karteikarte bzw. Patientenakte hohe Anforderungen an die Sicherung sowohl in technischer als auch organisatorischer Hinsicht. Denn elektronische Dokumente müssen so wie ihre papierbasierten Pendant mit Änderungen und Ergänzungen ihren rechtlichen Beweiswert beibehalten. Das Überprüfen von Änderungen sowie die Integrität sind nur mit einem wesentlich höheren technischen Aufwand möglich. Die „qualifizierte elektronische Signatur“ sowie die Zeitstempelung im Dokument sind hier maßgebende Mechanismen. Die qualifizierte Signatur ist vom Gesetzgeber der Schriftform gleichgestellt und bietet eine rechtliche Sicherheit. Als Steigerung der fortgeschrittenen elektronischen Signatur wird sie durch qualifizierte Zertifizierungsdienste vergeben und verwaltet. Vergabeverfahren, Zertifikatverzeichnis sowie Zeitstempel sind Merkmale, die eine hohe Sicherheit zur Integrität und Authentizität abbilden. Die Beweissicherheit ist von großer Bedeutung.

## Organisatorische Sicherheit

Um IT-Sicherheitsmaßnahmen wirkungsvoll umsetzen zu können, muss im MVZ nicht nur eine IT-Sicherheitskultur aufgebaut, sondern auch ein IT-Sicherheitsbewusstsein nachhaltig gelebt werden. Die Mitarbeiter spielen dabei eine wichtige Rolle. Viele Statistiken über Sicherheitsvorfälle belegen, dass Mitarbeiter das größte Risiko für die IT-Sicherheit darstellen und die meisten Sicherheitsvorfälle durch unsachgemäßes Verhalten verursacht werden. Aus diesem Grunde sind ausreichende IT-Sicherheitskenntnisse unabdingbar, damit Anomalien, die auf Angriffe hindeuten können, sowie Zwischenfälle rechtzeitig erkannt werden. Sensibilisierung durch Schulungen und Veranstaltungen sind die Ba-

sis zur eigenverantwortlichen Umsetzung von Maßnahmen. Hier müssen die Grundprinzipien der IT-Sicherheit, Maßnahmen zur Gefahrenerkennung, die Risikoeinschätzung sowie die Definition von IT-Sicherheitsrichtlinien behandelt werden.

### IT-Sicherheitsmanagement

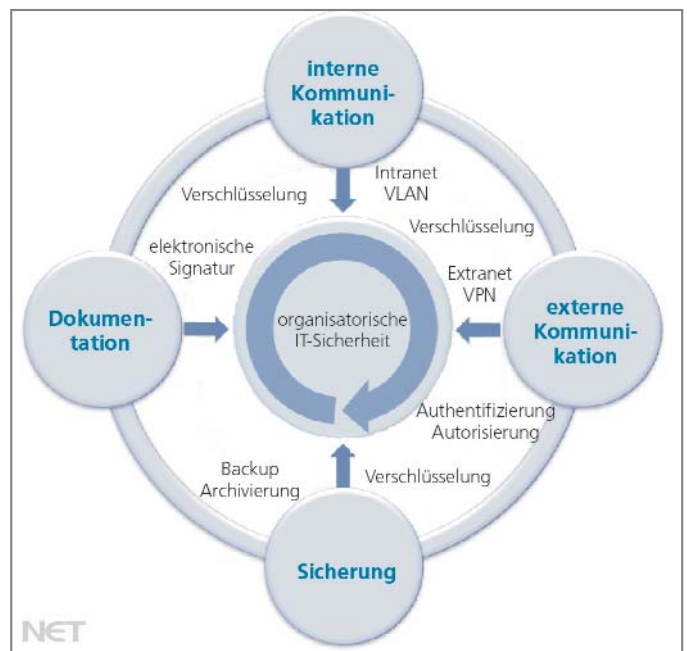
IT-Sicherheitsmanagement erfordert Ressourcen und produziert Kosten. Doch die Budgets für die IT-Sicherheit sind knapp bemessen oder fehlen gar, obgleich Dienstleister, Hersteller und Organisationen aus dem Life-Science- und Gesundheitssektor unisono die Notwendigkeit betonen, dass sensible Daten adäquat geschützt werden müssen. Es verwundert auch nicht, dass es als Behinderung der Geschäftsprozesse angesehen wird. Oft gehen Einrichtungen wie z.B. Krankenhäuser jedoch einen individuellen Weg und folgen selten Standards. Auch wenn die Zertifizierung von IT-Sicherheit nicht verpflichtend ist, dient sie der Nachweisbarkeit eines geprüften Sicherheitsniveaus gegenüber Dritten. Durch die Zertifizierung von Workflows und Geschäftsprozessen ist ein effektiver Schutz gegen persönliche Haftung und Organisationsverschulden gegeben.

Gesetzliche Vorschriften zum Schutz personenbezogener Daten und der entsprechenden IT bzw. Telematik zur Unterstützung der Geschäftsprozesse erfordern den Einsatz von IT-Sicherheitskonzepten entlang von hierzu geeigneten Standards wie z.B. ISO 27001. Viele Verantwortliche sind sich der Risiken nicht ausreichend bewusst. Störungen und Ausfälle werden kaum beachtet. Allein bei der Speicherung von sensiblen Informationen sollten Geschäftsführer bedenken, dass sie nach dem Gesetz persönlich haften

müssen, wenn ihre IT nicht ausreichend abgesichert ist.

## Fazit

Ein angemessenes IT-Sicherheitsniveau kann nur durch geplantes und organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Sicherheitsmaßnahmen sind nicht nur eine technische Aufgabe, sondern auch eine organisatorische



Prinzipielle Aufgabenverteilung durch ein IT-Managementsystem

Herausforderung. Durch eine gute Verzahnung dieser beiden Bereiche ist eine erfolgreiche Umsetzung gegeben. Unter Beachtung entsprechender Verordnungen und Gesetze sollte eine systematische Vorgehensweise und Umsetzung nach Standards durch Sensibilisierung und Awareness-Bildung flankiert werden.

Das Einrichten und Aufrechterhalten eines angemessenen IT-Sicherheitsstandards in MVZ ist aufgrund der stetig steigenden Komplexität von IT-Anwendungen und -Infrastrukturen kein einfaches Unterfangen. Geeignete und standardisierte Konzepte und Maßnahmen müssen in die Prozesse der Organisation verankert werden. Selbstverständlich bindet dies Ressourcen und Kosten fallen an. Jedoch zahlt sich eine Investition in ein IT-Sicherheitsmanagement langfristig durch eine höhere Produktivität und Bonität des MVZ aus. (bk)