Langfassung des Beitrags „Medizintechnik + IT: Mit Sicherheit wichtig“ von Armin Gärtner, aus E-HEALTH-COM Ausgabe 2/2011, S. 22-26

conhIT-Update vom 7.4.2011

Hersteller-Informationen gemäß IEC 80001 – Ein Vorschlag

Im Herbst 2010 ist der internationale Entwurf der Norm 80001 weltweit angenommen worden und zur Medica 2010 als IEC 80001 in der englischsprachigen Form erschienen. Im Sommer 2011 wird die Norm als sogenannter Weißdruck mit der Nummerierung VDE 0756-1 erscheinen und kann damit spätestens angewendet werden. Eine der wesentlichen Fragestellung dreht sich um die Informationen, die ein Hersteller eines vernetzbaren bzw. in ein IT-Netzwerk zu integrierendes Medizinprodukts dem Betreiber zur Verfügung stellen muss bzw. sollte. Der folgende Beitrag beinhaltet einen ersten Vorschlag, welche Informationen und in welcher Form ein Hersteller dem Betreiber liefern kann und sollte.

1. Ausgangssituation

Die Integration von Medizinprodukten (Modalitäten, Software als eigenständiges Medizinprodukt) in ein IT-Netzwerk eines Krankenhauses kann zu Gefahren und Gefährdungen führen, die die Sicherheit und Funktionsfähigkeit des integrierten Medizinproduktes beeinflussen oder sogar erheblich stören können. Dadurch können sogar Patient, Anwender und Dritte direkt/indirekt beeinträchtigt oder sogar geschädigt werden.

Der gemäß Quelle 1 geschilderte Befall eines Krankenhaus-IT-Netzwerkes durch Malware (Schadsoftware) zeigt exemplarisch die Gefährdungspotenziale medizinischer Netzwerke und somit auch von Medizinprodukten. Daher besteht die Notwendigkeit, die Sicherheit und den Schutz von Medizinprodukten, die in IT-Netzwerke integriert werden, sowohl auf der Herstellerseite als auch auf der Betreiberseite permanent zu verbessern.

Es handelt sich dabei um einen iterativen Prozess, bei dem Hersteller und Betreiber gemeinsam die Informationsnotwendigkeiten klären und voneinander lernen können, wie und welche Sicherheits- und Schutzbedürfnisse vernetzter Medizinprodukte und medizinischer Netzwerke gemeinsam sicher zu stellen sind.

2. Grundlagen für Hersteller-Informationen zu ihren Medizinprodukten

Wo finden sich in den Regularien (Richtlinien, Normen) und speziell in der Norm IEC 80001 Grundlagen, Hinweise und Anforderungen an Hersteller-Informationen für den Betreiber über die Vernetzung bzw. Integration in ein IT-Netzwerk (medizinisches Netzwerk)?

Anforderungen an Informationen des Herstellers sind in folgenden Regularien und Normen niedergelegt:

- EG-Richtlinie Medical Devices Directive 93/42/EWG (MDD), Anhang I Grundlegende Anforderungen, Abschnitt 13
- IEC 80001, Kapitel 3.5

- DIN EN 60601-1 3rd, Kapitel 14.13 – informativer Anhang H.6

Um ein Medizinprodukt in Verkehr zu bringen, definiert ein Hersteller für das vorgesehene Produkt eine medizinische Zweckbestimmung gemäß § 3 Abs. 10 des Medizinproduktegesetzes (MPG). Diese Zweckbestimmung stellt die Basis für die Risikoklassifizierung und für den Einsatz des Produktes durch den Betreiber bzw. dessen Anwender dar und beinhaltet damit auch prinzipiell die vorgesehene Vernetzung.
Zum Nachweis der Konformität eines Medizinproduktes mit der zutreffenden EG-Richtlinie muss der Hersteller das entsprechende Konformitätsverfahren durchführen. Dies bedeutet, dass er die Grundlegenden Anforderungen nachweislich erfüllen muss. Die Grundlegenden Anforderungen gemäß Anhang I der EG-Richtlinie in der Fassung 2007/47/EG verlangen in Abschnitt 13 vom Hersteller, folgende Informationen bereit zu stellen:

13. Bereitstellung von Informationen durch den Hersteller

13.1. Jedem Produkt sind Informationen beizufügen, die — unter Berücksichtigung des Ausbildungs- und Kenntnisstandes des vorgesehenen Anwenderkreises — die sichere und ordnungsgemäße Anwendung des Produkts und die Ermittlung des Herstellers möglich machen.
Diese Informationen bestehen aus Angaben auf der Kennzeichnung und solchen in der Gebrauchsanweisung.

13.4. Wenn die Zweckbestimmung eines Produkts für den Anwender nicht offensichtlich ist, muss der Hersteller diese deutlich auf der Kennzeichnung und in der Gebrauchsanweisung angeben.

13.5. Die Produkte und ihre abnehmbaren Bauteile müssen — gegebenenfalls auf der Ebene der Produktlose und soweit vernünftigerweise praktikabel — identifizierbar sein, damit jede geeignete Maßnahme getroffen werden kann, um mögliche Risiken im Zusammenhang mit den Produkten und ihren abnehmbaren Bauteilen festzustellen.

13.6. Die Gebrauchsanweisung muss nach Maßgabe des konkreten Falles folgende Angaben enthalten:
c) bei Produkten, die zur Erfüllung ihrer Zweckbestimmung mit anderen medizinischen Einrichtungen oder Ausrüstungen kombiniert oder an diese angeschlossen werden müssen: alle Merkmale, soweit sie zur Wahl der für eine sichere Kombination erforderlichen Einrichtungen oder Ausrüstungen erforderlich sind;
d) alle Angaben, mit denen überprüft werden kann, ob ein Produkt ordnungsgemäß installiert worden ist und sich in sicherem und betriebsbereitem Zustand befindet, sowie Angaben zu Art und Häufigkeit der Instandhaltungsmaßnahmen und der Kalibrierungen, die erforderlich sind, um den sicheren und ordnungsgemäßen Betrieb der Produkte fortwährend zu gewährleisten;

Dies bedeutet, dass der Hersteller gemäß den Grundlegenden Anforderungen der EG-Richtlinie MDD

- eine Zweckbestimmung
- eine Gebrauchsanweisung (GA)

und sonstige Informationen mitliefern muss, um z. B. die sichere Kombination von Medizinprodukten mit anderen Produkten zu ermöglichen.
Aus den Formulierungen der Grundlegenden Anforderungen ergeben sich durchaus umfangreiche Informationsverpflichtungen für Hersteller, die nachfolgend beispielhaft diskutiert werden.

3. Informationen nach IEC 80001
IEC 80001 definiert einen (Risikomanagement-)Prozess, mit dem der Betreiber seine Sorgfaltspflichten beim Betrieb vernetzter Medizinprodukte in einem IT-Netzwerk gemäß Medizinproduktegesetz (MPG) und Medizinproduktebetreiberverordnung (MPBetreibV) bezüglich der Sicherheit und des Schutzes (sowie Effektivität) von Patienten, Anwendern und Dritter nachkommen und belegen kann. Um diese Aufgabe wahrnehmen zu können, benötigt der Betreiber entsprechende Informationen vom Hersteller eines zu integrierendes Medizinproduktes.
Die Norm wird als reine Prozessnorm angesehen, d. h. sie richtet sich weitestgehend an den Betreiber von vernetzbaren Medizinprodukten. Das bedeutet, der Betreiber muss aktiv werden, die Normenanforderungen umzusetzen. Dennoch entlässt die IEC 80001 Hersteller nicht völlig aus der Verantwortung, indem sie dem Hersteller vorgibt, dem Betreiber Informationen zur Verfügung zu stellen, die dieser benötigt, vernetzbare Medizinprodukte sicher in einem medizinischen Netzwerk zu betreiben.

In Abschnitt 1 (Anwendungsbereich, Zweck) der Norm wird zum Zweck (Scope) ausgeführt:
"This standard applies to RESPONSIBLE ORGANIZATIONS, MEDICAL DEVICE manufacturers and providers of other information technology for the purpose of RISK MANAGEMENT of an ITNETWORK incorporating MEDICAL DEVICES as specified by the RESPONSIBLE ORGANIZATION."

Damit richtet sich die Norm auch an Hersteller, die gemäß Abs. 3.5 Informationen zur Verfügung stellen können:

3.5 Medical Device manufacturer(s)
Pursuant to applicable regulations and relevant standards, each medical device manufacturer shall make applicable accompanying documents to the responsible organization that describe the intended use and give instructions necessary for the safe and effective use of the medical device.

Sinngemäß lautet dieser Abschnitt in deutscher Übersetzung:
In Übereinstimmung mit gültigen Vorschriften und den entsprechenden Normen muss der Medizinprodukte-Hersteller der verantwortlichen Organisation Begleitpapiere zur Verfügung stellen, die die Zweckbestimmung beschreiben und die Anweisungen für den sicheren und effektiven Gebrauch des Medizinproduktes geben.

Dieser Abschnitt referenziert sehr deutlich auf die vorab zitierten Grundlegenden Anforderungen der EG-Richtlinie MDD.

Kapitel 3.5 der Norm konkretisiert diese Anforderungen bezüglich von Informationen, die der Hersteller zu der Integration eines Medizinproduktes in das IT-Netzwerk des Betreibers zur Verfügung stellen muss. Diese Angaben referenzieren auf die Zweckbestimmung des Medizinproduktes, auf die Leistungsmerkmale und

Konfiguration des IT-Netzwerkes bis hin zu möglichen Angaben des Routing durch das Betreiber-Netzwerk.

- Sicherheitsspezifikationen: Angaben, unter welchen Voraussetzungen ein Medizinprodukt in ein Netzwerk zu integrieren ist, d. h. was muss der Betreiber sicherstellen, z. B. Installation in einem Subnetzwerk (VLAN), Sicherheitskonzept in Form einer Firewall usw.
- Angaben und Anforderungen bezüglich der Leistungsfähigkeit des IT-Netzwerkes, damit das zu integrierende Medizinprodukt bestimmungsgemäß funktionieren kann (z. B. Netzwerk-Datenübertragungsrate, WLAN-Standard usw. usw.)
- Technische Spezifikationen des Netzwerkanschlusses des Medizinproduktes
- Beschreibung der Datenübertragung (Informationsfluss) zwischen dem Medizinprodukt, dem medizinischen IT-Netzwerk und anderen Geräten im IT-Netzwerk. Gegebenenfalls muss auch das erforderliche Routing angegeben werden, wenn es Einfluss auf das IT-Netzwerk hat bzw. von Bedeutung für die wesentlichen Eigenschaften des IT-Netzwerkes ist.
- Der Hersteller sollte Angaben in Form einer Liste zu möglichen Risiken des Einsatzes des Medizinproduktes erstellen, wenn das medizinische Netzwerk eines Betreibers nicht die notwendigen Leistungsmerkmale erbringt, die für den bestimmungsgemäßen Einsatz und Leistung des Medizinproduktes erforderlich sind.
    - Beispiel: Was passiert, wenn zeitkritische Vitalparameteralarme eines Patientenmonitorings nicht rechtzeitig über das Netzwerk übertragen werden, weil das Netzwerk bezüglich der erforderlichen Datenübertragungsrate unterdimensioniert und/oder zeitweise überlastet ist?

Weder die IEC 80001 noch die Norm DIN EN 60601-1 3rd mit Kapitel 14.13 mit Anhang H.6 (siehe Abschnitt 4) enthalten konkrete Informationen bzw. Vorschläge bezüglich produktspezifischer Informationen.
Die notwendigen Informationen, die ein Betreiber benötigt, können sich durchaus von Produktkategorie zu Produktkategorie sehr unterscheiden.
Das Gefährdungspotenzial eines bildgebenden Ultraschallgerätes ist in Hinblick auf die Patientensicherheit deutlich niedriger einzuschätzen als das Gefährdungspotenzial eines Linearbeschleunigers.
Art und Umfang der notwendigen Informationen für die Integration eines Medizinproduktes in ein IT-Netzwerk hängen also von der Produktkategorie und auch von dem medizinischen bzw. technischen Anforderungsprofil des Betreibers ab. Dies bedeutet, dass Hersteller und Betreiber sich durchaus im Rahmen der von der IEC 80001 vorgeschlagenen Zuständigkeitsvereinbarung (Responsibility Agreement) verständigen können, welche weiteren Informationen ausgetauscht bzw. zur Verfügung gestellt werden (müssen), die ein Hersteller eh bereits liefert und/oder anbietet.

4. Informationen gemäß DIN EN 60601-1 3rd Kapitel 14.13

Im Laufe der Entwicklung und Erarbeitung/Diskussion des Normenentwurfes hat sich herauskristallisiert, dass Kapitel 14.13 der DIN EN 60601-1 3rd als eine Basis für die von der IEC 800001 vorgeschlagenen Informationen eines Herstellers angesehen wird.

Das Kapitel 14.13 und vor allem der informative Anhang H.6 Netzwerk/Datenverbund der Norm enthalten Beispiele von Informationen und Angaben, die ein Hersteller von Medizinprodukten zur Verfügung stellen muss bzw. auf die sich der Betreiber vor der Beschaffung eines vernetzbaren Medizinproduktes beziehen sollte.
Die Norm definiert ein IT-Netzwerk/Datenverbund als jedes Mittel, das zum Senden oder zum Empfangen von Informationen zu oder von anderen Geräten entsprechend den Spezifikationen des Herstellers eingesetzt wird.
Wird ein Medizinprodukt mit anderen Geräten durch ein IT-Netzwerk und/oder Datenverbund verbunden, das außerhalb der Verantwortung des Medizinprodukte-Herstellers liegen, muss die technische Beschreibung des Herstellers/Lieferanten gemäß Abschnitt 14.13 der DIN EN 60601-1 3rd folgende inhaltliche Angaben und Hinweise enthalten:

1. Ein Hersteller muss die notwendigen Anforderungen an das Netzwerk des Betreibers definieren, damit das zu vernetzende Medizinprodukt seine Zweckbestimmung erfüllen kann.
2. Er muss weiterhin die möglichen Risiken beschreiben, die auftreten können, wenn das Betreiber-IT-Netzwerk nicht in der Lage ist, die notwendigen Leistungen zu erbringen.
3. Er muss den Betreiber darauf hinweisen, dass die Integration eines Medizinproduktes in ein IT-Netzwerk, das auch andere Geräte enthält, zu neuen, vorher nicht bekannten Gefährdungen für den Patienten, Anwender oder Dritte führen könnte.
4. Er muss den Betreiber darauf hinweisen, dass der Betreiber für diese Gefährdungen ein Risikomanagement durchführen sollte und dass jede weitere Änderung zu neuen Gefährdungen führen und daher zusätzliche Risikoanalysen erfordern kann.
5. Als Änderungen eines IT-Netzwerkes werden aus Sicht der Norm folgende Maßnahmen und Aktivitäten gesehen:
    a. Änderungen an der Konfiguration des IT-Netzwerkes;
    b. Anschließen zusätzlicher Komponenten an das IT-Netzwerk;
    c. Entfernen von Geräten/Komponenten aus dem IT-Netzwerk;
    d. „Software/Hardware-Update“ von Geräten, die mit dem IT-Netzwerk verbunden sind;
    e. „Software/Hardware-Upgrade“ von Geräten, die mit dem IT-Netzwerk verbunden sind.
    f. U.a.

Es ist aber jedem Betreiber freigestellt, im Rahmen einer Beschaffungsmaßnahme mit dem bzw. den Anbieter(n) von Medizinprodukten zu vereinbaren, weitere Informationen zur Verfügung zu stellen, die über die Mindestanforderungen des Kapitels 14.13 der DIN EN 60601-1 3rd hinausgehen. Dazu schlägt der Normentwurf eine vertragliche Vereinbarung vor, mit der die beiden Parteien eine Zuständigkeits-/Verantwortlichkeitsvereinbarung bzw. Informationsvereinbarung treffen können.

5. Beispiele für Herstellerinformationen

Mittlerweile haben Hersteller bereits begonnen, erste spezifische Informationen zur Vernetzung ihrer Produkte in ein Betreiber IT-Netzwerk und bezüglich Virenschutz zur Verfügung zu stellen. Nachfolgend werden einige Beispiele vorgestellt.

PACS (Picture and Communication System)

Hersteller von PACS-Lösungen als Medizinproduktsoftware erklären in Form einer Stellungnahme, dass sie folgende Unterlagen dem Kunden für ihr Produkt zur Verfügung stellen:

- *EG-Konformitätserklärung*
- *DICOM Conformance Statement (englisch)*
- *HL7 Conformance Statement (englisch)*
- *HL7 Conformance Statement (englisch)*
- *Funktions- und Interoperabilitätszertifikat im Rahmen der elektronischen Bild-Archivierung (PACS)*

In den Handbüchern sind die Zweckbestimmung des Medizinproduktes PACS-Software (Darstellung von Bilddaten zur Befundung), die geforderten Leistungsmerkmale des IT-Netzwerkes, die erforderlichen Konfigurationen des IT-Netzwerkes beschrieben.

Weitere Forderungen, wie z. B. die technischen Spezifikationen des Netzwerk-Interfaces, sind aufgrund der Software-Eigenschaft der PACS-Lösung nicht relevant. Besondere Restrisiken, die vom Betreiber gehandhabt werden müssten, sind uns nicht bekannt.
Bezüglich gelieferter Hardware erfüllt das Unternehmen die Forderungen, die an das Unternehmen als IT-Lieferant gestellt werden und versichert, dass die angebotene/verkaufte Hardware und Betriebssysteme die zum Betrieb der PACS-Lösung notwendigen Systemvoraussetzungen erfüllt und Unverträglichkeiten mit oder Einschränkungen bzgl. der PACS-Lösung nicht bekannt sind.
Alle technischen Beschreibungen und technischen Handbücher der Hardware- und Betriebssystem-Hersteller werden mit der Lieferung an den Kunden übergeben.

WLAN-Betrieb
Für den Betrieb eines Systems wie eines mobilen Patientenmonitors mit einer WLAN-Anbindung kann ein Hersteller beispielhaft folgende Sicherheits-Informationen zur Verfügung stellen:

- Unterstützte Standards IEEE 802.11a, 802.11b, 802.11g
- Sicherheitsstandards WPA2™-PSK; WPA2-Enterprise; Advanced Encryption Standard (AES)/802.11i; 802.1x Certificate-based authentication (EAP-TLS, TTLS, PEAP)
- Authentifizierungsmethoden RADIUS 802.1x;Pre-shared Key (PSK)
- usw. usw.

Schutz vor elektronischen Viren bei Netzwerkanbindung von aktiven Medizinprodukten
Der Hersteller stellt in seinen Unterlagen zum Thema Virenschutz folgende detaillierte Informationen für den Betreiber zur Verfügung (auszugsweise):
In einem vernetzbaren Laborgerät als Medizinprodukt nach der IvD-Richtlinie wird Windows XP als Betriebssystem eingesetzt. Die in diesem Betriebssystem eingesetzte Firewall ist aktiviert und alle nicht verwendeten Ports sind geblockt. Dies bedeutet, dass nur ein Port offen ist, um einen Remote-Zugriff des Programms NetOp (Remote Control Funktionalitäten) zu ermöglichen. Das Programm nutzt den Port 6502, der sowohl für TCP/IP als auch UDP geöffnet ist. Das Laborgerät kann nicht über ein Netzwerk „angepingt“ werden.

Alle anderen Funktionen und Services des Betriebssystems, auf das die Applikationssoftware des Laborgerätes zugreifen kann/könnte, sind abgeschaltet, also Remote registry und E-Mail-Funktion
Weiterhin steht die Windows Shell für den Bediener nicht zur Verfügung, das bedeutet, dass Programme wie der Explorer, das Control Panel und Shortcut Keys nicht verfügbar sind.
Der Hersteller gibt vor, dass nur durch ihn geschulte und autorisierte Anwender Software-Installationen jeglicher Art auf dem Produkt durchführen dürfen. Dies betrifft insbesondere vom Hersteller des Betriebssystems vorgesehene Patches, Release-Wechsel usw., die dem Betreiber nach Freigabe durch den Gerätehersteller auf CD übersandt werden. Der Hersteller des Laborgerätes gibt klar vor, dass das Gerät nicht in das automatische Patchmanagement einer Klinik eingebunden werden darf.

Wichtig ist der Hinweis, dass dieser Hersteller kontinuierlich die Bedrohungslage durch Malware für seine Produkte beobachtet. Stellt er fest, dass Malware seine Produkte bedroht, gibt er entsprechend validierte Patches über CD an den Betreiber frei.
Alle externen Medien wie Datenbanken, Server usw., die an das Laborprodukt angeschlossen werden, müssen vor dem Anschluss durch einen aktuellen Virenscanner gescannt werden, um das Gerät vor Malwarebefall zu schützen.

Hersteller definieren einen Virenschutz als Vorgabe, der im Rahmen von Wartungsverträgen mit Remote Zugriff auf die Modalitäten aktualisiert wird. Der Hersteller verpflichtet sich dabei, in einer definierten Zeit Patches des Virenschutzes zu validieren und für seine Produkte freizugeben, die dann auf Modalitäten des Betreibers gespeichert werden. Der Betreiber muss dann die Installation der Patches aktiv durchführen und z. T. Modalitäten herunter- und neu hochfahren.

Insgesamt gibt es derzeit (Frühjahr 2011) durchaus etliche positive Beispiele, wie Hersteller längst begonnen haben, ihre Informationsverpflichtung „nach IEC 8001“ nachzukommen. Es gibt aber auch Hersteller, die darauf verweisen, dass sie ihre Aktivitäten, entsprechende Informationen zur Verfügung zu stellen, erst nach „Inkrafttreten“ der IEC entwickeln, d.h. wenn die Norm als sogenannter Weißdruck in Deutschland vrsl. im Sommer 2011 erschienen ist.

6. Informationsnotwendigkeiten des Betreibers

Welche Informationsbedürfnisse hat nun der Betreiber? Was benötigt er für Informationen und Angaben, um seiner Verpflichtung, vernetzbare Medizinprodukte gemäß den Anforderungen des Medizinproduktegesetzes und der Medizinproduktebetreiberverordnung entsprechend sicher, geschützt und effektiv zu betreiben?
Der Betreiber braucht die formalen Unterlagen wie Zweckbestimmung, Konformitätserklärung, Gebrauchsanweisung und sonstige sicherheitsbezogene Informationen und Instandhaltungshinweise (siehe MPBetreibV § 2 Abs. 5) für seine Unterlagen und Dokumentation. Für die sichere und geschützte IT-Integration benötigt der Betreiber Informationen zu IT-Sicherheitskonzepten wie Firewall, Gateway-Lösungen sowie Angaben zum Virenschutz und Patchmanagement, damit ein Medizinprodukt im Netzwerk des Betreibers bestimmungsgemäß arbeiten kann.

Nachfolgend werden in Form einer Liste beispielhaft Informationen zusammengeführt. Diese Liste erhebt keinen Anspruch auf Vollständigkeit und kann nach Belieben ergänzt werden.
Mit dieser vorgeschlagenen Informationsliste kann der Betreiber eine Dokumentation für seine integrierten Medizinprodukte zusammenstellen und als Basis für das dann durchzuführende Risikomanagement nach Kapitel 4 der IEC 80001 nutzen.

Information-Angaben	Hinweis-Erläuterung
Formalrechtliche Informationen	
Zweckbestimmung des Medizinproduktes	i. d. R. in der Gebrauchsanweisung erhalten
Konformitätserklärung nach der/den zutreffenden Richtlinien	Nach Richtlinie MDD 93/42/EWG bzw. MPG für Medizinprodukte freiwillig, nach anderen EG-Richtlinien wie Maschinenrichtlinie besteht Verpflichtung der Mitlieferung
Systemerklärung § 12 MPG	Erklärung für ein Medizinproduktesystem mit allen Angaben für die im System kombinierten Geräte einschließlich Betriebssystem und Applikationssoftware
Gebrauchsanweisung	Sollte die technischen Angaben enthalten, die für die Integration erforderlich sind
Technische Beschreibung	Kann in der Gebrauchsanweisung enthalten sein
Sonstige sicherheitsbezogene Informationen	MPBetreibV § 2 Abs. 5
Instandhaltungshinweise	MPBetreibV § 2 Abs.5
Hinweise bezüglich der Kombination mit anderen Produkten	MPBetreibV § 5 Abs. 1
Technische Informationen	
Angaben zum Netzwerkbetrieb	
Angaben zur Hardware und Betriebssystem bei plattformunabhängigen Produkten wie Medizinprodukt Software	Gilt für plattformunabhängige Produkte wie Software (PACS u. a.)
Angaben zur Kombinierbarkeit des Medizinproduktes mit anderen Medizinprodukten und/oder Nichtmedizinprodukten	z. B. Hinweis: Anbindung an ein datenverarbeitendes System/IT-Netzwerk bestimmungsgemäß vorgesehen
Erforderlichenfalls Angaben zu Schnittstellenprotokollen	z. B. HL7
DICOM Conformance Statement	Wichtig: Conformance Statement reicht nicht für eine erfolgreiche Integration, aus! Schnittstellenkonzept erforderlich
HL7 Conformance Statement	Wichtig: Conformance Statement reicht nicht für eine erfolgreiche Integration, aus! Schnittstellenkonzept erforderlich
Funktions- und Interoperabilitätszertifikat	Nur für PACS

im Rahmen der elektronischen Bild-Archivierung (PACS)	
Sicherheitsinformationen	
Angaben zu Virenschutz und Patchmanagement	Wichtig: Herstellerkonformität des Medizinproduktes muss bei Verwendung eines Virenschutzes und des Patchmanagements erhalten bleiben!
Betriebssystem und Patchmanagement	Der Lebenszyklus eines Medizinproduktes von beispielsweise 10 Jahren umfasst ca. drei Betriebssystemwechsel mit laufenden Patches und Sicherheitspaketen.
Sicherheitstools	Einsatz von Überwachungstools, Software zur Kapselung von Rechnern und Software (Betriebssystem, Applikation)
Angaben für Sicherheitskonzept bzw. Integrationskonzept	Kann das Medizinprodukt problemlos in das IT-Netzwerk integriert werden oder sind Maßnahmen wie VLAN, Virenschutz, Abschirmung durch Firewall usw. erforderlich?
Angaben zu Remote Service: Remote Zugriff auf Medizin Rechner in einem Medizinproduktesystem?	i. d. Regel vertraglich geregelt, Klärung des Zugriffs im Rahmen des Datenschutzes
Angaben zur Nutzung von Netzwerkdruckern	Hersteller liefert Medizinproduktesystem mit lokalem Drucker, Betreiber will Netzwerkdrucker einsetzen
WLAN: Angaben zu Standards und Sicherheitsfunktionen	
Angaben zu Maßnahmen des Herstellers, mit denen er eine Viren-Kontamination von Notebooks/Sticks der Service-Techniker verhindert	
Spezifische Informationen nach IEC 80001 (evtl. redundant mit Sicherheitsinformationen)	
Zweckbestimmung des zu integrierenden Medizinproduktes	
Erforderliche Leistungsmerkmale des IT-Netzwerkes, in das das Medizinprodukt integriert werden soll	
Erforderliche Konfiguration des IT-Netzwerkwerkes, in das das Medizinprodukt integriert werden soll	
Beschreibung des vorgesehenen Datenaustausches zwischen Medizinprodukt und IT-Netzwerk sowie weiteren Geräten	Wichtig: DICOM- und HL7-Conformance reichen nicht aus, um einen erfolgreichen Datenaustausch zu ermöglichen. Auf Basis einer Workflowbeschreibung ist ein Schnittstellenkonzept zu erstellen.

Information des Herstellers über mögliche Gefährdungssituationen, wenn das IT-Netzwerk des Betreibers nicht über die notwendigen und geforderten Leistungsmerkmale verfügt und somit das zu integrierende Medizinprodukt seine Zweckbestimmung nicht erfüllen kann.	
Unterstützung IHE-TF „Audit Trail and Node Authentication“ (RFC-3881, ISO/ CD27789)	
Unterstützung „Software Identifikation Tags“ nach ISO/IEC 19770 incls. Individueller Betreiber-Erweiterung	

Tabelle 1: Beispiele für Informationen eines Herstellers (ohne Anspruch auf Vollständigkeit)

Diese u. a. Unterlagen/Informationen können in den Begleitpapieren eines Herstellers enthalten sein.
Wenn dies nicht ausreicht bzw. nicht der Fall ist, können Hersteller und Betreiber eine weiterführende Zuständigkeitsvereinbarung (Responsibility Agreement) abschließen, mit der geregelt werden kann, welche sonstigen Informationen darüber hinaus zur Verfügung gestellt werden können/sollen.

So kann/sollte z. B. folgende Fragestellung im Vorfeld einer Beschaffung geklärt werden:

1. Ein Hersteller bietet ein Medizinproduktesystem mit lokalem Drucker an, beispielweise EKG-System mit Laserdrucker. Kann dieser durch einen Druckerserver bzw. Netzwerkdrucker des Betreibers ersetzt werden? Welche Anforderungen an Druckerserver seitens eines Herstellers bestehen? Bleibt die Herstellerkonformität nach der Richtlinie MDD erhalten? Darf der Betreiber nur von Microsoft zertifizierte Treiber einsetzen? Wer überwacht das und hält nach, nur zertifizierte Treiber eingesetzt werden?

2. Wie sieht der Arbeitsablauf aus, in den beispielsweise das CT-Gerät eingebunden wird? Welche DICOM-Protokolle sind notwendig (Query, Mail, Worklist etc.) um den Ablauf lückenlos zu unterstützen? Welche Subsysteme liefern die Daten bzw. empfangen die Bilder?

Sicherheitsaspekte Service-Notebooks/USB-Sticks
Immer wieder berichten Mitarbeiter aus Krankenhäusern (MT, IT) informell, dass trotz aller Vorsichtsmaßnahmen Service-Techniker elektronische Viren über kontaminierte Service-Notebooks und/oder Sticks in das Betreiber-Netzwerk einschleusen. Betreiber und Hersteller müssen daher sich verständigen (siehe auch Responsibility Agreement), wie der Hersteller durch interne Maßnahmen sicherstellt, dass derartige Vorfälle nicht mehr auftreten. Hersteller und Betreiber können dazu vertraglich vertrauliche Informationen austauschen, die der Betreiber sowohl benötigt, um das Risikomanagement für das Medizinische Netzwerk durchzuführen als auch nachzuvollziehen, wer und wie einen Virus bei einem Service-Einsatz eingeschleust hat.

7. Zuständigkeits-/Verantwortungsvereinbarung (Responsibility Agreement)
IEC 80001 sieht in Kapitel 4.3.4 eine Zuständigkeitsvereinbarung zwischen Hersteller und Betreiber vor, mit der Verantwortlichkeiten beispielsweise durch einen Vertrag mit einem oder gegebenenfalls auch mehreren Herstellern für ein zu integrierendes Medizinprodukt festgelegt werden können. Was bedeutet das und welche Möglichkeiten bietet die Norm damit Herstellern und Betreibern? Wie kann man diese Vereinbarung nutzen, um die Sorgfaltspflichten des Betreibers über den Lebenszyklus eines vernetzten Medizinproduktes mit Hilfe des Herstellers zu erfüllen?
Die Norm führt dazu aus, dass eine Zuständigkeitsvereinbarung ein oder mehrere Projekte (Integrationsprojekte) und/oder Instandhaltungsprojekte (Medizinischer Netzwerke umfassen kann, die zwischen Hersteller und Betreibern abgeschlossen werden kann. Sie soll auf diese Weise die Verantwortlichkeiten für alle Aspekte des Lebenszyklus des Medizinproduktes in einem medizinischen Netzwerk definieren und die Aufgaben regeln, die erforderlich sind, um die Schutzziele (Sicherheit, Schutz und Effizienz) des medizinischen Netzwerkes zu erreichen und zu erfüllen.

Mit einer solchen Zuständigkeitsvereinbarung können Hersteller und Betreiber beispielhaft vereinbaren und festlegen:

- Verantwortliche Ansprechpartner (Z. B., wer ist Ansprechpartner des Betreibers und führt das Risikomanagement durch? Wer ist der verantwortliche Ansprechpartner des Herstellers für sicherheitsrelevante Vorfälle wie Virenbefall z. B. am Wochenende?)
- Laufende Sicherheitsinformationen des Herstellers an den Betreiber über aktuelle Gefährdungen z. B. durch Malware
- Gewährleistung eines aktuellen Patchmanagements auf der Betriebssystemebene und des Virenschutzes innerhalb definierter Fristen
- Informationen über Verbesserungen von sonstigen IT-Sicherheitskonzepten
- Informationen über Release-Wechsel, Treiberwechsel, Änderungen von Schnittstellenkonfigurationen durch den Hersteller
- Vertragliche Regelung der Vertraulichkeit von ausgetauschten Informationen (Wo und in welcher Form fangen Firmengeheimnisse an, was kann der Betreiber grundsätzlich an vertraulichen Informationen von einem Hersteller erwarten? Usw. usw.)
- Informationen über Lebenszyklen der IT-Komponenten eines Medizinproduktesystems (Medizinprodukte erreichen das Dreifache der Lebensdauer von IT-Komponenten wie PC)
- U. a.

Kapitel 4.3.4 Zuständigkeitsvereinbarung der IEC 80001 gibt mehr allgemeine Inhalte für derartige Informationen, sodass Hersteller und Betreiber gemeinsam definieren müssen, welche Ziele und konkreten Inhalte die Vereinbarung haben sollte. Ein wesentliches Ziel des Betreibers besteht darin, sicher zu stellen, dass bei Änderungen wie dem Patchmanagement von Betriebssystem und Virenschutz die Herstellerkonformität des Produktes mit der EG-Richtlinie erhalten bleibt. Dies bedeutet, dass der Hersteller eines Medizinproduktes Patches vertraglich geregelt in einer angemessenen Zeit validiert und freigibt und über aktuelle Bedrohungen und Gefährdungen seines Produktes in IT-Netzwerken den verantwortlichen Ansprechpartner des Betreibers kurzfristig informiert.

Auftraggeber und Auftragnehmer derartiger Zuständigkeitsvereinbarungen können diese u. a. Regelungen individualrechtlich vereinbaren.
Eine solche Zuständigkeitsvereinbarung kann also die Verpflichtung umfassen, dass der Hersteller über sämtliche Weiterentwicklungen, Aktualisierungen, Sicherheitsinformationen des zu beschaffenden Medizinproduktes bzw. Medizinproduktesystems im Rahmen der Hersteller-Konformität informiert und anbietet. So kann z. B. ein Hersteller im Rahmen einer solchen vertraglichen Vereinbarung auch den sicheren, effektiven Betrieb und Schutz eines medizinischen Netzwerkes wie einer Radiologie übernehmen.

8. Betreiber-Aufgaben

Der Betreiber muss seine Prozesse der Beschaffung und Instandhaltung von vernetzbaren Medizinprodukten verändern und/oder weiterentwickeln, um die definierten Schutzziele der Norm 80001 auf der Basis des Medizinproduktegesetzes und der Medizinproduktebetreiberverordnung innerhalb seiner Organisation bewältigen zu können. Zum anderen bedingt die Norm eine aktive Diskussion und Einbindung von Herstellern in die Prozesse des sicheren und geschützten Betriebes von medizinischen Netzwerken in Krankenhäusern.
In aktuellen Ausschreibungen finden sich beispielhafte Passagen:

- Der Auftragnehmer versichert, dass das Medizinprodukt gemäß den Bestimmungen der IEC 80001 betrieben werden kann.
- Der Auftragnehmer verpflichtet sich, die Bestimmungen der IEC 80001 für die Integration seines Produktes zusammen mit dem Auftraggeber anzuwenden.
- u. a. Formulierungen.

Der Betreiber sollte spezifisch seine Informationsbedürfnisse spezifizieren, indem er seine Strategie und die daraus resultierenden Anforderungen an die Sicherheit, den Schutz und die Effizienz eines Medizinischen Netzwerkes klärt. Dies ist eine Gemeinschaftsaufgabe der Organisationsstrukturen von Medizintechnik, IT und auch des Einkaufs. So muss der Betreiber z. B. sein Patchmanagement für die verschiedenen IT-Produkte und Medizinprodukte(-systeme) definieren, um damit Zielklarheit für die Diskussion und Informationsaustausch mit Herstellern zu gewinnen.
Die pauschale Forderung nach Informationen gemäß IEC 80001 hilft dem Betreiber wenig, wenn dieser noch keine Zielklarheit darüber hat, wie er seine medizinischen Netzwerke betreiben will; die IEC 80001 sollte daher genutzt werden, die Informationsnotwendigkeiten bis hin zu Angaben für das Risikomanagement auf Betreiberseite zu definieren.

9. Zusammenfassung und Ausblick

Mit der Norm ist die Sicherheit der medizinischen Netzwerke und der damit verbundenen Aufgaben für Betreiber (und für Hersteller) klar in den Fokus des Interesses getreten. Die IEC 80001 stellt also eine Möglichkeit dar, mit der der Betreiber seine Sorgfaltspflichten bzw. Obliegenheitspflichten beim Betrieb von vernetzten Medizinprodukten erfüllen und nachweisen kann

Die dazu notwendigen Prozesse des Informationsaustausches zwischen Herstellern und Betreibern werden sich mit Erscheinen des Weißdruckes der Norm vrsl. Anfang Mai 2011 deutlich entwickeln. Die noch zu spürende Verunsicherung auf beiden Seiten wird sich im Laufe der Zeit legen, wenn beide Partner die Norm als Chance

sehen, voneinander zu lernen, wie die Sicherheit und der Schutz medizinischer Netzwerke aufgebaut und weiterentwickelt werden kann. Dieser beidseitige Lernprozess ist durchaus als Chance zu sehen. Die Frage, wer welche Hol- und Bringschuld übernimmt, wird sich klären, vor allem, wenn die Betreiber ihre Sicherheitsstrategie bei der Integration von Medizinprodukten in Medizinische IT-Netzwerke und die daraus resultierenden Konsequenzen definiert haben.

Literatur und Quellenangaben

1. http://www.heise.de/newsticker/meldung/Virus-legt-Krankenhaus-lahm-1122484.html
2. Gärtner, A.; Medizinproduktesicherheit Band 5: Medizinische Netzwerke und Software als Medizinprodukt, TÜV Media GmbH Köln 2009, ISBN 978-3-8249-1167-7
3. http://www.zvei.org/fileadmin/user_upload/Fachverbaende/Elektromedizinische_Technik/FAQs_zur_IEC_80001-Rev__2_1_____Stand_15_07_2010-m.pdf
4. Gärtner, A. (Hrsg.); Medizintechnik und Informationstechnologie (MIT) TÜV Media Verlag Köln, April 2011
5. http://www3.netop.com/netop-935.htm, letzter Zugriff 19.01.2011

Armin Gärtner
Ingenieurbüro für Medizintechnik
Ö. b. u. v. Sachverständiger für Medizintechnik und Telemedizin
Edith-Stein-Weg 8
40699 Erkrath
Armin.gaertner@t-online.de