Handlungsempfehlungen zur Verbesserung der Informationssicherheit an Kliniken

EINE VERÖFFENTLICHUNG DES
UPKRITIS BRANCHENARBEITSKREISES
MEDIZINISCHE VERSORGUNG

STAND: 27.07.2017

Dateiname: TLP-White_Handlungsempfehlungen_Kliniken_1.2.docx

Inhalt

1 Zweck / Zielsetzung dieses Dokumentes

Die Abhängigkeit der Kliniken in Geschäfts- und Behandlungsprozessen von IT nimmt in allen Bereichen stetig zu. Unabhängig von der Reichweite des IT-Sicherheitsgesetzes besteht dringender Handlungsbedarf bei der **Verbesserung der Informationssicherheit**. Der Fokus liegt hierbei auf der Verfügbarkeit unternehmenswichtiger und unternehmenskritischer Systeme, Prozesse und Daten bzw. Informationen. Informationssicherheit ist schon lange kein Thema nur für die IT-Abteilung.

Zur Erreichung dieses Ziels wurden in diesem Dokument Empfehlungen durch den BAK Medizinische Versorgung zusammengestellt, deren Umsetzung für Kliniken mit überschaubarem Aufwand möglich ist.

In den Kapiteln 3 – 10 sollen konkrete Prüffragen den Einstieg in das Thema vereinfachen.

2 Management Summary

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, IT-SiG) ist am 25. Juli 2015 als Artikelgesetz in Kraft getreten und hat das BSI-Gesetz (BSIG) stark erweitert.

Nach §8a BSIG müssen Betreiber 'Kritischer Infrastrukturen' ihre für die Versorgung der Bevölkerung kritischen Prozesse nach dem Stand der Technik absichern und dieses gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) geeignet nachweisen.

Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Als Kriterienwerke hierfür sind entweder anerkannte Normen und Standards oder alternativ vom BSI anerkannte branchenspezifische Sicherheitsstandards (B3S) zugelassen.

Welche Krankenhäuser als 'Kritische Infrastruktur' (KRITIS) eingestuft werden, regelt nach §2 und §10 BSIG die BSI-Kritis-Verordnung (BSI-KritisV). Demnach liegt der Schwellwert für Krankenhäuser bei einer Fallzahl von 30.000 stationären Fällen pro Jahr.

Unabhängig von der Einstufung als KRITIS empfiehlt der Branchenarbeitskreis Medizinische Versorgung (BAK MV) dringend, folgende Anforderungen umzusetzen:

1. Einführung einer geeigneten **Organisationsstruktur,** um den besonderen Anforderungen der IT-Sicherheit begegnen zu können .

   Für den BAK MV ist die Absicherung der Dienstleistung Medizinische Versorgung KEIN reines IT-Thema und erfordert Konzepte und Verfahrensrichtlinien, die über die jeweiligen IT-Abteilungen hinausreichen.

   Die Verantwortlichkeit sollte in der Nähe der Geschäftsführung, z.B. in einer Stabstelle mit der Rolle eines Informationssicherheits-Beauftragten, angesiedelt sein.

2. Identifikation aller **kritischen Patientenversorgungsprozesse** der stationären Versorgung.

3. Identifikation der diese kritischen Prozesse unterstützenden **IT-Infrastruktur**, **IT-Verfahren** sowie **Schnittstellen** zu Unterstützungsprozessen.

4. Einführung eines **Information Security Management Systems** (ISMS) nach dem Stand der Technik. Diese Anforderung folgt auch der im Mai 2016 in Kraft getretenen EU-Datenschutzgrundverordnung (DSGVO) und ist für KRITIS verpflichtend.

5. Einbindung des **IT-Risikomanagements** für die identifizierten kritischen Prozesse in das Unternehmensrisikomanagement.

   Auf der Grundlage der resultierenden Risiken für die Patientenversorgung soll eine Priorisierung vorgenommen und geeignete sowie angemessene technische und organisatorische Maßnahmen zur Reduktion der Risiken abgeleitet, umgesetzt und bzgl. ihrer Wirksamkeit bewertet werden.

6. Einführung eines **Business Continuity Managements**, zumindest für die IT-Infrastruktur und IT-Verfahren, welche die kritischen Patientenversorgungsprozesse unterstützen.

7. Die Etablierung eines **Meldeverfahrens / Meldestelle** für die Meldung von relevanten Vorfällen an die Datenschutzaufsichtsbehörden und an die Meldestelle des BSI in Verbindung mit der Anbindung an einen CERT-Dienst zur Informationsbeschaffung über aktuelle Bedrohungen. Dies ist für KRITIS verpflichtend.

Diese Anforderungen müssen von KRITIS-Betreibern innerhalb einer Zweijahresfrist ab Inkrafttreten der BSI-KritisV umgesetzt und geprüft werden. Die Auditergebnisse müssen ebenfalls innerhalb dieser Frist dem BSI zur Verfügung gestellt werden.

Eine Ausnahme bildet das Meldeverfahren, dies ist innerhalb von 6 Monaten zu etablieren.

Bußgelder bei Nichterfüllung der Pflichten sind bis zur Höhe von 100.000€ möglich.

Der BAK Medizinische Versorgung empfiehlt zudem, an zentraler Stelle sämtliche gesetzlichen und anderen regulatorischen Compliance-Anforderungen an die Krankenhäuser zu sammeln und von dort in die betroffenen/beteiligten Bereiche zu kommunizieren.

Bei der Umsetzung der o.g. Anforderungen empfiehlt der BAK MV auf bestehende Normen und Konzepte zurückzugreifen. Einen pragmatischen Ansatz bietet das BSI mit seinen BSI-Standards[1]. Weitergehende Konzepte und Umsetzungsstrategien zum ISMS sind der ISO 27000 Familie zu entnehmen, bzgl. (IT-)Risikomanagement stehen weitere ISO und IEC Normen zur Verfügung[2] und auch für (IT-Service) Continuity Management liegen Normen vor[3].

Als weitere Grundlage werden die aktuell in Entwicklung befindlichen B3S zur Verfügung stehen.

[1] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

[2] ISO 31000, ISO 27005 und IEC 80001

[3] ISO 22301 sowie ISO20000-1

Nach Einschätzung des BAK MV werden durch diese zusätzlichen Anforderungen neue Aufgaben und Tätigkeitsfelder für Krankenhäuser formuliert, die aufgrund Ihrer Dauerhaftigkeit, ihres Umfangs und ihrer Kritikalität nicht kostenneutral und nicht allein mit dem vorhandenen Mitarbeiter Know-How umgesetzt werden können.

3 Erstellen einer Leitlinie zur Informationssicherheit

Informationssicherheit wird durch eindeutige und transparente Organisation der Verantwortlichkeiten und Kompetenzen erreicht. Die Geschäftsführung verabschiedet hierzu eine eindeutige Leitlinie, in der die Eckpunkte der Informationssicherheit festgelegt sind.

Es wird klargestellt, wer für die Informationssicherheit des Unternehmens welche Verantwortlichkeiten und welche Kompetenzen übertragen bekommt. Entsprechend der Organisation der Verantwortlichkeiten für die Einhaltung des Datenschutzes ist die Geschäftsführung dafür verantwortlich, eine eindeutige und nachvollziehbare Organisation der Informationssicherheit zu installieren.

Auf der Basis dieser eindeutigen Leitlinie werden einerseits Verantwortlichkeiten und Kompetenzbereiche der Abteilungen untereinander abgegrenzt und andererseits das Miteinander in Fragen der Informationssicherheit geregelt.

4 Etablierung eines Informationssicherheitsmanagements

Zur Erhöhung und eindeutigen Festlegung der Kompetenzen und Aufgabenbereiche muss ein Informationssicherheitsmanagement (ISMS) etabliert werden. Hierzu ist es sinnvoll, ggf. in Abstimmung mit der Personalvertretung, einen Informationssicherheitsbeauftragten (ISB) zu bestellen, der zu allen sicherheitsrelevanten Fragen im Bereich der IT zu befragen, gleichzeitig aber auch als überwachende Instanz für alle sicherheitsrelevanten IT-Prozesse zuständig ist. In das ISMS müssen je nach Organisation des Hauses verschiedene Rollen bzw. Aufgabenbereiche eingebunden werden, sodass die Verantwortlichen für die Server- und Netzwerkbetreuung ebenso mit einbezogen werden, wie diejenigen für Medizintechnik, Haus- und Kommunikationstechnik und natürlich auch der Datenschutzbeauftragte oder das Risiko- und Notfallmanagement. Zu den Aufgaben eines Informationssicherheitsmanagements gehören die Behandlung und Nachbehandlung von Sicherheitsvorfällen inklusive der Planung von vorbeugenden Maßnahmen und die Überwachung der Umsetzung.

Eine erste Analyse des Informationssicherheitsstatus der in der Klinik eingesetzten IT-Systeme, incl. der in der Medizin- und Betriebstechnik genutzten Systeme, stellt die Basis der ersten Risikobewertung dar (vgl. 5).

Gemeinsam mit den für den Betrieb der Systeme Verantwortlichen erstellt der Informationssicherheitsbeauftragte eine IT-Risikobewertung. Ebenfalls gemeinsam sind aus der IT-Risikobewertung Handlungsmaßnahmen (Risikokontrollmaßnahmen) abzuleiten und einerseits mit den für den Betrieb Verantwortlichen, andererseits ggf. auch mit Nutzern abzustimmen. Welche Maßnahmen mit welcher Priorität tatsächlich umzusetzen sind, hat letztlich die Unternehmensführung im Rahmen einer Gesamtrisikobewertung zu entscheiden. Die Aufgabe des Informationssicherheitsbeauftragten ist es dann, die Durchführung der IT-Risikokontrollmaßnahmen einzuleiten, zu überwachen und schließlich mit einer erneuten Analyse des Informationssicherheitsstatus zu verifizieren.

Analyse und Bewertung des Informationssicherheitsrisikos sind als permanente Prozesse zu etablieren. Insbesondere die stetige Fortentwicklung der Bedrohungslage erzwingt dieses Vorgehen. Nicht nur die Einführung neuer Systeme bzw. die Änderung bestehender Vernetzungen müssen von einem Informationssicherheitsmanagement begleitet werden, sondern auch schon bestehende Systeme müssen bei der Betrachtung mit einbezogen werden. Eine Ausrichtung an der ISO27001 ist dabei sinnvoll.

Aufgabe des Informationssicherheitsmanagement ist es auch, die ermittelte Organisationsstruktur in Hinblick auf Einflüsse auf die IT-Sicherheitsstruktur zu analysieren und ggf. um IT-Sicherheitsaspekte zu ergänzen. (vgl. 4.2)

Für die organisatorische Einordnung des ISB empfiehlt sich eine Stabsstelle direkt unterhalb der Geschäftsführung.

5 Bestandsaufnahme

Basis aller Bemühungen für ein umfassendes Informationssicherheitsmanagement stellt eine gründliche Bestandsaufnahme der vorherrschenden Strukturen dar. Die Bestandsaufnahme darf dabei nicht nur die konkreten IT-Komponenten umfassen, sondern muss auch das bauliche und organisatorische Umfeld berücksichtigen. Zu betrachten sind dabei nicht nur die Systeme, die der IT-Abteilung unterstehen, sondern alle informationstechnischen Systeme, also auch TK-Anlagen, Gebäudeleittechnik, Medizintechnik usw.

5.1 Bauliche Bestandsaufnahme

Eine belastbare Beurteilung der Informationssicherheit kann nur auf der Basis einer möglichst vollständigen Kenntnis der physikalischen Gegebenheiten der IT-Infrastruktur erfolgen.

Viele Gebäude einer Klinik bestehen aus unterschiedlichen Haupt- und Nebengebäuden, die mit der Zeit erweitert oder zurückgebaut wurden. Besonders in Altbaubeständen haben sich über die lange Betriebszeit der Gebäude „Bausünden“ eingeschlichen, die einem sicheren Betrieb des IT-Systems entgegenstehen. Aber auch neuere Gebäude sind baulichen Veränderungen unterworfen, die ggf. Auswirkungen auf die verbaute IT-Infrastruktur haben.

Daher sollte eine allgemeine bauliche Bestandsaufnahme aller Gebäude mit IT-Technik durchgeführt werden. Ein besonderes Augenmerk ist hierbei auf die Trassenführung von Daten- und Versorgungsleitungen, den Zutritt und den Zutrittsschutz, die Klimatisierung, Wasser- und Brandschutz, die unterbrechungsfreie Stromversorgung, die Absicherung von Netzwerkzugängen und Kabeltrassen und WLAN-Accesspoints zu legen.

Exemplarische Prüffragen:

- Ist die IT-Infrastruktur (z.B. Serverräume, Netzwerkschränke, Unterverteiler, WLAN-Accesspoints) gegen unbefugten Zutritt bzw. gegen Manipulation geschützt?
- Ist die IT-Infrastruktur durch Redundanzen (z.B. redundante Datenleitungen, redundant angebundene Server- und Netzwerkkomponenten, alternative Stromversorgungen) für einen unterbrechungsfreien Betrieb vorbereitet?
- Werden Serverräume in zwei unterschiedlichen Brandabschnitten betrieben?

- Sind Server- und Verteilerräume frei von wasserführenden Leitungen?
- Werden die Serverräume mittels redundanter Strom- und Klima-Installationen versorgt und sind über redundante Datenverbindungen gekoppelt?
- Gibt es weitergehende strukturelle Sicherungsmaßnahmen wie umfassende Einbruch- und Brandmelde- sowie Rauchabzugsanlage und ggf. erweiterten Hochwasserschutz?
- Ist die Lage der Räume unkritisch, also entfernt oder geschützt vor weiteren Gefahrenquellen?
- …

Auf Basis der Bestandsaufnahme können die Gebäude in unterschiedliche Kategorien eingeteilt werden. Die Kategorien sollten beschreiben, welche Gebäude aus Sicht des Informationssicherheitsmanagements die Anforderungen an die Informationssicherheit bis zu welchem Grad erfüllen. Gemeinsam mit den Verantwortlichen für die IT-Infrastruktur und Gebäudeinstandhaltung oder -management erstellt das Informationssicherheitsmanagement eine Anforderungsliste zur Aufnahme des Sanierungs- bzw. Sicherungsbedarfs in die Bauplanung des Klinikums.

Bei Neubau und Umbau sollte das Informationssicherheitsmanagement frühzeitig in die Planungen einbezogen werden.

5.2 Informationssicherheits-Organisation

Unter dem Begriff „Informationssicherheits-Organisation“ werden alle Dokumentationen erfasst, die die IT-Abteilung und die angrenzenden Bereiche betreffen.

Für die Beurteilung der Informationssicherheit ist es notwendig, die etablierten organisatorischen Strukturen zu erfassen. Neben den strukturellen Gegebenheiten sind die an der Klinik etablierten Kommunikationswege, Zuständigkeiten, Notfallpläne etc. aufzunehmen.

Nur bei gründlicher Analyse und Dokumentation können fehlende oder unzureichende Strukturen (Ansprechpartner und Zuständigkeiten, alternative Kommunikationswege, Vertretungsregelungen, Kompetenzlücken bzw. -Konflikte, Eskalationspfade und Notfallpläne) identifiziert und zielgerichtet behoben werden.

Die zu beteiligenden Bereiche bzw. Personen müssen mittels stringenter Prozessdefinitionen einerseits über eindeutige Verfahrensbeschreibungen und Handlungsanweisungen verfügen, andererseits müssen die notwendigen Kompetenzen und Verantwortlichkeiten für alle transparent festgelegt sein.

Ein dem wachsenden IT-Umfeld stetig anzupassendes Eskalations- und Risikomanagement ist zu etablieren und muss Eingang in das Sicherheitskonzept finden.

Exemplarische Prüffragen:

- Welche IT-Dokumentationen bestehen?
- Werden diese Dokumentationen befolgt?
- Werden die Dokumente regelmäßig auf Aktualität überprüft?
- Wiedersprechen sich diese mit Dokumentationen aus anderen Bereichen?
- Welche Zuständigkeiten verhindern oder erschweren ggf. angemessene Reaktionen auf IT-Sicherheitsvorfälle oder deren Prävention?

- Wo sind Zuständigkeiten bzgl. der Informationssicherheit klar geregelt?
- Sind Zuständigkeiten personell redundant ausgelegt und in Notfallsituationen erreichbar?
- Existieren Notfallpläne für Notfallsituationen?
- Werden regelmäßig Notfallsituationen geübt?
- Welche verbindlichen hausweiten Vorgaben mit Bezug zur Informationssicherheit existieren?
- Existieren Dokumentationen und Priorisierungen, um einen Wiederanlauf zu ermöglichen? Berichtet der ISB direkt der Geschäftsführung?
- Erfolgen bereits regelmäßige Audits mit Bezug zur Informationssicherheit?
- Ist ein IT-Risikomanagement etabliert?
- …

5.3 IT-Systeme

Zur Herleitung notwendiger sicherheitsverbessernder Maßnahmen ist die Kenntnis über die eingesetzten IT-Systeme essentiell. Neben den zentralen IT-Systemen sollten auch die dezentralen, ggf. nicht über das Netzwerk verbundenen, aber im Rahmen zentraler Dienstleistungen wesentlichen IT-Systeme erfasst werden. Bei der Betrachtung der Informationssicherheit geht es nicht nur um die zentrale IT, sondern um die Sicherstellung von essentiellen IT-Dienstleistungen für den Betrieb des Krankenhauses. Daher wird idealerweise bei der Erfassung der IT-Systeme auch der durch die Systeme unterstützte Prozess mit erfasst. Nur so ist eine belastbare Beurteilung der Informationssicherheit und des Restrisikos möglich.

Neben den IT-Strukturplänen sollten auch das Verfahrensverzeichnis des Datenschutzbeauftragten, die Systeme der Betriebstechnik sowie das Verzeichnis der Medizingeräte in den Bestand mit einbezogen werden.

Exemplarische Prüffragen:

- Welche IT-Systeme (vgl. Kap. 4) sind im Unternehmen im Einsatz?
- Welche Versorgungsdienste sind zum Betrieb dieser Systeme erforderlich?
- Für welche Prozesse sind welche IT-Systeme im Einsatz?

5.4 Betrieb von IT-Systemen

Beim Betrieb aller IT-Systeme muss auf angemessene Ausfallsicherheit und entsprechende Datensicherung und/oder den Einsatz von Archivsystemen geachtet werden. Es empfiehlt sich, z.B. beim Betrieb einer Terminalserverfarm, ergänzende PCs einzusetzen sowie USV-versorgte „Notfall-Arbeitsplätze“ für administrative Tätigkeiten in Serverraumnähe zu betreiben. So kann bei einem Ausfall der Daten-Infrastruktur dennoch auf zentrale Systeme zugegriffen werden.

Das Netzwerk selbst darf nur hinter einer Firewall (mit DMZ für etwaige Anwendungen, die von extern erreichbar sein müssen) betrieben werden. Ein eventueller Fernzugriff ist zu kontrollieren und nur auf Bedarf zu aktivieren. Es empfiehlt sich, mindestens ein abgesichertes Netzsegment, möglichst ohne Internetzugang, speziell für medizinische Systeme einzurichten.

Wichtig ist, Kenntnis von etwaigen Störungen zeitnah zu erhalten (z.B. über System-Managementsysteme), das Vorhalten relevanter Ersatzteile bzw. redundanter Systeme und der Abschluss notwendiger Wartungs- & Supportverträge sowie ggf. Versicherungen für unternehmenskritische IT-Systeme.

Exemplarische Prüffragen:

- Ist ein unterbrechungsfreier Betrieb von Servern gewährleistet?
- Ist eine Datensicherung der Server im Einsatz und wird sie regelmäßig überprüft?
- Ist ein Langzeitarchiv im Unternehmen etabliert?
- Ist der Personenkreis der Administratoren eingegrenzt?
- Sind die Datenzugriffsmöglichkeiten auf das erforderliche Mindestmaß beschränkt?
- Sind die Regeln auf der Firewall klar definiert und grenzen den Netzwerkverkehr auf den jeweiligen Anwendungsfall ein?
- Sind VLANs im Netzwerk etabliert und klar definiert?
- Wie sind die Netzwerke vor unbefugter Nutzung geschützt?
- Sind die nach außen angebotene Daten, Dienste & Programmfunktionalitäten auf das erforderliche Mindestmaß beschränkt?
- Erfolgt der Datenaustausch nur über vertrauenswürdige Kanäle?
- Werden Störungen an die verantwortlichen Personen automatisiert gemeldet?
- Ist ein Malwareschutz zugelassen und aktiviert?
- Existiert für Anwendung und System jeweils ein Rechte & Rollenkonzept?
- Sind die Administratorenteams redundant ausgelegt?
- Werden ausgeschiedene Mitarbeiter zeitnah gesperrt?
- …

5.5 Konfiguration der Endgeräte

Die Endgeräte bringen allein aufgrund der hohen Zahl ein hohes Gefährdungspotential mit sich. Zu Endgeräten zählen aus Sicht des BAK MV nicht nur PCs, sondern auch z.B. Drucker, Tablets, Smartphones sowie weitere Geräte der Medizintechnik.

Eine Bestandsaufnahme sollte von allen beteiligten Abteilungen gemeinsam erfolgen.

Exemplarische Prüffragen:

- Wie viele Endgeräte werden im Klinikum betrieben?
- Welche davon unterliegen einer zentralen Administration?
- Benötigen die installierten Anwendungen besondere Rechte auf dem PC?
- Welche Client-Systeme können nach zentralen Vorgaben einheitlich konfiguriert werden?
- Verschlüsselung der lokalen Datenträger (zumindest für mobile IT-Systeme)
- Wie werden die Schnittstellen (USB, CD/DVD etc.) geschützt?
- An welchen Rechnern darf keine stetige Aktualisierung des Betriebssystems erfolgen?
- An welchen Rechnern kann die Deinstallation nicht mehr genutzter Systeme und Programme erfolgen?
- Kann der Betrieb nur im Haus zugelassener Anwendungen sichergestellt werden?
- Erfolgt der Einsatz eines Virenschutzes und lokaler Firewall?
- Ist Zugang nur mit eindeutigem personenbezogenen Benutzernamen und Passwort möglich?

- Wird eine sinnvolle Qualität sowie feste Änderungsintervalle des Passwortes beachtet?
- Erfolgt ein Auto-Logout nach inaktiver Zeit?
- Werden Accounts nach mehrmaligen Fehlversuchen gesperrt?
- ….

6 Sensibilisierung IT-Sicherheit

Ein wichtiger Baustein einer funktionierenden Informationssicherheit ist die regelmäßige Bewusstmachung der unterschiedlichen Gefährdungsszenarien eines IT-Systems. Die korrekte Anwendung technischer Sicherungsmaßnahmen ist dabei ebenso notwendig wie die Sensibilisierung der Anwender für z.B. social engineering.

Ein gutes Instrument zur Verbesserung der Sensibilität gegenüber Gefährdungen sind regelmäßige Schulungen der Anwender. Idealerweise sind IT-Sicherheitsschulungen Teil der IT-Anwenderschulungen und werden als Element des Gesamtprozesses verstanden. Bewährt haben sich Schulungsmaßnahmen als Voraussetzung für die Zugangsberechtigung an die verwendeten Systeme. Nur wer die Schulungsmaßnahmen besucht hat, bekommt auch einen Zugang zum IT-System.

Die stetige Weiterentwicklung von Gefährdungen der IT-Sicherheit machen Auffrischungsschulungen notwendig. Diese sollten mit für die Mitarbeiter relevanten Inhalten verknüpft werden, wie z.B. „Sicheres Surfen im Internet“, „Schutz vor E-Mail-Phishing“ oder „Sicherer Umgang mit privaten Geräten im dienstlichen Alltag“.

Ein wesentlicher Faktor der Verstetigung von IT-Sicherheitsschulungen liegt in der vorbehaltlosen Unterstützung der Maßnahmen durch die Führung des Unternehmens. Besonders eindrückliches Verständnis für IT-Sicherheit ist durch sog. Livehacking durch externe Berater (ggf. in Zusammenhang mit einem Penetrationstest) zu erzielen.

Weiter bieten sich gemischte Teilnehmerkreise für eine IT-Sicherheitsschulung an. Die unterschiedlichen Betrachtungswinkel zum Thema IT-Sicherheit fördern das Verständnis untereinander und tragen zu einem gemeinsamen Gesamtbild der Gefährdungslage bei.

IT-Administratoren sollten unabhängig von den allgemeinen Veranstaltungen regelmäßig geschult werden und über die aktuelle Entwicklung der IT-Sicherheitsgefährdungen informiert sein.

Exemplarische Prüffragen:

- Werden die Anwender durch Schulungen in regelmäßigen Intervallen auf Gefährdungen eines IT-Systems hingewiesen?
- Werden die Schulungen durch die Führung des Unternehmens unterstützt?
- Wird auch die Unternehmensleitung entsprechend sensibilisiert?
- Werden die IT-Administratoren unabhängig von den Anwendern regelmäßig geschult?
- Informieren sich die IT-Administratoren selbstständig über IT-Sicherheitsgefährdungen?
- Finden Lernerfolgskontrollen statt?
- ..

7 Erweiterung von Beschaffungs- und Ausschreibungsunterlagen

Vor der Beschaffung von IT-Hard- und Software (s. Kap.4) sollten Leistungsverzeichnisse erstellt werden, die das zu beschaffende Produkt genauestens beschreiben.

Durch die Erweiterung der Leistungsverzeichnisse um IT-Sicherheitskriterien können und müssen die Produkte auch aus diesem wichtigen Blickwinkel beurteilt werden.

Neben den technischen Anforderungen sind auch Mitwirkungsleistungen des Herstellers bei der Einbringung seines Systems in die bestehende IT-Infrastruktur in Bezug auf Informationssicherheit zu eruieren.

Exemplarische Prüffragen:

- Werden vom Hersteller Informationen zur IT-Sicherheit des Systems zur Verfügung gestellt?
- Können im Krankenhaus existierende Mindeststandards zur IT Sicherheit erfüllt werden?
- Werden Unterstützungsleistungen bei der Einbindung in ein Medizingerätenetz (EN/DIN 80001) angeboten?
- Wie erfolgt die Einbindung in die Gebäude- und Sicherheitstechnik der Klinik?
- Wie wird durch den Betrieb die vorhandene Kommunikations- und Medientechnik beeinflusst?
- …

Durch Bewertung der sicherheitsrelevanten Anforderungen und Ausschluss der Systeme, die diesen nicht genügen, kann die Informationssicherheit in einem Unternehmen in deutlichem Maße verbessert werden.

Ein Betreiber kann einen Zugewinn an Informationssicherheit mit dem Betrieb von sicherheitszertifizierten Produkten erzielen.

In Kapitel 13 finden Sie einen Verweis auf eine Veröffentlichung des UP KRITIS, in der bereits Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in kritischen Infrastrukturen enthalten sind. Diese Empfehlungen sind als Grundlage für (Vertrags)Verhandlung zwischen Betreibern Kritischer Infrastrukturen und deren Lieferanten, Herstellern oder Dienstleistern gedacht.

8 Organisatorische Konzepte für einen IT-Sicherheitsvorfall

Trotz aller Sicherungsmaßnahmen ist ein IT-Sicherheitsvorfall nicht zu 100% zu verhindern. Es gilt daher, bereits im Vorfeld die notwendigen Schritte und Maßnahmen zu definieren, um handlungsfähig zu sein. Alle Anwender sollten daher in Nicht-IT-gestützten Ausfallverfahren (Papierersatzverfahren) unterwiesen sein.

Auf der Basis der vorgenannten Kriterien ist das IT-Sicherheitsmanagement zusammen mit der Geschäftsführung in der Lage, die relevanten kritischen IT-Systeme zu identifizieren. Die Einteilung in

unterschiedliche Kritikalitäten ermöglicht gezielte Maßnahmen, um einzelne Systeme, aber auch das Gesamtsystem, bei einem Vorfall abzusichern bzw. betroffene Systeme/Systembereiche zu isolieren.

Die zu erstellenden IT-Notfallpläne sollten unbedingt als Ergänzung zu den ohnehin notwendigen Katastrophen- und Notfallplänen etabliert werden. Je nach Schwere des IT-Sicherheitsvorfalls kann die Notwendigkeit der Aktivierung des Notfall- oder Wiederanlaufplans notwendig werden.

Konkret sind dazu Betriebsdokumentationen mit wahrscheinlichen Störungsszenarien, Ersatzprozessen und Wiederherstellungsdokumentation zu erstellen und regelmäßig auf Anwendbarkeit und überprüfen.

Exemplarische Prüffragen:
- Sind kritische IT-Systeme im Unternehmen definiert?
- Sind Notfallpläne / Notfallverfahren erstellt und bekannt?
- Sind Ersatzverfahren, die bei einem IT-Ausfall zum Einsatz kommen, etabliert und bekannt?
- Gibt es Ersatzprozesse und Wiederanlaufpläne?
- Finden regelmäßige Audits im Bereich IT-Sicherheit statt?
- ..

9 Frühzeitige Einbindung bei Projekten

Bei der Planung von Projekten, die bei Umsetzung mit der Nutzung von IT-Infrastruktur einhergehen, ist das Informationssicherheitsmanagement – wie grundsätzlich die Verantwortlichen für den Betrieb der IT-Infrastruktur – frühzeitig mit einzubeziehen. Nur auf diese Weise können die Anforderungen an eine sichere Informationsinfrastruktur und -verarbeitung angemessen berücksichtigt werden.

Exemplarische Prüffragen:
- Werden die IT-Verantwortlichen und die Verantwortlichen für das Informationssicherheitsmanagement bei der Planung von Projekten rechtzeitig eingebunden?
- Werden sicherheitsrelevante Aspekte bei der Planung von Projekten berücksichtigt?
- Gibt es ein abgestimmtes Freigabeverfahren für einzuführende Produkte?
- …

10 Kommunikationskultur

Um angemessen Cybergefahren vorzubeugen bzw. auf Cyberangriffe reagieren zu können, sollte im Unternehmen eine stringente Kommunikationskultur etabliert werden. Dabei hilft es, sich den folgenden, grundsätzlichen Kommunikations-Fragen zu stellen:

- Werden die richtigen Personen informiert?
- Ist die Information verständlich?
- Erfolgt die Information sachgerecht?
  z.B. Warnmeldungen als popup, Hintergrundinformationen als Ergänzung
- Haben die Informierten Möglichkeiten zur Rückkopplung?
- Kann auf bisherige Informationen zurückgegriffen werden?

- Erfolgt die Information bei Veränderungen mit angemessenem zeitlichen Vorlauf und wird diese kurz vor der Veränderung aktualisiert bzw. in Erinnerung gebracht?
- …

11 Richtlinien und Konzepte

Um der Komplexität der Umsetzung von Informationssicherheit an einem Krankenhaus gerecht werden zu können, bietet sich die Erstellung bzw. Überarbeitung von Richtlinien und Konzepten für einen sicheren Betrieb von IT-Systemen an.

Exemplarische Prüffragen:
Gibt es

- eine IT-Strategie?
- eine Leitlinie/Dienstanweisung zur Informationssicherheit für alle Anwender?
- ein Datenschutzkonzept, incl. Zugriffsschutz auf IT-Systeme?
- eine Klassifizierung von Daten?
- ein Datensicherungskonzept?
- eine IT-Sicherheitskonzeption?
- ein Risikomanagement?
- ein Krisenmanagement?
- den Geregelten Einsatz von Anwendungen und Apps?
- eine Sicherheitsrichtlinie zur Nutzung mobiler Datenträger?
- eine Dienstanweisung/Regeln zur Nutzung von Internetzugängen und E-Mail?
- …

Die Aufteilung der Richtlinien, Vorgaben und Handlungsempfehlungen auf die verschiedenen Dokumente wird sich in den Häusern nach den jeweils vorhandenen Strukturen richten. Einiges ist vielleicht schon per Betriebsvereinbarung geregelt, diese lässt sich allerdings i.d.R. schwerer anpassen als eine Dienstanweisung.

12 Schlussbemerkung

Der Einsatz von hochverfügbaren Komponenten, ein permanentes Monitoring des Systemzustands, regelmäßige Datensicherung und ausgefeilte Notfallpläne sind die Basis für den verantwortungsvollen Betrieb einer Krankenhaus IT-Infrastruktur, eingebettet in ein effektives – möglichst schlankes – IT-Sicherheitskonzept.

Den technischen Instrumentarien und organisatorischen Maßnahmen müssen zwingend Mitarbeiter mit notwendiger Kompetenz zugeordnet werden.

Entscheidend für eine erfolgreiche Etablierung einer Informationssicherheit im Krankenhaus ist die Umsetzung der Regelungen im täglichen Umgang mit den IT-Systemen. Richtlinien und Handlungsempfehlungen müssen gelebt werden, damit sie greifen. Vielfach wird dies Änderungen in der Unternehmenskultur erfordern.

Andererseits kann heute ein Krankenhaus seine Kernkompetenzen nur dann effektiv bereitstellen, wenn es seine IT-Systeme gegen Ausfälle oder Fehlfunktionen bestmöglichst absichert.

13 Literatur, ergänzende Dokumente

- Broschüre "IT-Sicherheitsgesetz"; Bundesamt für Sicherheit in der Informationstechnik - BSI; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=5
- Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG; Bundesamt für Sicherheit in der Informationstechnik - BSI; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Orientierungshilfe_8a_3.pdf?__blob=publicationFile&v=4
- Überblick IT-Grundschutz - Entscheidungshilfe für Manager; Bundesamt für Sicherheit in der Informationstechnik - BSI; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Ueberblick-IT-Grundschutz.pdf?__blob=publicationFile&v=3
- Broschüre „Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT“, Management-Kurzfassung; Bundesamt für Sicherheit in der Informationstechnik - BSI; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/RisikoanalyseKrankenhaus.pdf?__blob=publicationFile&v=4
- Leitfaden „Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT“; Bundesamt für Sicherheit in der Informationstechnik - BSI; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/RisikoanalyseKrankenhausIT_Leitfaden_pdf.pdf?__blob=publicationFile&v=2
- Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) - BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958); https://www.gesetze-im-internet.de/bundesrecht/bsi-kritisv/gesamt.pdf
- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) - BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das durch Artikel 3 Absatz 6 des Gesetzes vom 18. Juli 2016 (BGBl. I S. 1666) geändert worden ist; https://www.gesetze-im-internet.de/bundesrecht/bsig_2009/gesamt.pdf
- BSI IT-Grundschutz; https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
- IT-Security Standards; https://www.security-standards.de/ITSecurityGrid.html
- Anforderungen an Lieferanten; http://www.kritis.bund.de/SubSites/Kritis/DE/Publikationen/Sektoruebergreifend/UP%20KRITIS/160718_Anforderungen_an_Lieferanten.html
- ISO/IEC 27K -Normenfamilie der Informationssicherheit
- DIN EN 80001-1 - Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten
- ISO/TR 11633-1 - Informationssicherheitsmanagement für die Fernwartung für Medizinprodukte und Informationssysteme im Gesundheitswesen

14 Abkürzungen

B3S	branchenspezifische Sicherheitsstandards
BAK MV	Branchenarbeitskreis Medizinische Versorgung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
BSI-KritisV	BSI-Kritis-Verordnung
CERT	Computer Emergency Response Team (Computersicherheits-Ereignis- und Reaktionsteam)[4]
DSGVO	EU-Datenschutzgrundverordnung
ISB	Informationssicherheitsbeauftragter
ISMS	Information Security Management Systems
ITSiG	IT-Sicherheitsgesetz
KRITIS	Kritische Infrastruktur

[4] https://de.wikipedia.org/wiki/Computer_Emergency_Response_Team

15 Traffic Light Protocol

Im Rahmen des zugrunde liegenden Informationsverbundes UP KRITIS ist der Austausch von nicht-öffentlichen und vertraulichen Informationen notwendig. Das Traffic Light Protocol (TLP) ist eine Vereinbarung zum Schutz dieser Informationen. Das TLP regelt nicht den Schutz staatlich geheim zu haltender Informationen.

TLP-White: Unbegrenzt
Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP-White ohne Einschränkungen frei weitergegeben werden.

TLP-Green: Organisationsübergreifende Verteilung
Informationen in dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Information darf jedoch nicht veröffentlicht werden.

TLP-Amber: Organisationsinterne Verteilung
Informationen in dieser Stufe dürfen innerhalb der Organisationen der Empfänger weitergegeben werden, jedoch nur auf der Basis „Kenntnis, nur wenn nötig“. Der Informationsersteller muss zusätzlich beabsichtigte Einschränkungen der Weitergabe klar spezifizieren.

TLP-Red: Persönlich, nur für benannte Empfänger
TLP-Red-Informationen sind auf den Kreis der Anwesenden in einer Besprechung oder einer Video-/Telefonkonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. In den meisten Fällen werden **TLP-Red**-Informationen mündlich oder persönlich übergeben.

Weitere Details unter www.upkritis.de