IT-Sicherheits-Richtlinie

FB_5_3020

Präambel

Dieses Dokument ergänzt die Leitlinie Informationssicherheit [QM: FB_5_5002] um organisatorische und technische Richtlinien.

Inhalt

IT-Sicherheits-Richtlinie
FB_5_3020

Abkürzungen

kDL	Kritische Dienstleistung
B3S	Branchenspezifischer Sicherheitsstandard
EU-DSGVO	Datenschutzgrundverordnung der Europäischen Union
IT-SiG	IT-Sicherheitsgesetz

Organisatorische Richtlinien

Überblick

Der Einsatz der Informationsverarbeitung ist von entscheidender Bedeutung für die Handlungsfähigkeit des Klinikums geworden. Ziel der vorliegenden IT-Sicherheitsrichtlinie ist die Gewährleistung des ordnungsgemäßen und sicheren IT-Einsatzes in allen IT-gestützten Verfahren des Klinikums. Dies umfasst auch die Erfüllung der datenschutzrechtlichen Anforderungen im Sinne von Datensicherheit und Datenschutz. Die IT-Sicherheit wird vom Vorstand des Klinikums als gleichrangiges Ziel neben den Zielen Erhöhung der Patientenorientierung, Steigerung der Effizienz und Verbesserung der Arbeitsbedingungen erachtet. Sach- und zeitgerechter Aufgabenerfüllung ist grundsätzlich Vorrang einzuräumen, jedoch dürfen diese Entscheidungen nicht zu Sicherheitsmängeln führen. Der Vorstand des Klinikums fordert daher die Orientierung des Handelns der Mitarbeiter und Mitarbeiterinnen aller Ebenen an den nachstehenden Zielen:

- Sicherstellung des hohen Ansehens unseres Klinikums in der Öffentlichkeit durch rechtzeitige und richtige Bedarfsdeckung sowie durch Wahrung der Integrität und Vertraulichkeit der hier gehaltenen Informationen sowie der ärztlichen Schweigepflicht,
- Sicherstellung der Kontinuität der Aufgabenerfüllung,
- Sicherstellung der Kontinuität in der Qualität der erbrachten Leistungen,
- Erhaltung der in Technik, Verfahren und Wissen investierten Werte und
- Minimierung der im Schadensfall entstehenden Kosten.

Um die gesteckten Ziele zu erreichen, wird in dieser Richtlinie ein Sicherheitsmanagement für das Klinikum festgelegt. Innerhalb dessen trägt jeder Einzelne seinen Anteil an Verantwortung und ist verpflichtet die ihn betreffenden Aufgaben sorgfältig zu erfüllen. Nur wenn alle Mitarbeiter orientiert an den Zielsetzungen vertrauensvoll und verantwortungsbewusst zusammenwirken kann die vorliegende IT-Sicherheitsrichtlinie erfolgreich umgesetzt werden.

Sicherheitspolitischer Rahmen

Das Klinikum der Universität München ist mit den Standorten Innenstadt und Großhadern eines der größten Krankenhäuser in Deutschland und Europa. Es ist eine Einrichtung der höchsten medizinischen Versorgungsstufe. Gleichzeitig ist das Klinikum im Rahmen der Medizinischen Fakultät der Universität eine wichtige und bedeutende Stätte der medizinischen Forschung und Lehre.

Im Mittelpunkt unserer Arbeit steht das Wohl der Patienten. Dies gilt gleichermaßen für unsere Aufgaben in Forschung und Lehre wie in der unmittelbaren Krankenversorgung. Durch die an unserem Klinikum geleistete Forschung, durch die Ausbildung guter Ärztinnen und Ärzte einschließlich weiterer

medizinischer Berufe, sowie durch unser Engagement bei der Behandlung der Patienten wollen wir diesen eine optimale Versorgung bieten und zusätzlich zur Verbesserung der Krankenversorgung im Allgemeinen beitragen. Dies alles stellt hohe Ansprüche an die Qualität und die Zuverlässigkeit unserer Leistungen.

Der Einsatz der Informationsverarbeitung nimmt in allen Bereichen und Tätigkeitsfeldern des Klinikums stetig zu. Sie ist somit von entscheidender Bedeutung für die Handlungsfähigkeit des Klinikums geworden. In zentral wichtigen Abläufen besteht heute schon eine unmittelbare Abhängigkeit von der Funktionsfähigkeit der Informationstechnik. Mit der eingesetzten Hard- und Software speichern wir Informationen über die Patienten unseres Klinikums und andere personenbezogene Daten. Wir werten diese innerhalb unserer Aufgaben in der Krankenversorgung, der Lehre und der Forschung aus und übermitteln auch Daten an andere Stellen. Beim Umgang mit den Informationen unterliegen wir strengen standesrechtlichen und gesetzlichen Auflagen (z. B. Ärztliches Standesrecht, EU-DSGVO, Bayer. Krankenhausgesetz, Verordnungen wie die Röntgenverordnung, Medizinproduktegesetz etc.).

Grundlegend für die Erfassung und die weitere Verwendung von Patientendaten ist die ärztliche Schweigepflicht. Sie bildet eine der Voraussetzungen für ein vertrauensvolles Verhältnis zwischen Arzt und Patient, welches für eine erfolgreiche medizinische Behandlung notwendig ist.

Die Patienten setzen voraus, dass wir mit den über sie gesammelten Informationen verantwortungsvoll umgehen und ihr Persönlichkeitsrecht schützen. Das Ansehen und die Wirkungsmöglichkeiten des Klinikums hängen in starkem Maße davon ab, dass diese Erwartungen voll erfüllt und nicht in Frage gestellt werden.

Das Klinikum stellt sich dieser Verpflichtung und strebt jederzeit ein angemessen hohes Sicherheitsniveau an.

Die gespeicherten Informationen stellen einen wesentlichen Faktor für die Tätigkeiten des Klinikums dar. Durch unberechtigte Änderungen können hohe Schäden verursacht werden. Ihre Manipulation, Zerstörung oder Preisgabe sowie die Verletzung gesetzlicher Anforderungen kann das Klinikum und seine Patienten empfindlich treffen. Bei extremer Beeinträchtigung kann sogar die geordnete Krankenversorgung zeitweise zum Erliegen kommen. Mit geeigneten Sicherheitsmaßnahmen ist diesen Bedrohungen entgegenzuwirken. Die Sicherheit der IT-Systeme ist ein Beitrag zur Erreichung der Ziele des Klinikums. Hierzu müssen nicht nur geeignete technische, sondern auch effektive organisatorische Maßnahmen ergriffen werden, wobei für die zu schützenden Informationen und IT-Systeme ein angemessenes Sicherheitsniveau anzustreben ist. Die aktive Beteiligung aller Mitarbeiter und Mitarbeiterinnen ist dabei unumgänglich.

Die Bedrohungen ändern sich permanent. Sicherheitsmaßnahmen zum Schutz der Informationsverarbeitung müssen deshalb kontinuierlich an organisatorische und technologische Veränderungen angepasst werden.

Die Sicherheitsmaßnahmen müssen technisch machbar, wirtschaftlich vertretbar und für die Benutzer der IT-Systeme zumutbar sein.

Zumutbar heißt, dass die Krankenversorgung, Lehre und Forschung nicht unangemessen eingeschränkt werden soll. Der Vorrang dieser Aufgaben darf jedoch an keiner Stelle zu Sicherheitsmängeln führen.

Zumutbarkeit setzt voraus,

- dass ein Sicherheitsbewusstsein bei jeder Mitarbeiterin und jedem Mitarbeiter aktuell vorhanden ist,
- dass IT-Sicherheitsmaßnahmen organisch in die Abläufe integriert sind und
- dass jeder Mitarbeiter im Umgang mit der Informationstechnik und den IT-Sicherheitsmaßnahmen ausreichend geschult ist.

Geltungsbereich

Die vorliegende IT-Sicherheitsrichtlinie ist verbindlich für alle Bereiche des Klinikums (Kliniken, Institute, Verwaltung). Sie ist verpflichtend für alle Betreiber und Nutzer der IT-Systeme und Informationen des Klinikums. Darunter fallen auch in Medizingeräte integrierte IT-Systeme oder IT-Systeme, die nicht an eines der lokalen Netze im Klinikum angeschlossen sind. Die IT-Sicherheitsrichtlinie besitzt bindende Wirkung für die Kommunikation mit Stellen außerhalb des Klinikums (z. B. Arztpraxen, Kliniken, Krankenkassen, Geschäftspartnern, öffentliche Stellen). Sie gilt für Planung, Realisierung und Betrieb von IT-Systemen unter dem Aspekt der IT-Sicherheit.

Ziele

Ziel der IT-Sicherheitsrichtlinie ist die Gewährleistung des ordnungsgemäßen und sicheren IT-Einsatzes in allen IT-gestützten Verfahren des Klinikums. Dies umfasst auch die Erfüllung der datenschutzrechtlichen Anforderungen im Sinne von Datensicherheit und Datenschutz. Insbesondere gilt dies für die Ärztliche Schweigepflicht. Soweit sich aufgrund der Risikoabschätzungen nicht höhere Anforderungen ergeben, orientiert sich das Klinikum am Branchenspezifischen Sicherheitsstandard Gesundheit (B3S) der im Rahmen des IT-SiG erarbeitet wurde. Mit den dort beschriebenen Abläufen, Planungen und Maßnahmen wollen wir das Risiko für IT-Infrastruktur, IT-Anwendungen und Informationen so gering als möglich halten. Damit wollen wir auch sicherstellen, dass eventuelle Ereignisse in ihrer schädigenden Auswirkung begrenzt werden können.

Der Vorstand des Klinikums fordert daher die Orientierung des Handelns der Mitarbeiter und Mitarbeiterinnen aller Ebenen an den nachstehenden Zielen:

- Sicherstellung des hohen Ansehens unseres Klinikums in der Öffentlichkeit durch rechtzeitige und richtige Bedarfsdeckung sowie durch Wahrung der Integrität und Vertraulichkeit der hier gehaltenen Informationen sowie der ärztlichen Schweigepflicht,
- Sicherstellung der Kontinuität der Aufgabenerfüllung,
- Sicherstellung der Kontinuität in der Qualität der erbrachten Leistungen,
- Erhaltung der in Technik, Verfahren und Wissen investierten Werte und
- Minimierung der im Schadensfall entstehenden Kosten.

Im Zweifel sind Verhaltensweisen unter IT-Sicherheitsaspekten zu prüfen, und von den jeweils verantwortlichen Vorgesetzten dem Vorstand des Klinikums zur Entscheidung vorzulegen.

IT-Sicherheitsmanagement

Das IT-Sicherheitsmanagement des Klinikums ist ein Dreischichtensystem von interdisziplinären Aufgaben.

Die oberste Ebene bilden die strategischen Entscheidungen. Hier ist der Vorstand des Klinikums gefordert, Risiken und Krisen zu bewältigen und Schäden für die Organisation oder Dritte zu verhindern. Das Ergebnis manifestiert sich in der Informationssicherheitsleitlinie. Sie repräsentiert den Willen des Vorstands.

Diese IT-Sicherheitspolitik mündet auf der konzeptionellen Ebene in den permanenten Prozess der IT-Sicherheitskonzeption. Dem technischen und organisatorischen Wandel entsprechend wird das IT-Sicherheitskonzept regelmäßig fortgeschrieben.

Das operative Vorgehen bildet die dritte Ebene, in der die Handlungsanleitungen des IT-Sicherheitskonzeptes, orientiert an dieser IT-Sicherheitspolitik, am Arbeitsplatz jedes einzelnen Mitarbeiters umzusetzen sind.

Zwischen den drei Ebenen besteht ein Geflecht von Verantwortlichkeiten, mit denen jeder Einzelne, orientiert an den Zielsetzungen dieser IT-Sicherheitspolitik, der Sicherheit in der Informationsverarbeitung des Klinikums angemessen Rechnung trägt. Die verteilte Verantwortung zur Gewährleistung der IT-Sicherheit erfordert das Zusammenwirken aller Beteiligten, um die gesteckten Ziele zu erreichen. Die Konkretisierung dieser Verantwortlichkeiten und Aufgaben im Bereich der IT-Sicherheit ergibt sich aus den folgenden Festlegungen:

- Dem Vorstand des Klinikums obliegt die Gesamtverantwortung. Im Rahmen des Sicherheitsmanagements obliegt ihm das Risikomanagement und das Krisenmanagement für das Klinikum. Er kennt die Risiken des IT-Einsatzes sowie das Restrisiko. Mit der Zielsetzung der Reduzierung von Risiken und der Bewältigung von Krisen erlässt er die IT-Sicherheitspolitik und überwacht regelmäßig die Erreichung der gesetzten IT-Sicherheitsziele im laufenden Betrieb des Klinikums.
- Der Datenschutzbeauftragte veranlasst die notwendigen Maßnahmen zur Einhaltung der datenschutzrechtlichen Vorschriften, er prüft deren Wirksamkeit, berichtet dem Vorstand über Schäden und Schwachstellen. Die im BayDSG ausdrücklich erwähnten Pflichtaufgaben eines Datenschutzbeauftragten sind:
    - Durchführung des datenschutzrechtlichen Freigabeverfahrens
    - Führung des Verfahrensverzeichnisses
    - Beratung der Beschäftigten
- Der Datenschutzbeauftragte des Klinikums wird von den lokalen Datenschutzbeauftragten in den Kliniken, Instituten und den Verwaltungsabteilungen des Klinikums in seinen Aufgaben unterstützt. Sie veranlassen und kontrollieren die Einhaltung der erforderlichen technischen und organisatorischen Datenschutzmaßnahmen in ihrem Bereich und sie sind die lokalen Ansprechpartner für den Datenschutz.
- Der Informationssicherheitsbeauftragte des Klinikums ist Ansprechpartner in Sachen IT-Sicherheit. Er koordiniert die Umsetzung der IT-Sicherheitspolitik in der Zusammenarbeit mit den Fachabteilungen der MIT sowie mit den lokalen EDV- und Datenschutzbeauftragten. Zu diesen Aufgaben gehören die Einschätzung der Risiken sowie die Erstellung und die Fortschreibung des ISMS. Über den Sicherheitsstatus und die Schwachstellen berichtet er an den Abteilungsleiter der MIT und den Vorstand.

- Jeder Vorgesetzte (Klinik- bzw. Institutsvorstand, Abteilungsleiter) ist namentlicher Verfahrensverantwortlicher in seinem Bereich. Dies umfasst die Verantwortung für die ordnungsgemäße Aufgabenerfüllung, sowie den sorgsamen Umgang mit Informationen unabhängig davon, ob es sich um ein manuelles, technisches oder IT-gestütztes Verfahren handelt. Bei IT-gestützten Verfahren bezieht sich diese Verantwortlichkeit nicht nur auf Aufgabenerfüllung und Informationen, sondern auch auf Kommunikationsbeziehungen und -inhalte. Jeder Vorgesetzte ist verpflichtet, den Schutzbedarf der IT-Anwendungen und Informationen und die mit dem IT-Einsatz verbundenen Risiken abzuschätzen und entscheidet über die erforderlichen Sicherheitsanforderungen sowie die notwendigen Rechte an Informationen und Prozessen. Er trägt dafür Sorge, die IT-Sicherheit in die Aufgaben und Prozesse seines Fachbereiches zu integrieren. Er sorgt für die Anwendung, Angemessenheit, Aktualität und Kontrolle der Sicherheitsmaßnahmen. Er motiviert seine Mitarbeiter für die Einhaltung der Maßnahmen und die Zielsetzungen der IT-Sicherheitspolitik. Er fördert Vorschläge zur Verbesserung der IT-Sicherheit und gibt diese über den lokalen EDV-Beauftragten an den Informationssicherheitsbeauftragten der MIT weiter.
- Die lokalen EDV-Beauftragten sind im Auftrag ihres Vorgesetzten (Klinik- bzw. Institutsvorstand, Abteilungsleiter) die primären Ansprechpartner für alle den jeweiligen Bereich betreffenden DV-Fragen. Als Ansprechpartner zu allen Fragen der lokalen DV-Organisation sind sie auch für eine systematische Sicherheitsadministration und Sicherheitsrevision zuständig. Sie registrieren die lokalen Verletzungen der IT-Sicherheitsziele, ermitteln die Risiken, die sich aus einer sicherheitsrelevanten Entscheidung bei der IT-Planung oder aus einer Handlung oder Unterlassung beim IT-Einsatz ergeben und melden diese ihrem Vorgesetzten und dem Informationssicherheitsbeauftragten. Dies gilt insbesondere bei der Öffnung von IT-Systemen nach außen. Die EDV-Beauftragten motivieren die Mitarbeiter ihres Bereichs für das Einhalten der IT-Sicherheitsmaßnahmen und veranlassen die notwendigen Schulungen.
- Jeder Betreiber von IT-Systemen gilt als verantwortlicher Verfahrens- und Informationstreuhänder für die ihm anvertrauten Informationssysteme. Er ist verantwortlich für die Festlegung und Umsetzung der notwendigen Schutzmaßnahmen seines IT-Systems. Diese müssen den von den Verfahrensverantwortlichen (Klinik- bzw. Institutsvorstand, Abteilungsleiter) vorgegebenen Sicherheitsanforderungen entsprechen. Aus dieser Verantwortung ergibt sich die Verpflichtung, den lokalen EDV-Beauftragten sowie die Verfahrensverantwortlichen über Risiken zu informieren, die sich aus einer sicherheitsrelevanten Entscheidung bei der IT-Planung oder aus einer Handlung oder Unterlassung beim IT-Einsatz ergeben. Er dokumentiert die Einrichtung der vorgesehenen Maßnahmen und führt Buch über deren Anwendung. Diese Dokumentation ist Element der Sicherheitsadministration und Basis für die Sicherheitsrevision. Er ist in besonderem Maße gefordert, sein eigenes Handeln oder Unterlassen am Schutzbedarf seines IT-Systems und an der Maßgabe dieser IT-Sicherheitspolitik zu orientieren.
- Jeder einzelne Mitarbeiter ist den mit seinem Vorgesetzten erarbeiteten Sicherheitsanforderungen sowie zur Einhaltung der IT-Sicherheitsregeln dieser IT-Sicherheitspolitik verpflichtet. Für die richtige Anwendung der Sicherheitsmaßnahmen an seinem Arbeitsplatz ist er selbst verantwortlich. Erkannte Sicherheitsmängel sind sofort an den lokalen EDV-Beauftragten zu melden. Über Verletzungen des IT-Sicherheitsstandards, sowie über mögliche Verbesserungen der IT-Sicherheit informiert der Mitarbeiter umgehend den lokalen EDV-Beauftragten. Wir erwarten von jedem Mitarbeiter, dass er sein Verhalten an den Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit der Informationen orientiert und legen in seine Verantwortung, dass er
    - Informationen und Funktionen nur zum bestimmungsgemäßen Gebrauch einsetzt,

  - Informationen und Funktionen nur bestimmungsgemäß erzeugt oder verändert,
  - Informationen und Funktionen gegen Missbrauch schützt und nur bestimmungsgemäß zugänglich macht oder weitergibt,
  - mit den ihm anvertrauten Ressourcen verantwortungsbewusst umgeht und
  - auch über den eigenen Arbeitsplatz hinaus für den ordnungsgemäßen IT-Einsatz Sorge trägt.
- Wir wollen nach dem Grundsatz der lernenden Organisation einen stetigen Prozess der Qualitätsverbesserung leben. Neben dem Erwerb fachlicher Kompetenz ist dazu auch der Aufbau von IT-Kompetenz bei jedem Mitarbeiter erforderlich. Wir gestehen jedem Mitarbeiter zu, ohne Furcht vor negativen Sanktionen Fehler zu machen, fordern jedoch gleichermaßen, im Team gemeinsam nach Verbesserungsmöglichkeiten zu suchen, Qualitätsentwicklungen auf dem Gebiet der IT und der IT-Sicherheit im Team zu diskutieren und in die Arbeit der Organisation einzubringen. Nur bei grob fahrlässigen oder vorsätzlichen Verstößen gegen diese IT-Sicherheitspolitik behält sich der Vorstand die Entscheidung über die notwendigen Disziplinarmaßnahmen vor.

Sicherheitsleitsätze für die Arbeit im Klinikum

- Jeder Mitarbeiter ist verpflichtet, mit den Patientendaten und anderen personenbezogenen Daten verantwortungsvoll umzugehen und sie nur im Rahmen seiner Aufgaben zu verwenden. Es ist selbstverständlich, dass Handlungen sich an den einschlägigen Gesetzten orientieren.
- Die Benutzungsrichtlinien für Informationverarbeitungssysteme der Ludwig-Maximilians-Universität sind einzuhalten. Genauso sind alle anderen für das Klinikum als allgemeinverbindlich erklärten und im Intranet des Klinikums veröffentlichten Richtlinien sorgfältig zu beachten.
- Die technischen Möglichkeiten zur Sicherstellung von Funktionalität, Integrität und Vertraulichkeit sind richtig anzuwenden. Organisatorische Sicherheitsmaßnahmen werden in den Geschäftsprozessen so verankert, dass sie kontinuierlich von allen Mitarbeitern mitgestaltet, angewendet und weiterentwickelt werden können.
- Alle IT-Systeme müssen vor der Beschaffung von der Abteilung für Medizintechnik und IT (MIT) begutachtet werden. Ausgenommen davon sind von der MIT festgelegte Standardkonfigurationen z. B. für PCs, die auf der Intranetseite des Klinikums veröffentlicht sind. Die fachliche Beurteilung von IT-Projekten, IT-Beschaffungsmaßnahmen sowie von HBFG-Anträgen erfolgt durch die MIT. Dabei wird insbesondere auch die Vereinbarkeit mit der IT-Strategie geprüft. Jedes beschaffte IT-System wird durch die dafür zuständigen Systemadministratoren unter Berücksichtigung aller dafür relevanten Sicherheitsrichtlinien konfiguriert, installiert und getestet. Für den Betrieb im Klinikum sind die fachliche Freigabe durch den verantwortlichen Leiter des betreffenden Bereichs, die datenschutzrechtliche Freigabe durch den Datenschutzbeauftragten des Klinikums und die sicherheitstechnische Freigabe durch den lokalen EDV-Beauftragten erforderlich. Die Installation und Anpassung der System- oder Anwendungssoftware erfolgt ausschließlich in Verantwortung der zuständigen Systemadministratoren.
- Der Betrieb anderer, insbesondere privater IT-Systeme (z.B. privater PCs) ist grundsätzlich nicht zulässig. Die Nutzung von Software muss sich auf die für den jeweiligen Arbeitsplatz freigegebenen Applikationen beschränken. Die zur Verfügung gestellte Hard- und Software darf nur für dienstliche Aufgaben eingesetzt werden, das Anfertigen von Programmkopien ist

genauso untersagt wie das Kopieren von dienstlichen Daten. Eine Ausnahme bildet das Erstellen von Kopien für Sicherungszwecke.

- Der Zutritt zu Gebäuden und Räumlichkeiten, der Zugang zu IT-Systemen und der Zugriff auf IT-Anwendungen und Informationen wird stets nur in dem Umfang gewährt, in dem dies für die Aufgabenerfüllung erforderlich ist. Gleichermaßen ist jeder Mitarbeiter gefordert, unerlaubten Zugang zu IT-Systemen und Zugriff auf Prozesse oder Informationen zu verwehren.
- Die Verarbeitung personenbezogener Daten ist nur im Rahmen der festgelegten Zwecke und der dafür zugelassenen Verfahren erlaubt. Eine anderweitige Nutzung oder Weitergabe ist untersagt.
- Informationen aus externen Quellen dürfen nur über entsprechende Sicherheitsschleusen in die IT-Systeme des Klinikums gelangen.
- Vor der Überführung von IT-Vorhaben in den Verfahrensbetrieb ist eine ausreichende Schulung zum Umgang mit dem IT-System, den IT-Sicherheitsanforderungen sowie zum korrekten Umgang mit den Sicherheitseinrichtungen unabdingbar. Dies gilt auch für die Einführung von Mitarbeitern in neue Aufgabengebiete. Die relevanten Inhalte ergeben sich aus dem jeweiligen IT-Schulungskonzept.
- Jeder IT-Nutzer setzt die vorhandenen Sicherheitselemente bewusst und richtig ein und beachtet die Sicherheitsrichtlinien des Klinikums.
- Jeder Mitarbeiter ist verpflichtet, hinsichtlich der ordnungsgemäßen Nutzung der IT-Systeme und Informationen seines Verantwortungsbereiches dem Vorstand des Klinikums - vertreten durch den lokalen Datenschutzbeauftragten oder den lokalen EDV-Beauftragten - Rechenschaft abzulegen. Sicherheitsmängel sind zu melden und deren Beseitigung in Zusammenarbeit mit dem IT-Sicherheitsmanagement aktiv zu betreiben. Bei auftretenden Problemen steht die gemeinsame Lösung im Vordergrund. Wir wollen aus eventuellen Fehlern lernen, um sie in Zukunft zu vermeiden.

Technische Richtlinien

Betrieb von Geräten an Netzen des Klinikums

Die Regelungen für den Betrieb von Geräten an Netzen des Klinikums der Universität München sind in der Richtlinie „FB_5_1053 – Richtlinien Betrieb Gerät MedVer-Netz“ beschrieben.

Diese Regelungen werden durch die Richtlinien

FB_5_3006 - Richtlinie zum Einsatz mobiler PCs

Richtlinie für den Einsatz von WLAN Geräten

RES Sicherheitszonen Netz

ergänzt.

Netz- und Systemmanagement (Netztrennung und Segmentierung)

Es muss eine angemessene Trennung verwendeter Netzwerke (Segmentierung) eingerichtet werden, um im Schadensfall mögliche Auswirkungen zu begrenzen. Die Segmentierung kann sich dabei an den organisatorischen Strukturen des Krankenhauses orientieren und als „Zonenkonzept“ umgesetzt werden.
Ergänzende Informationen dazu sind in den RES Sicherheitszonen Netz enthalten.

Die Segmentierung der Netzwerke muss Informationssysteme, die für die kDL relevant sind, so in absicherbare Netzwerksegmente aufteilen (z. B. im Rahmen eines Zonenkonzepts), dass die jeweiligen Systeme gegenüber sich ausbreitenden Gefährdungen im Netzwerk möglichst geschützt sind.

Absicherung Fernzugriffe

Fernzugriffe müssen so eingerichtet/gekapselt werden, dass andere IT-Systeme im KUM, die nicht im Fernzugriffsfokus stehen, nicht negativ beeinflusst werden können.

Fernwartungszugriffe müssen nachvollziehbar protokolliert werden.

Für Fernzugriffe müssen sichere Kommunikationsverbindungen verwendet werden und deren Anforderungen sollen regelmäßig kontrolliert werden.

Die möglichen Zugänge und Kommunikationsschnittstellen für einen Verbindungsaufbau von außen müssen auf das notwendige Maß beschränkt werden. Ebenso müssen alle Kommunikationsverbindungen nach vollzogenem Fernzugriff getrennt werden.

Es müssen unter Berücksichtigung des erforderlichen Schutzbedarfes des IT-Systems oder der Anwendung sichere Authentisierungsmechanismen für die Administratoren eingesetzt werden.

Härtung und sichere Basiskonfiguration der Systeme und Anwendungen

Für die Inbetriebnahme von Systemen und Anwendungen müssen Vorgaben zur sicheren Basiskonfiguration und ggf. Maßnahmen zur Härtung der eingesetzten Systeme festgelegt und angewendet werden.

Es muss eine regelmäßige Analyse und ggf. Anpassung der Vorgaben zur sicheren Basiskonfiguration und Härtung im Hinblick auf mögliche technische Schwachstellen durchgeführt werden.

Es muss ein Freigabe- und Kontrollverfahren für die Installation von Software auf betriebsrelevanten Systemen implementiert werden.

Schutz vor Schadsoftware

Die Umsetzung der allgemeinen Maßnahmen zum Schutz vor Schad-software nach DIN ISO 27799 muss geprüft werden, insbesondere die folgenden Maßnahmen:

a. Vorgabe einer Richtlinie zum Verbot des Einsatzes nicht autorisierter Software sowie den Risiken, die sich aus der Nutzung von Software aus unbekannten Quellen ergeben können, sowie möglichen Schutzmaßnahmen

b. Maßnahmen zur Vermeidung und Erkennung von nicht autorisierter Software sowie zur Vermeidung bekannter oder potenziell verdächtiger Software, E-Mail-Anhänge und Webseiten

c. Reduzierung möglicher Schwachstellen durch regelmäßige Updates gemäß den vom Hersteller entsprechender Systeme gesetzten Rahmenbedingungen (Freigabe)

Zum Schutz von unternehmenskritischen Informationen muss ein System zur Vorbeugung und Erkennung schädlicher Software eingerichtet werden.

Zum Schutz vor Ausführung von Schadsoftware soll die Ausführung von unbekannten Programmen verhindert werden (Application-Whitelisting). Die Ausführung von Makros in Bürosoftwareprodukten muss kontrolliert erfolgen.

Intrusion Detection / Prevention

Es soll ein System zur Vorbeugung und Erkennung von nicht autorisierten Zugriffsversuchen auf das Netzwerk und die Systeme des Krankenhauses implementiert werden, das neben dem Verhindern unberechtigter Zugriffsversuche (z. B. durch Firewall) auch den prinzipiell erlaubten Netzwerkverkehr auf gefährliche Inhalte kontrolliert.

Es müssen regelmäßige Überprüfungen auf Schwachstellen des eigenen Netzes erfolgen, um sowohl externe Angriffsmöglichkeiten zu identifizieren, als auch interne Schwachstellen zu erkennen, die aufgrund eines Firewall-Schutzes (derzeit) nicht zu einer direkten Gefährdung führen.

Identitäts- und Rechtemanagement

Die Forderung, ein adäquates Identitäts- und Berechtigungsmanagement in jedem Krankenhaus zu etablieren, wurde schon im Rahmen des technischen Datenschutzes seitens der Aufsichtsbehörden gefordert. Dies gilt nicht nur für Gesundheitsdaten, die besonderen Anforderungen hinsichtlich des Schutzbedarfs sowie der damit verbundenen Informationsverarbeitung unterliegen, auch der Zugriff z. B. auf Administrationsberechtigungen oder Netzwerksysteme muss angemessen geschützt werden. Zugang zu und Zugriff auf entsprechende Informationen darf nur durch berechtigte Nutzer erfolgen. Werden in Notfallsituationen bestehende Zugriffsbeschränkungen temporär aufgehoben, um die medizinische Versorgung sicherzustellen, bestehen besondere Anforderungen an eine nachträgliche Kontrolle dieser Zugriffe.

Das KUM muss ein Rollen- und Berechtigungskonzept erstellen und umsetzen, welches den unbefugten Zugriff auf personenbezogene Daten durch angemessene Maßnahmen verhindert. Der Zugriff auf Gesundheitsdaten im Rahmen vertraglicher und gesetzlicher Verpflichtungen (z. B. Behandlungsvertrag, gesetzliche Übermittlungspflichten) muss kontrolliert werden.

Es muss eine Richtlinie zur Zugriffskontrolle erstellt werden, die Zugriffsrechte und -beschränkungen auf Informationen und Funktionen im Informationsmanagementssystem und dessen Erteilung bzw. Entzug regelt. Hierbei sollen insbesondere die folgenden Punkte berücksichtigt werden:

- Einheitliche Beschreibung, Dokumentation und Umsetzung des Identitäts- und Berechtigungsmanagements,
- Erstellung eines Überblicks über Gruppen und Arten von Identitäten und Berechtigungen, die typischerweise in den verschiedenen Bereichen einer Institution verwaltet werden,
- Vorgaben für Beantragung und Vergabe von Zugriffsrechten und deren Änderungen sowie eine nachvollziehbare Dokumentation,
- Vorgaben zur Verwaltung von Identitäten, Benutzerkennungen und Berechtigungen,
- Umgang mit den Benutzerkennungen, Berechtigungen und Authentisierungsmitteln durch die Benutzer,
- Vorgaben zum Umgang mit Kennungen von Administratoren, Notfallbenutzern und anderen privilegierten Benutzern sowie Vorgaben zur Gewährung von zeitlich eingeschränktem Zugriff auf erweiterte Berechtigungen,
- Festlegung von Berechtigungsstrukturen, Dokumentation und Genehmigungsverfahren für die Vergabe von Berechtigungen, Festlegen und Einhalten von Administrationsprozessen,
- Vorgaben zur Erstellung und restriktiven Zuweisung von Berechtigungen auf den Zielsystemen,
- regelmäßige Überprüfung der Berechtigungen nach den Prinzipien Need-to-Know und Least Privileges,
- regelmäßige Prüfung aller Berechtigungen auf Aktualität (keine Berechtigungen für inaktive oder gelöschte Benutzer, keine unberechtigte Kumulation von Zugriffsrechten infolge von innerbetrieblichen Aufgabenwechseln oder Ausbildungsprogrammen),
- regelmäßige Prüfung aller Berechtigungen, ob diese einem Benutzer unter Umgehung des Identitäts- und Berechtigungsmanagements direkt auf den Zielsystemen zugewiesen wurden

Nach Beendigung des Arbeitsverhältnisses zwischen Personal und Krankenhaus muss sichergestellt werden, dass erteilte Zugangsrechte unmittelbar entzogen werden (insbesondere auch bei Studenten, Praktikanten und Aushilfspersonal).

Sichere Authentisierung

Der Zugang zu IT-Systemen und Informationen ist durch ein sinnvolles und risikofokussiertes Authentisierungsverfahren abzusichern.

Es muss ein formaler Prozess zur Vergabe/Zuweisung von Authentisierungsdaten etabliert werden, der

- Nutzer zur Geheimhaltung individueller Authentisierungsdaten verpflichtet
- die erstmalige Übermittlung von (temporären) Authentisierungsdaten zum Nutzer regelt
- Vorgaben für Änderungsintervalle sowie Komplexität von Passwörtern enthält
- Vorgaben für die Änderung temporärer Passwörter nach der ersten Anmeldung an einem Informationssystem enthält
- die Identität eines Nutzers sicherstellt, dessen Authentisierungsdaten geändert werden sollen

Diese Anforderungen sind in der Passwort-Richtlinie näher beschrieben und geregelt.

Authentifizierungsverfahren müssen so gewählt werden, dass die Zugriffssicherheit auf Daten und IT-System bezogen auf die Erbringung der kDL angemessen umgesetzt wird. Dabei sollen auch die Einsatzmöglichkeiten einer 2-Faktor-Authentifizierung zur Erhöhung der Sicherheit berücksichtigt werden.

Kryptographische Absicherung

Mit Hilfe eines Kryptographiekonzeptes können die Vertraulichkeit, AUTHENTIZITÄT oder INTEGRITÄT von Informationen gewährleistet werden.

Das KUM soll ein Kryptographiekonzept erstellen, welches die kryptographischen Verfahren als auch das Schlüsselmanagement der jeweiligen Anwendungsfelder (z.B. WLAN, VPN, SSL für E-Mail und Web) festlegt. Das Konzept soll weiterhin festlegen, in welchen Anwendungsbereichen Verschlüsselung verbindlich einzusetzen ist.

Das Kryptographiekonzept muss die technischen und organisatorischen Gegebenheiten des Krankenhauses, insbesondere die eingesetzte Medizintechnik, berücksichtigen. Die Festlegung von Art, Stärke und Qualität des jeweils erforderlichen Verschlüsselungsalgorithmus soll anhand von Risikoanalysen erfolgen.

Innerhalb des Kryptographiekonzeptes sollen alle relevanten IT-Technologien und Kommunikationsverbindungen aufgeführt werden.

Alle Informationen, Anforderungen und Regelungen sind im Kryptographiekonzept definiert.

Mobile Sicherheit, Sicherheit Mobiler Zugang und Telearbeit

Es sind unterstützende Sicherheitsmaßnahmen und -richtlinien zu etablieren, um die Risiken und den Schutz von Informationen bei der Nutzung von Mobilgeräten und Fernzugriffen innerhalb einer ungeschützten Umgebung (öffentliche Orte, Verkehrsmittel, Heimarbeitsplätze, etc.) zu steuern. Die Verwendung von privat genutzter Hardware („bring your own device“) ist hierbei explizit zu regeln.

Werden mobile Geräte, Telearbeitsplätze und mobile medizinische Geräte eingesetzt, soll deren Verwendung explizit freigegeben werden.

Nutzer mobiler Geräte und Telearbeitsnutzer müssen hinsichtlich des Schutzbedarfes mobiler Geräte, Telearbeitsplätze und den hierauf verarbeiteten Daten sensibilisiert und zur Einhaltung der festgelegten Regelungen der Richtlinie(n) verpflichtet werden, insbesondere wenn es sich um den Zugriff oder die Verarbeitung von Gesundheitsdaten handelt.

Neben der Bestimmung der spezifischen Risiken, die sich aus der Nutzung mobiler Technologien im Gesundheitswesen ergeben, müssen folgende Regelungen für Mobilgeräte und Telearbeitsplätze festgelegt werden:

- Anmeldung, Zugangskontrollen und Authentisierungsmethoden
- Anforderungen an den physischen Schutz des Gerätes, z. B. dass Daten nicht von unberechtigten Personen gelesen werden können, das Gerät niemals unbeaufsichtigt bleiben darf und ggf. bei Nichtbenutzung weggeschlossen werden sollte (Diebstahls-schutz sowie unerlaubter Zugriff und Zugang von Dritten)
- Einschränkung von Software-Installationen und Verfahren zur Software- bzw. System-Aktualisierungen
- Schutz vor Schadsoftware (z. B. Firewall, Virenschutz)
- Nutzung drahtloser Verbindungen (z. B. WLAN, Bluetooth) und Internet-Diensten
- Methoden zur Sicherung des Fernzugriffs
- Art der Informationen, die auf den Geräten verarbeitet bzw. lokal gespeichert werden dürfen
- Verschlüsselungsverfahren und Maßnahmen zum Schutz der Daten, insbesondere von Gesundheitsdaten
- Geregeltes Backupverfahren/-turnus und Sicherstellung der Einbeziehung dieser mobilen Geräte zu geplanten Backup-Zeiten
- Remotezugriff, Sperrung, Löschung und Deaktivierung des Gerätes sowie Meldeverfahren bei Verlust
- Widerruf von Berechtigungen und Zugriffsrechten sowie die Rückgabe von Betriebsmitteln
- Explizite Trennung von privater und geschäftlicher Nutzung (bei BYOD)
- Anforderungen an die Genehmigung mobiler oder Tele-Arbeitsplätze

Aufgrund der besonderen Herausforderungen im Hinblick auf Administration und Nutzungsverhalten SOLL BYOD nur in begründeten Ausnahmefällen zum Einsatz kommen, insbesondere die Nutzung privater (vom Nutzer administrierter) Endgeräte (z. B. Smartphones) muss kritisch geprüft werden. Dies schließt Vorgaben für die Speicherung personenbezogener Daten auf privaten Geräten ausdrücklich ein.

Für mobile Geräte (insbesondere Smartphones, Tabletts) soll ein Mobile Device Management implementiert werden.

Die Regelungen, Richtlinien und Anforderungen an die Telearbeit sind auf der SharePoint-Seite der Personalabteilung veröffentlicht.

Vernetzung von Medizingeräten

Für den Einsatz von Medizingeräten in medizinischen IT-Netzwerken sollen die Anforderungen der DIN EN 80001-1:2011 für das Risikomanagement berücksichtigt werden.

Die Aufrechterhaltung des Betriebs medizintechnischer Anlagen muss auch bei Verlust von Kommunikationsverbindungen oder Netzwerkintegrationen möglich sein, bzw. über entsprechende organisatorische Ersatzverfahren sichergestellt werden, soweit dies im Verantwortungsbereich des Betreibers der medizintechnischen Anlage liegt.

Datensicherung, Datenwiederherstellung und Archivierung

Die im Krankenhaus erhobenen und verarbeiteten Informationen (Gesundheitsdaten, unternehmenskritische Informationen, z. B. auch Konfigurationsdaten), müssen vor Verlust geschützt werden.

Die Vorgaben zur regelmäßigen Prüfung und Anfertigung von Sicherheitskopien von Informationen (Datenbanken, Dateisystemen, Archiven, Konfigurationsdaten), Software und Systemimages MÜSSEN in einem Datensicherungskonzept definiert werden.

Ordnungsgemäße IT-Administration

Systemadministratoren stellen die ordnungsgemäß funktionierende IT-Landschaft durch Wartung, Erweiterung und Notfallreaktionen sicher.

Systemadministratoren müssen über die notwendigen fachlichen Qualifikationen als auch über ausreichende Ressourcen verfügen, um die ihnen übertragenen Aufgaben zuverlässig und sorgfältig erledigen zu können.

Die Überwachung von Administrationstätigkeiten soll durch eine personenbezogene Rechtevergabe von Administrationsprivilegien im Logfilemanagement ermöglicht werden. Die Manipulation von Logfiles muss durch geeignete organisatorisch-technische Maßnahmen soweit möglich ausgeschlossen werden.

Es müssen Vertretungsregelungen für administrative Aufgaben und Verantwortlichkeiten getroffen werden. Die jeweiligen Vertreter der kDL sind in den Betriebshandbüchern festzuhalten.

Nach dem Ausscheiden von IT-Administratoren MÜSSEN deren persönliche Zugänge (insbesondere diese mit privilegierten Rechten) unmittelbar gesperrt und ihm/ihr bekannte Passwörter geändert werden (z.B. für Router, Master-Kennwörter, Notfall-Kennungen).

Patch- und Änderungsmanagement

Um Schwachstellen zu vermeiden und kontinuierlich zu schließen, ist ein kontrolliertes und gesteuertes Patch- und Wartungsmanagement nötig. Das Änderungs- und Patchmanagement muss im sensiblen

kDL-Kontext mit besonderer Sorgfalt erfolgen, um Risiken für entsprechende medizinische Prozesse zu minimieren.

Für Änderungen an Systemen (Hard- und Software) die unter die kDL-Systeme Fallen müssen formale Freigabeprozess implementiert werden, die eine adäquate Risikobewertung voraussetzen. Diese kann ggf. durch die betroffenen Bereiche erfolgen. Freigabeprozesse können dabei differenziert für unterschiedliche Klassen von Änderungen und ggf. unterschiedliche Freigabeebenen ausgestaltet werden. Der Freigabeprozess soll ebenfalls Vorgaben für eine Roll-Back-Planung enthalten.

Die ordnungsgemäße Einhaltung der Freigabeprozesse (z. B. für Patches, Freigabeprozess für Neueinführung von Systemen, Freigabeprozess von Changes) muss regelmäßig, mindestens alle 2 Jahre, überprüft werden.

Protokollierung

Zur Gewährleistung der Nachvollziehbarkeit von sicherheitsrelevanten Aktionen sowie aufgrund gesetzlicher Anforderungen an den Datenschutz muss ein Protokollierungs-konzept erstellt werden, welches die Nachvollziehbarkeit z. B. von Störungen, Warnungen, Informationssicherheitsvorfällen, Ausnahmen sowie Datenzugriffen von Benutzern und Administratoren entsprechend der gesetzlichen Vorgaben gewährleisten sollte.

Es muss ein Protokollierungs- und Auswertungskonzept erstellt werden, welches zumindest Festlegungen zu Art, Ablageort und Umfang der protokollierten Informationen sowie zu den Modalitäten der Auswertung der Protokolle enthält. Hierzu zählen insbesondere Anlässe für eine anlassbezogene Auswertung sowie Regelungen für stichprobenartige Auswertungen, Umfang, Verantwortliche und Beteiligte der Auswertungen (ggf. „4-Augen-Prinzip“) sowie Umsetzung der Betroffenenrechte (Informationspflichten).

Protokollierte Ereignisse sollen nachvollziehbar abgelegt werden und vor dem Zugriff und Manipulation Unbefugter geschützt zu werden.

Protokollierte Aktivitäten der Systemadministratoren müssen bei Systemen mit erhöhtem Schutzbedarf durch entsprechende Maßnahmen gegen nachträgliche Änderung, Löschung oder Deaktivierung durch die Systemadministratoren geschützt werden.

Zusätzlich zu sicherheitsrelevanten Ereignissen (Konfiguration der Protokollierung auf System- und Netzebene) SOLL eine zentrale Protokollierungsinfrastruktur auch allgemeine Betriebsereignisse protokollieren, die auf einen Fehler hindeuten, z. B. Ausbleiben von Protokollierungsdaten bzw. Nichterreichbarkeit eines protokollierenden IT-Systems, Betriebsereignisse, die auf eine außergewöhnliche Auslastung bzw. Beanspruchung einzelner Dienste hindeuten.

Handhabung von Datenträgern

Sowohl die EU-DSGVO als auch das BayKrG schreiben vor, Daten – gerade personenbeziehbare Patienten- und Mitarbeiterdaten – streng vertraulich zu behandeln und im Gewahrsam des Klinikums zu

belassen. Daher ist bei allen erdenklichen Speichermedien darauf zu achten, dass diese entweder technisch „sauber“ gelöscht werden (Degausser oder professionelle Lösch-Software mit mindestens 72 Überschreib-Zyklen) bevor sie das Haus verlassen oder aber im Gewahrsam des Klinikums verbleiben. In bestimmten Fällen kann es daher notwendig werden, Datenträger von den Herstellern der jeweiligen Systeme zu erwerben.

Entsprechende vertragliche Vereinbarungen müssen bereits bei der Anschaffung (Kauf, Leih- oder Leasing-Verträge) getroffen werden um spätere Unstimmigkeiten zu vermeiden.

Softwaretests und Freigaben

Zur Sicherstellung des ordnungsgemäßen Produktiveinsatzes von Anwendungen sollten diese durch ein geregeltes Verfahren getestet und freigegeben werden.

Vor dem Einsatz im Produktivbetrieb sollen angemessene Integrations-, System- und Freigabetests durchgeführt werden, bei denen die Funktionalität und Sicherheit der Software auf dem Zielsystem geprüft und freigegeben wird.

Wurde die Software abgenommen, muss sie danach für die Nutzung freigegeben werden. Die Freigabe der Software ist nachweisbar zu dokumentieren und geeignet zu hinterlegen.

Reale Gesundheitsdaten sollen nicht auf Entwicklungs- und Testumgebungen genutzt oder gespeichert werden. Ist eine Nutzung unvermeidbar, MUSS die Entwicklungs- und Testumgebungen entsprechend gehärtet oder die Daten anonymisiert bzw. pseudonymisiert werden.

Datenschutz

Die Berücksichtigung der Anforderungen des Datenschutzes und der gesetzlichen sowie unternehmensinternen Regelungen zum Datenschutz im Informationssicherheitsmanagement ist in der Informationssicherheitsrichtlinie zu fordern und umzusetzen. Ein Informationssicherheitsvorfall kann bei Verletzung der VERTRAULICHKEIT von Gesundheitsdaten immer auch einen Datenschutzverstoß zur Folge haben. Datenschutz und Informationssicherheit sind daher gemeinsam zu betrachten.