EHEALTHCOM
Magazin für Health-IT, vernetzte Medizintechnik und Telemedizin

Computer-Betriebssysteme in der Medizintechnik: Erfahrungen und Empfehlungen eines Krankenhauses

Expertenbeitrag von Armin Gärtner und Michael Voth

Einleitung

Computer-Betriebssysteme spielen eine wichtige Rolle in der Funktionalität von Medizinprodukten, entweder als „embedded“ in einem Medizinprodukt oder als Stand-alone Betriebssystem auf einem PC in Verbindung mit einem Medizinprodukt als Medizinproduktesystem. Ausgehend von der Ende Dezember 2012 erfolgten Abkündigung des kostenfreien Supports von Windows XP Professional betrachtet dieser Beitrag allgemein die Rolle von Betriebssystemen in Medizinprodukten.
Aus Sicht der Medizintechnik eines Krankenhauses und aus Sicht eines Sachverständigen werden Erfahrungen und Empfehlungen vorgestellt, wie Krankenhäuser und Industriepartner bei den diskutierten Fragestellungen zusammenarbeiten können/sollten.
Dazu gehören auch die Betrachtung der möglichen Gefährdungen durch Betriebssysteme ohne Patchmanagement bzw. der Weiterbetrieb abgekündigter Betriebssysteme aus Sicht des Risikomanagements z. B. nach DIN EN 80001-1 sowie die daraus resultierenden, möglichen wirtschaftlichen Konsequenzen.

1. Betriebssysteme in der Medizintechnik

1.1 Betriebssystem – Allgemeines

Quelle 1 beinhaltet folgende Definition bzw. Beschreibung der Funktion eines Betriebssystems (BS), auch als Operating System (OS) bezeichnet:
Ein Betriebssystem ist eine Sammlung von Computerprogrammen, die die Systemressourcen eines Computers wie Arbeitsspeicher, Festplatten, Ein- und Ausgabegeräte verwalten und diese Anwendungsprogrammen zur Verfügung stellen. Das Betriebssystem bildet dadurch die Schnittstelle zwischen den Hardwarekomponenten und der Anwendungssoftware des Benutzers.

Betriebssysteme bestehen in der Regel aus einem Betriebssystemkern (englisch: Kernel), der die Hardware des Computers verwaltet sowie speziellen Programmen, die beim Start unterschiedliche Aufgaben übernehmen. Zu diesen Aufgaben gehört unter anderem das Laden von Gerätetreibern. Betriebssysteme finden sich in fast allen Computern: als Echtzeitbetriebssysteme auf Prozessrechnern, auf PC und auf Mehrprozessorsystemen wie Hosts und Großrechnern sowie auf Smartphones und Tablet PC.

Die Aufgaben eines Betriebssystems lassen sich wie folgt zusammenfassen: Benutzerkommunikation; Laden, Ausführen, Unterbrechen und Beenden von Programmen; Verwaltung und Zuteilung der Prozessorzeit; Verwaltung des internen Speicherplatzes für Anwendungen; Verwaltung und Betrieb der angeschlossenen Geräte; Schutzfunktionen z. B. durch Zugriffsbeschränkungen u. a.

Die Gewichtung zwischen diesen Aufgaben wandelte sich im Laufe der Zeit, insbesondere wird dem Schutz heute eine höhere Bedeutung zugemessen als noch in den 1990`er Jahren.

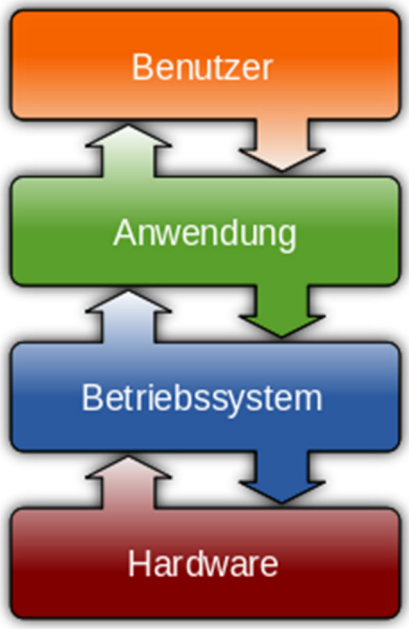


Abbildung 1: Zusammenhang zwischen Betriebssystem, Hardware, Anwendungssoftware und dem Benutzer [Quelle 1]

In der Normen-Sammlung DIN 44300 (Informationsverarbeitung und lokale Netze) wird Betriebssystem wie folgt definiert [Quelle 2]: *Die Programme eines digitalen Rechensystems, die zusammen mit den Eigenschaften dieser Rechenanlage die Basis der möglichen Betriebsarten des digitalen Rechensystems bilden und die insbesondere die Abwicklung von Programmen steuern und überwachen.*

An Betriebssysteme für medizinische Anwendungen werden die folgenden Anforderungen gestellt:

- Schnelligkeit *
- Geringer Ressourcenverbrauch
- Zuverlässigkeit und Stabilität
- Sicherheit.

** Bei einer Zeitanforderung im Minutenbereich, lässt sich ein System durchaus noch von Hand steuern, unterhalb dieser Marke (etwa 1 Minute) reicht eine Automatisierung auf Basis von Mechanik aus. Zeitanforderungen im Sekunden-Bereich lassen sich durchaus mit einem Standardbetriebssystem erfüllen, im Millisekunden-Bereich jedoch benötigt man ein Realzeitbetriebssystem. Unterhalb dieser Grenze hilft nur noch eine Realisierung in Hardware. [Quelle 3]*

Die benötigte Ausführungsgeschwindigkeit der einzelnen Rechenoperationen konnte in der Vergangenheit nur durch elektronische Schaltkreise erreicht werden. Heute werden stattdessen Echtzeitbetriebssysteme (Real Time Operating Systeme – RTOS) eingesetzt. Durch die zunehmenden Echtzeitfähigkeiten werden auch Standardbetriebssysteme immer häufiger in der Medizintechnik eingesetzt. Diese bieten gegenüber den reinen Echtzeitbetriebssystemen im Wesentlichen die folgenden Vorteile:

- Applikationsvielfalt
- geringerer Einarbeitungsaufwand
- gute Entwicklungswerkzeuge
- grafische Benutzeroberfläche mit gewohnter Benutzerführung
- lauffähig auf preiswerter Hardware
- bessere Interoperabilität.

1.2 Warum Standard-Betriebssysteme in der Medizintechnik?

Ein wesentlicher Aspekt, Standard-Betriebssysteme zu verwenden, ist ökonomisch basiert: Der Markt für Medizintechnik ist hart umkämpft. Der Zukauf von Systembestandteilen bietet gegenüber der Eigenproduktion den Vorteil einer verkürzten Markteinführungszeit bei gleichzeitiger Einsparung von Ressourcen und möglicher Steigerung der Qualität.
So äußert sich beispielsweise Fa. Microsoft in ihrem “OEM’s Guide to Medical Device Operating Systems” [Quelle 4], aus dem nachfolgend auszugsweise zitiert wird:

„Microsoft sieht vielfältige Möglichkeiten für die Entwicklung neuer Geräte in der Gesundheitsbranche. Durch die zunehmende Integration der Systeme wird die Effizienz der Gesundheitsversorgung erhöht. Allerdings ist es keine leichte Aufgabe, neue Geräte in den Markt zu bringen. Abgesehen von der Erfüllung regulatorischer und Qualitätsanforderungen, gibt es grundlegende Fragen rund um die Entwicklung von Medizinproduktesystemen.
Diese Fragen umfassen:
Die sorgfältige Planung von Gerätedesign und Verpackung, um den Anforderungen einer klinischen Umgebung gerecht zu werden und Akzeptanz bei Angehörigen der Gesundheitsberufe Gerät zu finden (…..).

Die Software, die das Gerät steuert, muss die einzigartige Funktionalität und den Wert des Gerätes unterstützen. Große Sorgfalt muss darauf verwendet werden, dass diese Software für die Rolle, die das Gerät erfüllen soll, optimiert wird.
Jedes Software-gesteuerte medizinische Gerät benötigt ein Betriebssystem. Das Betriebssystem regelt die interne Kommunikation zwischen der Anwendungssoftware und der Hardware.
Oft wird laut Microsoft dieser kritischen Komponente weniger Aufmerksamkeit zuteil als sie verdient.
Warum ist das Betriebssystem so entscheidend für den Erfolg eines medizinischen Gerätes? Die Wahl eines Betriebssystems betrifft nicht nur die Geschwindigkeit der Markteinführung, sondern auch, wie schnell die Entwicklungskosten wieder eingespielt werden können. Das Betriebssystem wirkt sich auf die langfristige Wirtschaftlichkeit eines Gerätes aus: Je länger ein Gerät am Markt eingesetzt wird, desto profitabler wird es sein.“

Das bedeutet, dass kommerzielle Standardsoftware bzw. Standard-Betriebssysteme in der Medizintechnik eingesetzt werden, die nicht ausschließlich und speziell für die regulatorischen und sicherheitstechnischen Anforderungen von vernetzten Medizinprodukten entwickelt wurden.

1.3 Beispiele für ein Medizinprodukte mit Betriebssystem

Folgende Beispiele zeigen die Verwendung von Betriebssystemen in der Medizintechnik und verdeutlichen die möglichen Konsequenzen:

Ein bildgebendes Ultraschallgerät stellt heute prinzipiell einen Computer dar, der angeschlossene Transducer steuert, Messwerte abfragt, verrechnet und die Bilder auf Graustufen- oder Farbmonitoren darstellt. Im Bereich Ultraschallgeräte werden häufig Betriebssysteme auf Windows-Basis eingesetzt.
Da immer wieder informell aus Krankenhäusern berichtet wird, dass auch vernetzte Ultraschallgeräte von Malware befallen werden, deutet dies daraufhin, dass auch in Ultraschallgeräten keine embedded Betriebssysteme eingesetzt werden.

Abbildung 2 zeigt ein idealtypisches, beispielhaftes Medizinproduktesystem als EKG-Schreiber in funktionaler Darstellung der einzelnen Komponenten. Das Betriebssystem stellt die Basis für die EKG-Auswertesoftware (Medizinprodukt) dar, die die Messwerterfassung, - auswertung und Anzeige der EKG-Kurven und Parameter auf einem Display steuert.

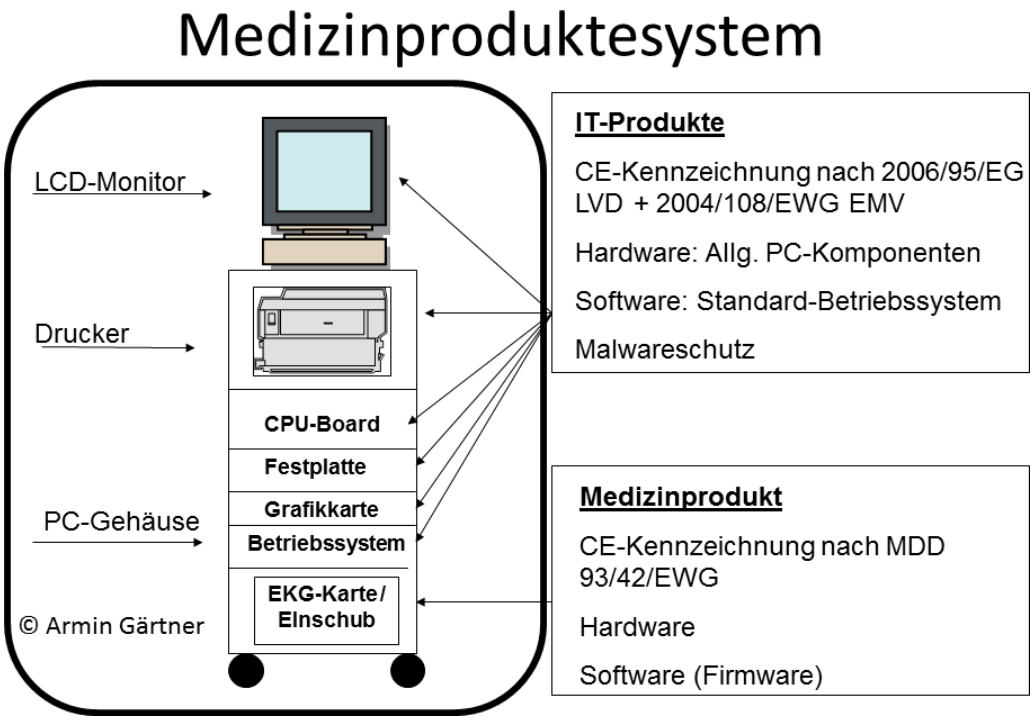


Abbildung 2: Medizinproduktesystem mit Betriebssystem

PC mit Standard-Betriebssystem als Steuerrechner eines Medizinproduktes
Häufig werden PC zur Datenakquise und/oder Steuerung von Medizinprodukten eingesetzt und beinhalten ebenfalls Standard-Betriebssysteme. Abbildung 3 zeigt einen solchen Steuerrechner, auf dem die Software zur Steuerung eines Linearbeschleunigers läuft.

Abbildung 3 zeigt auch, wie unterschiedlich sich die Lebenszyklen von Medizinprodukten und IT-Komponenten (Hardware und Betriebssysteme) entwickeln. Das Medizinproduktesystem besteht zum Zeitpunkt der Beschaffung aus einem Linearbeschleuniger, einem Steuerrechner als Standard-Hardware, dem Betriebssystem Windows XP sowie der Steuerungssoftware des Linearbeschleunigers.
Der Linearbeschleuniger kann eine Nutzungszeit zwischen 15 und 18 Jahren erreichen, ein Zeitraum, in dem Hardware und Betriebssystem bis zu vier Mal getauscht werden können, da sie Lebenszyklen von 3-4 Jahren häufig nicht überschreiten.

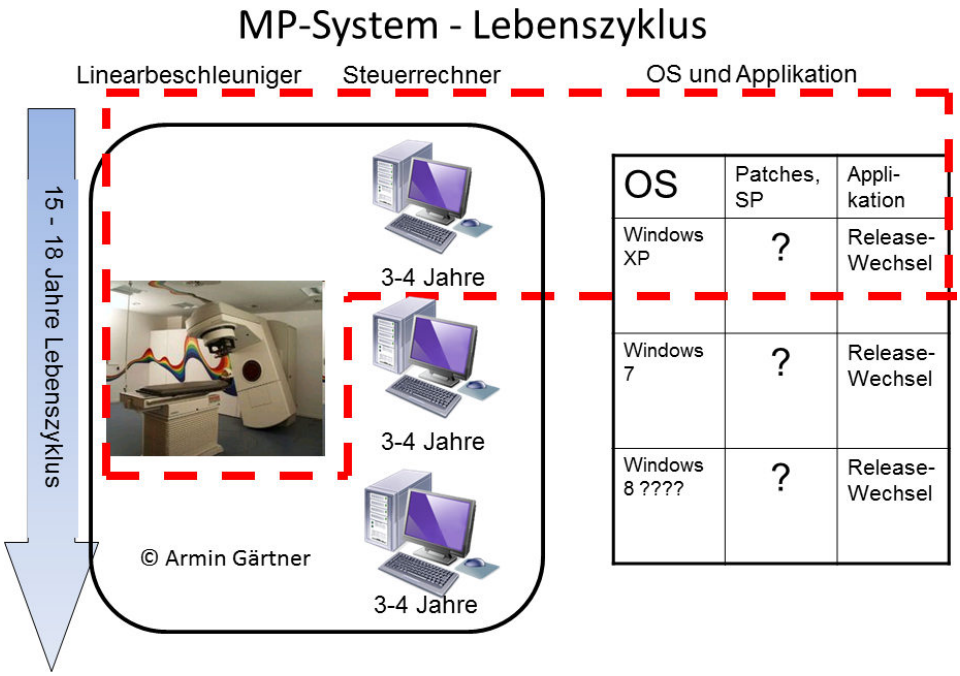


Abbildung 3: Medizinproduktesystem mit Steuerrechner (Windows XP)

Das Gesamtsystem mit allen Komponenten ist vom Hersteller dem vorgeschriebenen Konformitätsbewertungsverfahren nach der Medizinprodukterichtlinie Medical Devices Directive 93/42/EWG unterzogen worden; Wesentliche Änderungen wie z. B. die Migration eines Betriebssystems bedürfen der Zustimmung bzw. Freigabe durch den Hersteller.
Bei der Ausschreibung wurde das Betriebssystem des Steuerrechners nicht abgefragt und bei der Übergabe fehlte im Protokoll jegliche Angabe, welches Betriebssystem in welchem Patchzustand geliefert wurde. Weder Betreiber noch Hersteller klärten im Vorfeld die Problematik des laufenden Patchmanagements des Betriebssystems für das in einem allgemeinen IT-Netzwerk integrierte Medizinproduktesystem; auch der mit Inbetriebnahme des Linearbeschleunigers abgeschlossene Wartungsvertrag beinhaltete keinerlei Hinweise auf das Patchen des Betriebssystems durch Hersteller oder Betreiber.

1.4 Verwendete Betriebssysteme in der Medizintechnik

Für welches Betriebssystem sich der Hersteller eines Medizinproduktes entscheidet, hängt zum einen von der Art des Produktes ab, welches er entwickelt, und zum anderen von wirtschaftlichen Überlegungen.

Die Thematik der Betriebssysteme soll nachfolgend am Beispiel der vielfach eingesetzten Varianten von Microsoft diskutiert werden. Durch die vermehrte Nutzung von mobilen Systemen ist zu erwarten, dass auch Googles Android und Apples iOS in Zukunft Bestandteil von Medizinprodukten werden.

Betriebssystemübersicht

Ein Medizinprodukt soll möglichst einfach und sicher bedient werden. Daher wird zur Verbesserung der Gebrauchstauglichkeit das Betriebssystem für den Anwender oft komplett ausgeblendet und ist dann nur über spezielle Servicezugänge zu erreichen.

Für den Betreiber kann es daher mit einigem Aufwand verbunden sein, das Betriebssystem eines Medizinproduktes zu identifizieren. Einige Vorgehensweisen zur Informations-beschaffung werden nachfolgend beschrieben.
Schon an dieser Stelle sei darauf hingewiesen, dass der Betreiber ab sofort bei Beschaffungen von vernetzbaren Medizinprodukten bereits im Vorfeld klären sollte, welches Betriebssystem ein Hersteller in welchem Patchzustand anbietet bzw. mitliefert, da die Beschaffung eines älteren Betriebssystems möglicherweise finanzielle Konsequenzen über den Lebenszyklus des Medizinproduktes nach sich ziehen und auch ein Gefährdungspotenzial nach DIN EN 80001-1 darstellen kann.

Die Computerzeitschrift c´t informierte mit der letzten Ausgabe 2012 die breite Öffentlichkeit über die Abkündigung des Betriebssystems Windows XP Professional für das Frühjahr 2014. [Quelle 5]
Mit dem Ende des Lebenszyklus von Windows XP mit kostenfreiem Support rücken das Thema der Betriebssysteme in der Medizintechnik und Fragestellungen, wie damit ab 2014 umzugehen ist, erstmalig in vielfältiger Form in den Fokus der Betreiber, insbesondere was vernetzte Medizinprodukte anbetrifft.
Viele Medizinprodukte/Medizinproduktesysteme laufen mit Varianten des Betriebssystems Windows XP und werden vrsl. noch in den nächsten Jahren, auch nach dem Abkündigungstermin von Microsoft eingesetzt werden.

Tabelle 1 zeigt Beispiele des Einsatzes der Varianten von Windows und auch anderen Betriebssystemen in Medizinprodukten.

Hersteller	Produkt	Beispiele von Hersteller-Anwendungen
Microsoft	Windows XP Professional, Windows 7 Professional	Philips Xcelera PACS Carestream PACS Vue EEG System Nihon Kohden Neurofax
Microsoft	Windows XP embedded	Ultraschallgerät Philips iE33
Microsoft	Windows XP for embedded Systems	Röntgensysteme Siemens Uroskop Access
IBM	AIX	Monitoring Zentrale Dräger Infinity Central Station
Apple	Mac OS 10.8	DICOM Viewer Aycam Osirix Pro
WindRiver	VxWorks	Philips C-Bogen Veradius

Tabelle 1: Betriebssystemvarianten von Microsoft u. a. BS-Herstellern nach Herstellerangaben

Tabelle 2 zeigt den Lebenszyklus der Betriebssysteme Windows XP, Windows XP embedded sowie Windows XP for embedded Systems und wie unterschiedlich diese von Microsoft betreut werden bzw. ein kostenfreier Support angeboten wird.

Windows Variante	**generelle Verfügbarkeit**	**Lifecycle-Startdatum**	**Ablaufdatum für Mainstream Support**	**Ablaufdatum für Extended Support**	**Vertriebsende**
Windows XP Embedded		30.01.2002	11.01.2011	12.01.2016	

Windows XP Professional		31.12.2001	14.04.2009	08.04.2014	
Windows XP Professional for Embedded Systems	31.12.2001				31.12.2016

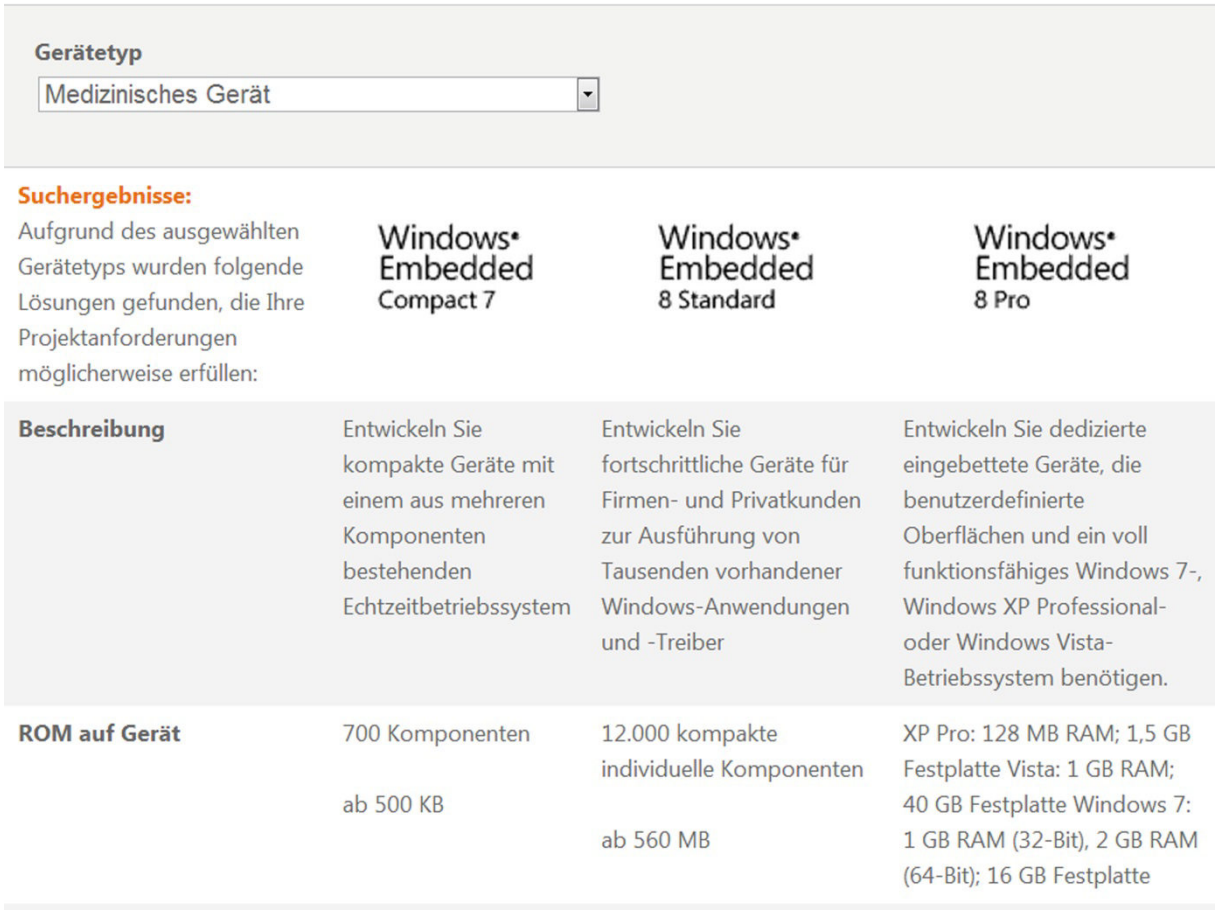
Tabelle 2: Windows XP Varianten und Lebenszyklusdaten (nach Angaben Microsoft)

Bei nicht vernetzten Medizinprodukten spielt die Sicherheit des verwendeten Betriebssystems für den Betreiber eine untergeordnete Rolle.
Bindet man hingegen ein Medizinprodukt und/oder ein Medizinproduktesystem in ein Med. IT-Netzwerk ein, muss der Betreiber immer ein Risikomanagement über diese Integration durchführen. Um dies sinnvoll durchführen zu können, muss das verwendete Betriebssystem und dessen Patchlevel bekannt sein. Nur dann können daraus resultierende Gefährdungen abgeleitet werden und mögliche Risiken bewertet werden.
Eine Risikobetrachtung in Form einer Risikoanalyse wird immer die Notwendigkeit der Aktualisierung des Betriebssystems mit einbeziehen müssen.

Embedded Systems

Setzt ein Hersteller spezielle Industrierechner ein, kommen die dafür angepassten Betriebssysteme zum Einsatz. Die Rechner zeichnen sich dabei durch eine besonders robuste Bauweise aus. Sie werden aufgrund ihrer kompakten Abmessungen mit den restlichen Systembestandteilen in ein Gehäuse eingebettet. Die Betriebssysteme sind oft sogenannte Real Time Operation Systeme (RTOS), die eine sehr stabile Ausführungssicherheit in Echtzeit garantieren. So kommt das in der Medizintechnik häufig eingesetzte Betriebssystem VxWorks von der Firma WindRiver [Quelle 6] auch dem Mars Rover Curiosity zum Einsatz.

Für Software, die in ein Medizinprodukt eingebettet wird, setzten die Hersteller aber immer häufiger auch die von Microsoft für diesen Einsatzzweck empfohlenen *embedded* Betriebssystem-Varianten ein gemäß Tabelle 3.



Gerätetyp

Medizinisches Gerät

Suchergebnisse:

Aufgrund des ausgewählten Gerätetyps wurden folgende Lösungen gefunden, die Ihre Projektanforderungen möglicherweise erfüllen:

	Windows Embedded Compact 7	Windows Embedded 8 Standard	Windows Embedded 8 Pro
Beschreibung	Entwickeln Sie kompakte Geräte mit einem aus mehreren Komponenten bestehenden Echtzeitbetriebssystem	Entwickeln Sie fortschrittliche Geräte für Firmen- und Privatkunden zur Ausführung von Tausenden vorhandener Windows-Anwendungen und -Treiber	Entwickeln Sie dedizierte eingebettete Geräte, die benutzerdefinierte Oberflächen und ein voll funktionsfähiges Windows 7-, Windows XP Professional- oder Windows Vista-Betriebssystem benötigen.
ROM auf Gerät	700 Komponenten ab 500 KB	12.000 kompakte individuelle Komponenten ab 560 MB	XP Pro: 128 MB RAM; 1,5 GB Festplatte Vista: 1 GB RAM; 40 GB Festplatte Windows 7: 1 GB RAM (32-Bit), 2 GB RAM (64-Bit); 16 GB Festplatte

Tabelle 3: Varianten embedded Betriebssysteme der Firma Microsoft [Quelle 7]

Wikipedia definiert embedded Betriebssystem folgendermaßen [Quelle 8]:
„Der Ausdruck eingebettetes System (auch engl. embedded system) bezeichnet einen elektronischen Rechner oder auch Computer, der in einen technischen Kontext eingebunden (eingebettet) ist. Dabei übernimmt der Rechner entweder Überwachungs-, Steuerungs- oder Regelfunktionen oder ist für eine Form der Daten- bzw. Signalverarbeitung zuständig, beispielsweise beim Ver- bzw. Entschlüsseln, Codieren bzw. Decodieren oder Filtern.
Eingebettete Systeme verrichten – weitestgehend unsichtbar für den Benutzer – den Dienst in einer Vielzahl von Anwendungsbereichen und Geräten, beispielsweise in Geräten der Medizintechnik.“

3. Anforderungen der Medizinprodukterichtlinie Medical Devices Directive 93/42/EWG (MDD 2007/47/EG)

Ein Hersteller, der ein Medizinprodukt bzw. ein Medizinproduktesystem in Verkehr bringen will, muss ein Konformitätsbewertungsverfahren mit einem Risikomanagement durchführen. Dazu muss er die sogenannten Grundlegenden Anforderungen der Medizinprodukterichtlinie Medical Devices Directive 93/42/EWG in der Fassung 2007/47/EG erfüllen, die auf das Produkt zutreffen.

Ein Hersteller muss dem Betreiber gemäß Absatz 13 der Grundlegenden Anforderungen (Anhang I) nach der MDD-Richtlinie Informationen bereitstellen. Die

DIN EN 60601-1 beinhaltet in der 3. Ausgabe in Kapitel 13.14 allgemein akzeptierte Definitionen, welche Informationen der Hersteller für die Integration eines Medizinproduktes in ein Betreibernetzwerk zur Verfügung stellen sollte [Quelle 9].
Dies ist bisher weder von Herstellern noch von Betreibern konsequent gelebt worden, ändert sich nun aber, indem immer mehr Hersteller solche Informationen zur Verfügung stellen bzw. Betreiber diese Informationen einfordern unter Verweis auf Kapitel 3.5 der DIN EN 80001-1:2011 [Quelle 9].

Verwendet der Hersteller ein Betriebssystem wie z. B. Windows XP für ein vernetzbares Produkt, so muss er im Rahmen des Risikomanagements mehrere Aspekte berücksichtigen:

- Ein Betriebssystem stellt ein Produkt außerhalb der Verantwortlichkeit des Herstellers dar und wird nach DIN EN 62304 als SOUP (Software of unknown provenance) angesehen [Quelle 10]. Der Hersteller muss also mögliche Auswirkungen eines Betriebssystems auf das sichere Verhalten des Medizinproduktes bewerten.
- Das Betriebssystem muss aus Sicherheitsgründen durch Patches aktualisiert werden , d. h. der Hersteller muss das Patchmanagement betrachten und den Betreiber informieren, wie dieses unter Beibehaltung der Herstellerkonformität des Produktes mit der Medizinproduktrichtlinie durchgeführt werden kann.
- Wenn der Hersteller in seiner Risikoanalyse erkennt, dass aus dem Betreiber-Netzwerk, das nicht unter der Herstellerverantwortung steht, Malware auf das Produkt gelangen und damit ein Betriebssystem beeinflussen kann, so muss er entweder selber einen Malwareschutz vorsehen und vorgeben oder dem Betreiber informieren, wie er einen solchen zu installieren und zu patchen hat, ohne dass die Herstellerkonformität mit der Medizinproduktrichtlinie tangiert wird.

Je nach Umfang stellt ein Patch eines Betriebssystems eine wesentliche Veränderung eines Medizinproduktes dar.
Wird ein Medizinprodukt wesentlich verändert, so muss der Hersteller seine Technische Dokumentation für den Nachweis der Konformität mit der Richtlinie überarbeiten und gegebenenfalls eine neue Konformitätserklärung ausstellen oder zumindest dem Betreiber bestätigen, dass die Konformität (wie durch einen Patch) nicht aufgehoben wird.
Die Frage, wann ein Patch eines Betriebssystems zu einer Neubewertung der Hersteller-konformität führt, lässt sich folgendermaßen beantworten:

Patches	**Auswirkungen auf die Konformität mit den Grundlegenden Anforderungen der Richtlinie MDD**
Patch als Reparatur (z. B. Anzeigefehler)	Keine Konformitätsüberprüfung

Sicherheitsrelevanter Patch (z. B. Schließen einer Eintrittslücke)	Risikoanalyse, ob sich Auswirkungen auf andere Funktionen ergeben im Sinne einer wesentlichen Änderung
Service Pack mit neuen Funktionalitäten	Neubewertung der Konformität mit neuer Konformitätserklärung bzw. Bestätigung, dass die Produktkonformität dadurch nicht beeinträchtigt wurde.

Tabelle 4: Auswirkungen von Patches auf die Konformität eines Produktes

Dies bedeutet, dass der Betreiber zusammen mit dem Hersteller klären muss, ob, wann und wie ein Patchmanagement für ein Medizinprodukt erfolgen muss und wie die Herstellerkonformität dabei erhalten bleibt.

3.1 Patchmanagement in der Medizintechnik

Patchmanagement bedeutet die regelmäßige, planmäßige Aktualisierung und die anschließende Überprüfung der Patchstände von Betriebssystemen. Alle relevanten IT-Systeme sollten durch das Patchmanagement erfasst sein. Die organisatorische Umsetzung des Patch- und Änderungsmanagements von Medizinprodukten mit Koordination und Kommunikation betrifft verschiedene Abteilungen eines Krankenhauses. Insbesondere sind der IT-Betrieb, das Informationssicherheitsmanagement und die Fachabteilungen wie beispielsweise die technische oder medizintechnische Abteilung entsprechend der Organisationsstruktur einzubinden.

Im Regelfall ist die Medizintechnik für die Instandhaltung und Sicherheit der technischen Medizinprodukte verantwortlich. Im Prinzip stellt das Aktualisieren des Betriebssystems eines Medizinproduktes (Patchen, Updates, Upgrades) nichts anderes als eine Instandhaltung dar. Damit gelten für das Patchen die Anforderungen des § 4 MPBetreibV.

Für die Durchführung dürfen nur Personen, Betriebe oder Einrichtungen betraut werden, die die Sachkenntnis, Voraussetzungen und die erforderlichen Mittel zur Durchführung dieser Aufgabe besitzen. Auch die Dokumentation des Patchzustandes im Medizinproduktebuch gehört zu den Betreiberaufgaben.

Führt die IT Abteilung das Patchen von IT-Produkten mittels Windows Software Update Service (WSUS) durch, kann dieser Nachweis bei IT-Systemen in Form von automatisierter Dokumentation der aufgespielten Patches geführt werden. Allerdings hat die Berichtserstellung auf die Clientüberwachung offensichtliche Schwächen (siehe Abschnitt 3.2).

Werden Patches in Medizinprodukte durch Servicetechniker eines Medizinprodukteanbieters eingespielt, sollte man darauf bestehen, dass der Patchlevel auf den Servicedokumenten eingetragen wird.

Bei Remotearbeiten durch die IT eines Medizinproduktherstellers gehört es mittlerweile zum Standard, über die erfolgreiche Durchführung der Arbeiten per E-Mail informiert zu werden. Auch in diesem Fall sollte der Patchlevel übermittelt werden.

Mit dem Hersteller des Medizinproduktes sollte geklärt werden, wie umfangreich die Funktionsprüfung nach dem Einspielen eines Patches ist und durch wen sie durchgeführt werden kann.

3.2 Patchmanagement für Microsoft-Produkte

Neue Patches für Microsoft-Produkte werden als Security Bulletins in der Regel einmal monatlich veröffentlicht, und zwar am zweiten Dienstag jedes Kalendermonats. Für besonders kritische Sicherheitslücken werden Patches auch zwischen diesen Terminen veröffentlicht. Für jede betroffene Produktfamilie publiziert Microsoft eine Übersichtsseite (Security Bulletin Summary) im Internet. Sie bietet eine Zusammenfassung mit Informationen zu allen Updates, die in diesem Monat für die jeweilige Produktfamilie erschienen sind. Die Security Bulletins sind über eine eindeutige Kennzeichnung (MSYY-XXX) identifizierbar, wobei YY für die aktuelle Jahreszahl steht.

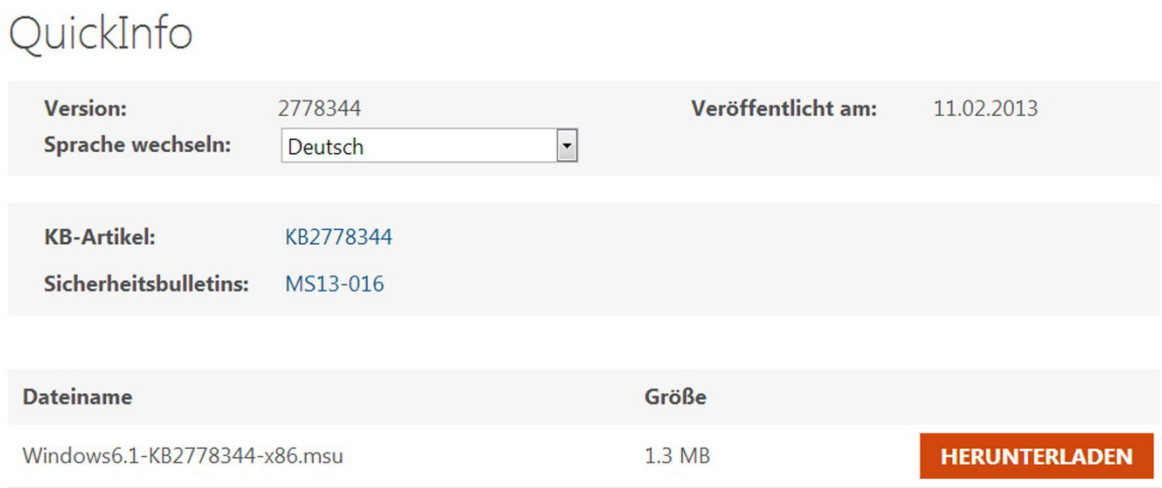


Abbildung 4: Beispiel Quickinfo zum Microsoft Security Bulletin MS13-016 (Sicherheitsanfälligkeiten in Windows-Kernelmodustreiber)

Das Security Bulletin beschreibt die mögliche Sicherheitslücken des betroffenen Systems und verweist auf den Patch, der diese beseitigen soll. Dieser ist über eine Komponentenkennung nach dem Schema KBXXXXXXX zu identifizieren.
Daneben gibt Microsoft zusätzlich noch Sicherheitsempfehlungen heraus, die Anleitungen und schadensbegrenzende Maßnahmen zur Beseitigung von öffentlich bekannten Sicherheitsschwachstellen beschreiben.
Die Patches (Microsoft spricht von Sicherheitsupdates) können manuell eingespielt werden oder automatisch über Softwareverteilprogramme. Microsoft selbst bietet mit den Windows Server Update Services (WSUS) eine Patch- und Updatesoftware an. Sie besteht aus einer Server- und einer Clientkomponente. WSUS unterstützt die Administratoren, Microsoft-Updates in großen lokalen Netzwerken auszuliefern. Es lädt Updatepakete aus dem Internet (Microsoft Update) und bietet sie den Windows-Clients zur Installation an. Der WSUS-Administrator kann am Server festlegen, welche Computer welche Updates installieren sollen. Microsoft stellt die Windows Server Update Services kostenlos zur Verfügung.
Laut einer Erhebung des Virenschutzunternehmens Sophos [Quelle 11] nutzen 66% der IT Manager dieses Werkzeug. Weitere 9% nutzen Lösungen von anderen Herstellern. Immerhin 25% patchen ihre Systeme nicht.

Laut Sophos hat das Windows Server Update Tool Schwächen in der Patch-Überwachung und meint damit, dass nicht sichergestellt ist, ob die einzelnen Systeme wirklich ordnungsgemäß gepatcht wurden.
Weiter führt Sophos in seinem Schreiben aus, dass WSUS über keine zuverlässige Berichtsfunktion verfügt, die Aufschluss darüber geben könnte, welche Patches auf ausgewählten Computern installiert wurden. Zudem wird nicht über alle Patches berichtet. WSUS berichtet lediglich über Patches, die zur Richtlinie der Windows Domäne hinzugefügt wurden. Der Genauigkeitsgrad der Berichte kann außerdem durch Benutzer verfälscht werden, die eine Patch-Installation unterbrechen oder während dieser einen Neustart vornehmen.
Auch kann WSUS keine Benutzer mit Administratorrechten erkennen, die bestehende Betriebssystem-Patches durch eigene Anpassungen unwirksam machen können.
Die Lösung sieht Sophos in der sogenannten End Point Security. Das ist ein Softwareagent, welcher das Patchen auf den einzelnen Endgeräten überwacht und den Status an die dazugehörige Serverkomponente meldet. Windows selbst bietet mit dem System Center Configuration Manager (SCCM) ebenfalls ein solches Tool an, welches auf einem vorhandenen WSUS Server aufbaut. Sowohl die Lösung von Microsoft, als auch die von Sophos oder anderer Anbieter verursachen zusätzliche Lizenzgebühren.

Microsoft bietet mit dem Microsoft Baseline Security Analyzer (MBSA) [Quelle 12] auch ein kostenloses Tool zur Überprüfung des Patchlevels an. Allerdings ist es notwendig, für jeden zu überprüfenden Computer über Administratorberechtigungen zu verfügen. Daher greift dieses Verfahren nur für Systeme, die entweder in die Domäne des Krankenhauses eingebunden sind oder bei der lokalen Installation des MBSA auf dem zu überprüfenden System.
Die Möglichkeit, eine End Point Security Software oder den MBSA auf Client Systemen zu installieren, scheidet für die meisten Medizinprodukte aus, da sie von den Herstellern nicht validiert ist. Die Installation einer solchen Software auf einem Medizinprodukt kann eine wesentliche Änderung darstellen, die vom Hersteller des Medizinproduktes vor Installation freigegeben werden sollte. Andernfalls läuft der Betreiber Gefahr, dass der Hersteller sich aus der Herstellerkonformität zurückzieht. Zum anderen muss immer grundsätzlich geprüft werden, ob eine End Point Security Software in irgendeiner Weise Echtzeit-Verarbeitung von Daten beeinträchtigen kann, sodass ein eigenständiger Einsatz einer solchen Software immer vom Hersteller des Medizinproduktes freigegeben werden sollte.
Erst wenn eine End Point Security Software Bestandteil des Betriebssystems wird, ist damit zu rechnen, dass auch Medizinproduktehersteller diese Lösung flächendeckend unterstützen.

3.3 Warum kann ein nicht gepatchtes Betriebssystem eine Gefährdung darstellen? a) generell und b) speziell in der Medizintechnik?

Bekanntermaßen kann Software nicht absolut fehlerfrei entwickelt und programmiert werden. Diese Problematik betrifft auch Betriebssysteme, die dadurch Fehler z. B. bei der Anzeige auf einem Display aufweisen aber auch sicherheitsrelevante Lücken beinhalten können, die durch Dritte ausgenutzt werden können. (Trojaner, Bot-Netzwerke, Key-Logger u. a. Gefährdungen wie Exploits)
Ein Exploit (englisch to exploit ‚ausnutzen') stellt in der Elektronischen Datenverarbeitung eine systematische Möglichkeit dar, mit Hilfe von Befehlsfolgen Sicherheitslücken und Fehlfunktionen von Programmen (oder ganzen Systemen) auszunutzen, die bei der Programmierung einer Software nicht erkannt wurden.
Das Ziel ist meist eine Manipulation, um sich Zugang zu Ressourcen zu verschaffen oder Systeme zu beeinträchtigen. [Quelle 13]
Das in Abschnitt 1.3 erwähnte Beispiel der Beschaffung eines Medizinproduktesystems, bestehend aus Linearbeschleuniger und Steuerrechner (Hardware, Betriebssystem, IT-Applikation in Form der Bestrahlungssoftware als Medizinprodukt) zeigt, welche Gefährdungen entstehen können, wenn vor der Beschaffung das Thema der Betriebssysteme und des Patchmanagements vernetzter Medizinprodukte nicht geklärt wird.
Auf dem Steuerrechner des Linearbeschleunigers gemäß Abbildung 3 wurde kein Patchmanagement bei der Beschaffung vorgesehen und nach Installation des Systems auch nicht eingerichtet. Das Betriebssystem verblieb ungepatcht, sodass sich nach einiger Zeit der sogenannte Conficker-Wurm aus dem IT-Netzwerk des Krankenhauses in dem Betriebssystem einnistete. Der Conficker führte zu keiner direkten Patientengefährdung im Sinne fehlerhafter Bestrahlung sondern sorgte durch sein typisches Verhalten indirekt zu einer Beeinträchtigung der Patientenversorgung im gesamten Krankenhaus.
Der Conficker versucht, Nutzer-Accounts zu knacken, die mit einfachen Passwörtern wie „Start; Heute u. a.) hinterlegt sind. In dem Beispiel führte dieses Verhalten des Conficker dazu, dass am Morgen eines Arbeitstages etliche Ärzte und Pflegepersonal sich nicht in ihren Account einloggen und somit nicht arbeiten konnten, weil die Accounts nach mehrfachem Einwahlversuchen mit falschen Passwörtern automatisch gesperrt wurden.
In Konsequenz bedeutete dies, dass Anwender nicht arbeiten konnten und somit Patienten nicht behandelt bzw. verlegt/verwiesen werden mussten, teilweise auch OP-Termine abgesagt wurden.
Erst das Einspielen des MS-Patches, der verhindert, dass der Conficker weiter auf dem Steuerrechner tätig war, beendete die Situation.
Auch wenn Patienten nicht direkt durch diesen Virus geschädigt wurden, so ergaben sich für etliche Patienten Unannehmlichkeiten und Widrigkeiten, die letztendlich auch zu Einnahmeausfällen des betreffenden Krankenhauses führten.

3.4 Betreiberpflicht: Instandhaltung von Medizinprodukten

Der Betreiber ist nach der Medizinprodukte-Betreiberverordnung gemäß § 2 Abs. 5 verpflichtet, Medizinprodukte instand zu halten.
Er darf sie nicht betreiben, wenn von ihnen Gefahren ausgehen, die Patient, Anwender oder Dritte gefährden können. Aus heutiger Sicht kann somit ein ungepatchtes Betriebssystem eine Gefährdung und je nach Bewertung und Einsatzsituation ein Risiko darstellen.

Das regelmäßige Patchen eines Betriebssystems eines Medizinproduktes fällt also unter die Instandhaltungspflichten eines Betreibers, wenn dieses vernetzt ist und eine Gefährdung durch Malwarebefall u. a. besteht oder bestehen kann.
Juristen sprechen in diesem Zusammenhang von den sogenannten Verkehrssicherungs-pflichten, die der Betreiber über seine Mitarbeiter sicherstellen muss.
Abbildung 3 zeigt daher exemplarisch, wie wichtig und notwendig es ist, dass Hersteller und Betreiber gemeinsam vor Beschaffung und Installation vernetzbarer Medizinprodukte die Anforderungen an die Instandhaltung der Produkte mit unterschiedlichen Lebenszyklen klären und vereinbaren, damit der Betreiber nicht unwillentlich bzw. unwissentlich in die Herstellerkonformität eintritt.

3.5 Versions- und Konfigurationsmanagement

Um Betriebssysteme aktuell zu halten, benötigt der Betreiber Informationen über den Soll- und Ist-Zustand der Produkte. Es ist Herstelleraufgabe, dem Betreiber Informationen zum validierten Sollzustand seiner Produkte zur Verfügung zu stellen. Der Betreiber hat die Aufgabe, den Istzustand zu überwachen und die Anpassung an den Sollzustand zeitnah umzusetzen. Dafür sollten mit jedem Hersteller/Lieferanten Vereinbarungen über das Versions- und Konfigurationsmanagement getroffen werden.
Diese Fragen sollten daher unbedingt vor einer Beschaffungsentscheidung bzw. vor der Auftragsvergabe eindeutig, auch in Hinblick auf Wartungsverträge vom Betreiber mit dem Hersteller geklärt werden.
Ein Wartungsvertrag für ein in Abbildung 3 beispielhaft gezeigtes Medizinproduktesystem sollte also bereits Vereinbarungen für das Patchmanagement des Betriebssystems und für die erforderliche Migration auf neue Hardware und Betriebssysteme im Laufe des Lebenszyklus beinhalten. Mit einer solchen grundsätzlichen Vereinbarung gewinnen Hersteller und Betreiber gemeinsam nicht nur Verhaltens- und Planungssicherheit sondern erfüllen auch einen Teil ihrer Verkehrssicherungspflichten.

3.6 Bereitstellung von Informationen

Damit der Betreiber geeignete Maßnahmen planen und anschließend umsetzen kann, benötigt er weiterführende Informationen vom Hersteller des Medizinproduktes. Idealerweise werden die entsprechenden Informationen schon vor der Beschaffung eingeholt bzw. zur im Beratungsgespräch zur Verfügung gestellt.

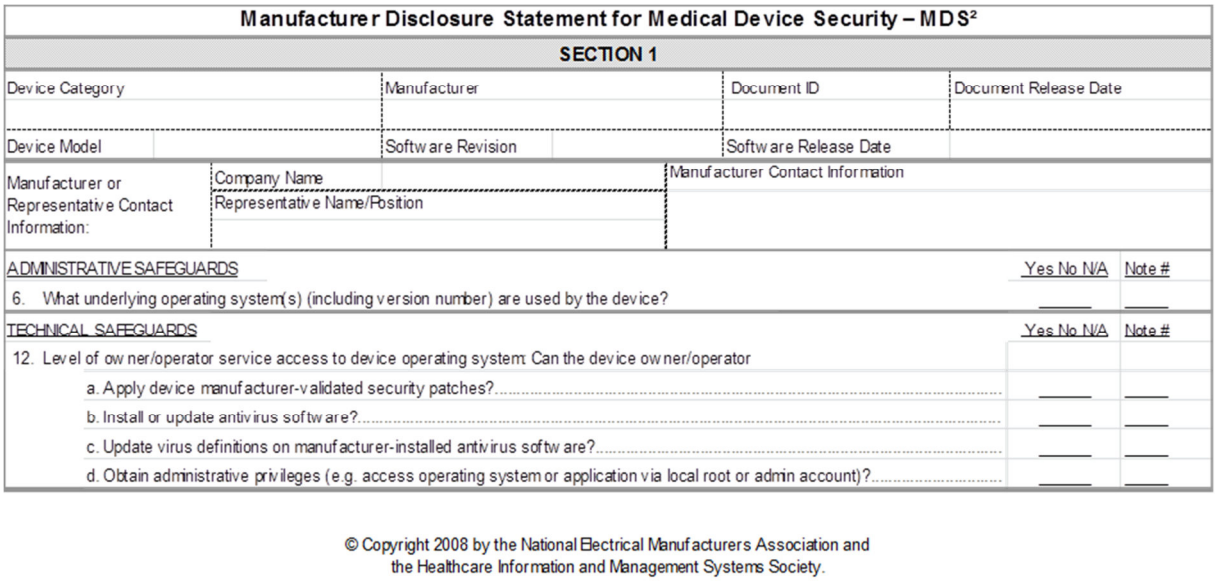
Der Betreiber kann diesen Prozess beschleunigen, in dem er die gewünschten Informationen exakt anfragt bzw. einfordert. Bewährt hat sich die Anfrage mittels Checkliste unter Verweis auf die DIN EN 80001-1 [Quelle 14] oder bei global aktiven Anbietern die Frage nach der Herstellererklärung „Manufacturer Disclosure Statement for Medical Device Security - MDS2“ der Nema (National Electrical Manufacturers Association).
Einige Hersteller stellen allein zu diesem Zweck einen Internetzugang bereit. Andere Hersteller gestallten ihre Produkte so, dass sie den Release Stand des Betriebssystems dem eingewiesenen Betreuer im Haus mitteilen.

3.6.1 Checkliste nach DIN EN 80001-1

Die DIN EN 80001-1 geht davon aus, dass die von der Obersten Leitung beauftragten Personen vom Hersteller eines Medizinproduktes entsprechende Informationen erhalten, um ihrer Aufgabe gerecht zu werden bzw. ein Risikomanagement durchzuführen zu können. Zu diesem Zweck hat die Deutsche Krankenhausgesellschaft (DKG) eine Checkliste entworfen. [Quelle 15]
Durch Lieferung der in der Checkliste geforderten Gebrauchsanweisung des Medizinproduktes und Beantwortung der Frage zur Vorgehensweisen zum Virenschutz und Software-Updates sollte erkennbar sein, welches Betriebssystem zum Einsatz kommt, in welchem Patchzustand es ausgeliefert wird und wie der Hersteller die laufende Aktualisierung unter Beibehaltung der Herstellerkonformität grundsätzlich durchführt.

3.6.2 Manufacturer Disclosure Statement (MDS2)

Bietet ein Hersteller seine Produkte in den Vereinigten Staaten von Amerika an, kann er für vernetzbare Medizinprodukte ein „Manufacturer Disclosure Statement for Medical Device Security – MDS2“ [Quelle 16] erstellen. Es wurde von der „National Electrical Manufacturers Association“ (NEMA) in Zusammenarbeit mit der „Healthcare Information and Management Systems Organisation“ (HiMSS) entwickelt. Dieses kann auch in Deutschland als Quelle für die benötigten Herstellerinformationen genutzt werden.



Manufacturer Disclosure Statement for Medical Device Security – MDS²			
SECTION 1			
Device Category	Manufacturer	Document ID	Document Release Date
Device Model	Software Revision	Software Release Date	
Manufacturer or Representative Contact Information:	Company Name Representative Name/Position	Manufacturer Contact Information	

ADMINISTRATIVE SAFEGUARDS	Yes No N/A	Note #
6. What underlying operating system(s) (including version number) are used by the device?		
TECHNICAL SAFEGUARDS	**Yes No N/A**	**Note #**
12. Level of owner/operator service access to device operating system: Can the device owner/operator		
a. Apply device manufacturer-validated security patches?		
b. Install or update antivirus software?		
c. Update virus definitions on manufacturer-installed antivirus software?		
d. Obtain administrative privileges (e.g. access operating system or application via local root or admin account)?		

Abbildung 5: Auszug des MDS 2 Formulars der NEMA [Quelle 16]

In Punkt 6. beantwortet der Hersteller die Frage nach dem Betriebssystem: *„Welches bzw. welche zugrundeliegende(n) Betriebssystem(e) (inklusive Versionsnummer) werden vom System genutzt?“*
Der Punkt 12. verlangt Auskünfte über die Vorgehensweise, die der Hersteller ans Patchmanagement stellt. Es wird erfragt, ob der Eigentümer oder Betreiber Service-Zugriff auf das Betriebssystem des Systems hat.

Der Punkt 12a ist von entscheidender Bedeutung!
Kann der Betreiber des Systems vom Gerätehersteller validierte Sicherheits-Patches einspielen?
Schon aus der Fragestellung heraus wird deutlich, dass laut amerikanischer Herstellervereinigung keine Sicherheitspatches auf ein Medizinprodukt eingespielt werden sollten, welche nicht durch den Hersteller validiert, d. h. freigegeben worden sind.
Die regulatorische Konsequenz ist, dass Medizinprodukte nicht in das Standard Patchmanagement der IT Abteilung eingebunden werden können, aber die Realität in den Krankenhäusern sieht anders aus.
Nachfolgend werden die Informationsangebote einiger Hersteller in Deutschland **beispielhaft** vorgestellt. Die Auflistung stellt keinerlei Wertung dar, sondern hat nur informativen Charakter. Sie gibt einen Überblick über die Möglichkeiten von Herstellern ihren Kunden die notwendigen Informationen bereitzustellen.

3.6.3 Herstellerinformationen

Informationen anzufragen, ist zeitaufwendig. Wenn Hersteller die Daten zum Abholen bereitstellen, ist dies ein Vorteil. Die Firmen GE und Philips bieten ihren Kunden Zugriff auf Sicherheitsdatenbanken (Product Security Databases) an. Dort wird der Zugriff auf die „Manufacturer Disclosure Statements for Medical Device Security“ ermöglicht. Somit ermittelt man das Betriebssystem seiner Systeme. Zusätzlich gibt

es Tabellen zum Produkt - Patch Mapping. Sie zeigen die freigegebenen Patches der einzelnen Systeme.

Die Abbildungen 6 und 7 zeigen die Security Informationsportale der Herstellers General Electric (GE) und Philips Medizin Systeme (PMS), die Tabellen 5 und 6 die jeweiligen Resultate einer Patchlevel Abfrage.

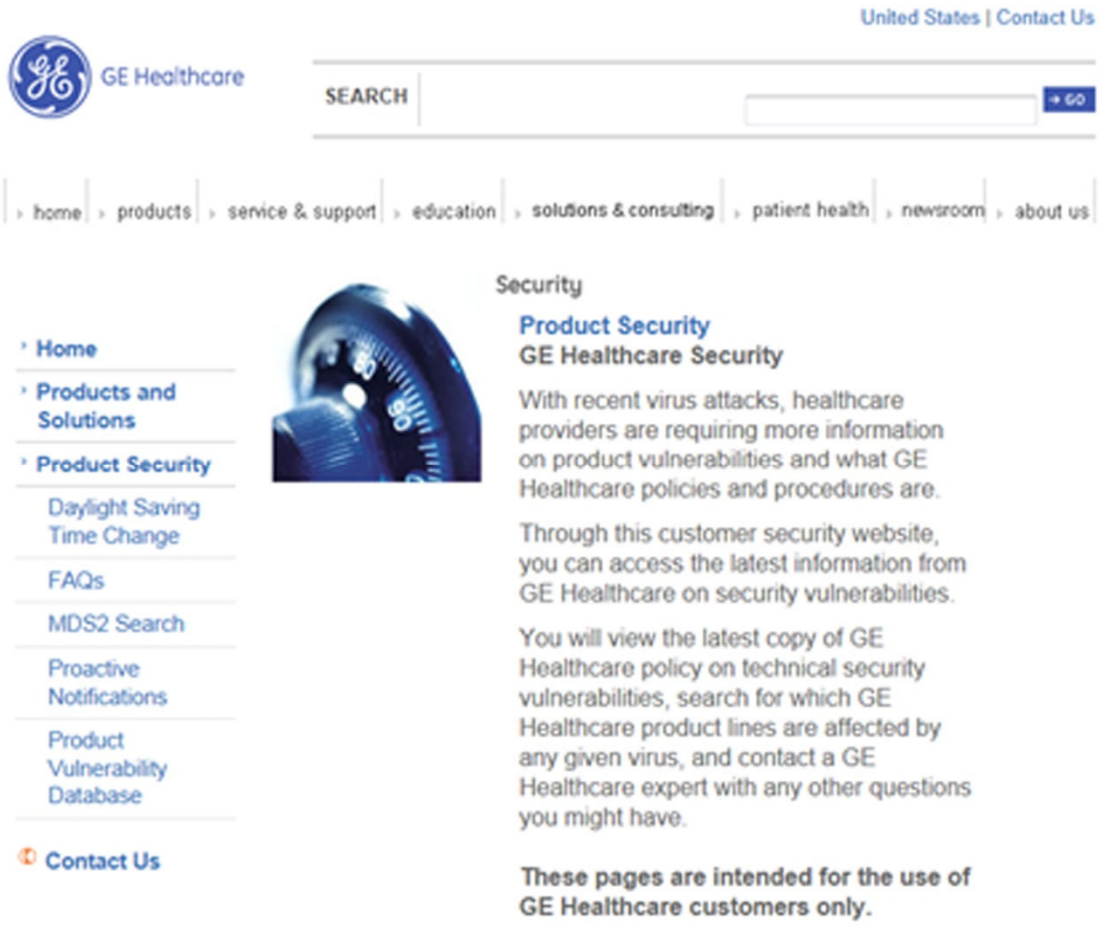


Abbildung 6: Informationsportal Fa. GE

Product - Patch Mapping Search Result

Search By : Product Name/Keyword = Mac-Lab/CardioLab/Specials/ComboLab IT/XT/XTi, Product Version = 6.9

5 Items found, displaying all items.

Product Name/Version	Patch Identifier	Patch Assessment Status	Patch Assessment Date	Patch Assessment Details
Mac-Lab/CardioLab/Specials/ComboLab IT/XT/XTi/6.9	MS12-054	Patch Approved	31-August-2012	
Mac-Lab/CardioLab/Specials/ComboLab IT/XT/XTi/6.9	MS12-053	Patch Approved	31-August-2012	
Mac-Lab/CardioLab/Specials/ComboLab IT/XT/XTi/6.9	MS12-036	Patch Approved	28-June-2012	
Mac-Lab/CardioLab/Specials/ComboLab IT/XT/XTi/6.9	MS12-020	Patch Approved	22-March-2012	
Mac-Lab/CardioLab/Specials/ComboLab IT/XT/XTi/6.9	MS12-004	Patch Approved	03-February-2012	

Tabelle 5: Patchlevel Elektrophysiologischer Messplatz, GE [Quelle 17]

Abbildung 7: Informationsportal Fa. Philips Medizin Systeme

PHILIPS

Note: Only Philips certified service personnel are to make changes to the system, including vulnerability patching, on this Philips medical device.

iE33				Applicable patches as of 2013-01-17
Version 6.3.1				Operating system not specified
Vulnerability / Patch ID	Last update by Philips	Activity Status	Recommended Customer Action	Notes / Instructions
MS13-008	2013-01-17	Already mitigated	None	Requires viewing a specially crafted or compromised website, which is not possible through normal use of the system.
MS13-007	2013-01-17	Already mitigated	None	The system utilizes a firewall configuration that blocks inbound HTTP connections.
MS13-006	2013-01-17	Not applicable	None	Vulnerability is not applicable to the installed Operating System
MS13-005	2013-01-17	Not applicable	None	Vulnerability is not applicable to the installed Operating System
MS13-004	2013-01-17	Already mitigated	None	Requires viewing a specially crafted or compromised webpage or running a specially crafted .NET application, none of which is possible through normal system use.
MS13-003	2013-01-17	Not applicable	None	Microsoft System Center Operations Manager is not installed
MS13-002	2013-01-17	Already mitigated	None	Requires viewing a specially crafted webpage, which is not possible through normal use of the system.

Tabelle 6: Patchlevel Ultraschallgerät IE33, Philips Medizin Systeme [Quelle 18]

3.6.4 Geräteinformationen

Sehr hilfreich ist es, wenn die Medizinprodukte selbst Auskunft über ihren Software Release Stand geben können. Die Speicherfoliensysteme der Firma Carestream bieten Systembetreuern diese Möglichkeit, wie in den Abbildungen 8 und 9 beispielhaft gezeigt wird.

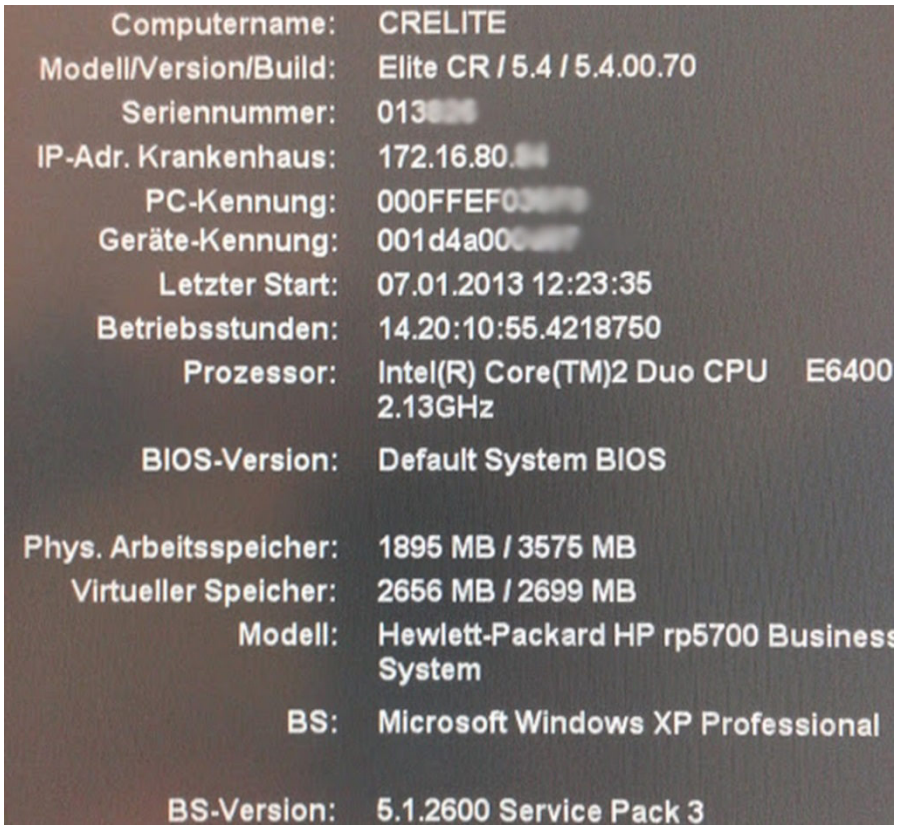


Abbildung 8: Carestream CR Elite Systemauskunft

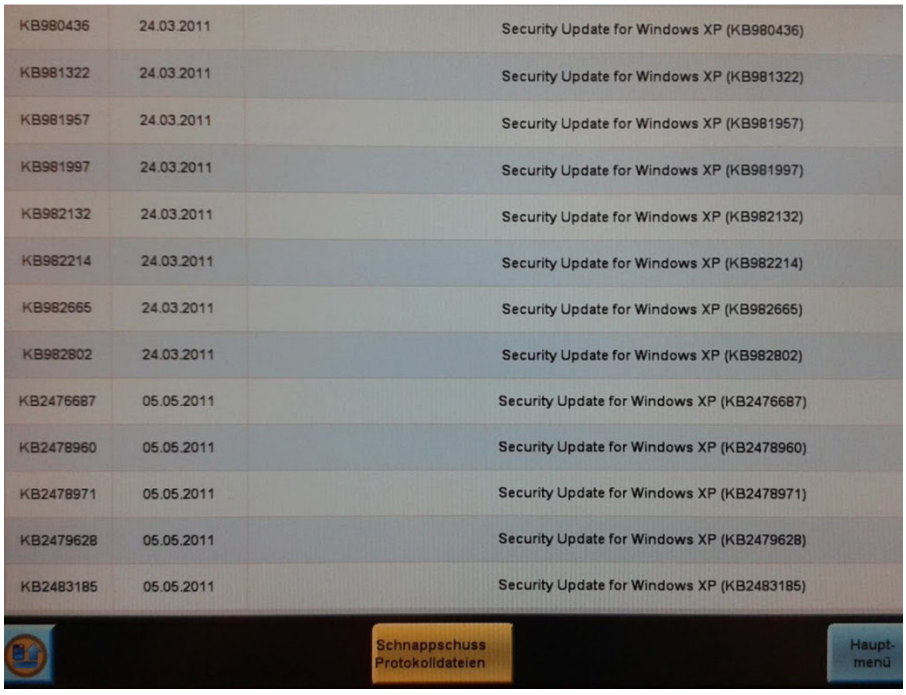


Abbildung 9: Carestream CR Elite Liste der installierten Microsoft Update Komponenten

Beispiel der Umsetzung in der St. Bonifatius Hospital gGmbH

Die vorgestellten Wege zur Informationsbeschaffung bilden die Grundlage für eine Vertragsgestaltung mit dem Hersteller oder Lieferanten eines Medizinproduktesystems.

Im Zuge der Planung eines Schlaflabors mit sechs Plätzen und einer zentralen Datenbank wurden Hersteller/Anbieter durch die mit der Beschaffung beauftragten Bereiche Wirtschaftsabteilung und Medizintechnik aufgefordert, eine Checkliste nach DIN EN 80001-1 zu beantworten.
Der Lieferant Heinen + Löwenstein stellte zusätzlich die MDS² Formulare des Herstellers Philips Respironics bereit.

Das System (Abbildung 10) beinhaltet mehrere Komponenten auf der Basis von PC-Betriebssystemen: Die Basisstation mit Linux, welche die physiologischen Daten des Patienten erfasst und die Arbeitsstation mit Microsoft Windows 7 Professional, welche zur Visualisierung, Aufzeichnung und Auswertung der erfassten Daten dient. Zusätzlich wird die Installation der Datenbank auf einem Windows Server 2008 realisiert, auf den die einzelnen Arbeitsstationen zugreifen.

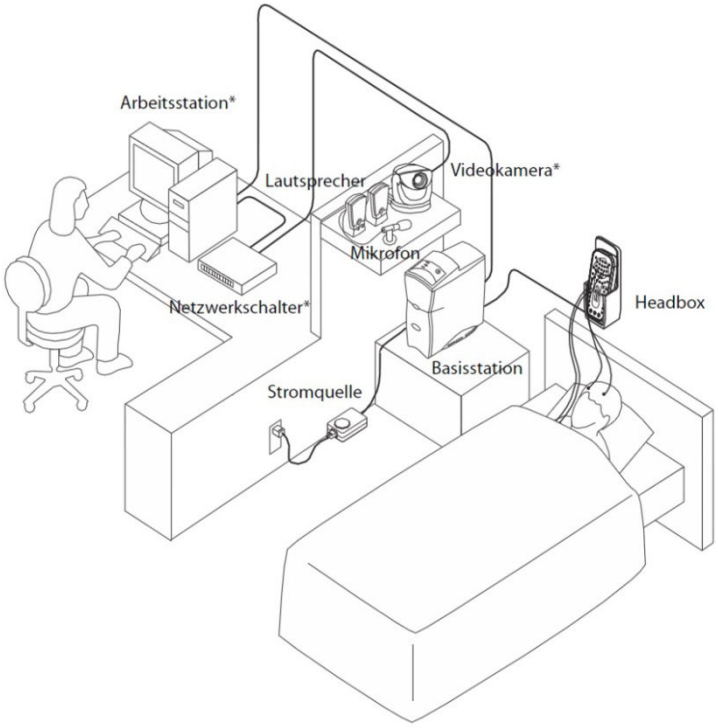


Abbildung 10: Aufbau eines Schlaflabors [Quelle 19]:

Das MDS² Formular der Basisstation zeigt, dass diese unter Linux 2.6.28 läuft. Durch das Statement im Punkt 12 a und der Erläuterung 5 + 7 wird ersichtlich, dass der geschulte Operator Sicherheitspatches auf die Basisstation einspielen darf. Das Einspielen der Patches wird über die Software (Sleepware) auf der Arbeitsstation realisiert.

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Sleep Diagnostics	Philips Healthcare	v2.0	May 4, 2012
Device Model: Alice 6	Software Revision: R5	Software Release Date	August 2011

Manufacturer or Representative Contact Information:	Company Name: Philips Healthcare	Manufacturer Contact Information
	Representative Name/Position: Product Security Manager	productsecurity@philips.com

ADMINISTRATIVE SAFEGUARDS	Yes No N/A	Note #
5. Does manufacturer offer operator and technical support training or documentation on device security features?	No	5
6. What underlying operating system(s) (including version number) are used by the device? Linux 2.6.28		
12. Level of owner/operator service access to device operating system: Can the device owner/operator		
a. Apply device manufacturer-validated security patches?	Yes	7
b. Install or update antivirus software?	No	
c. Update virus definitions on manufacturer-installed antivirus software?	No	
d. Obtain administrative privileges (e.g. access operating system or application via local root or admin account)?	No	

Abbildung 11: Auszug MDS² Formular Alice 6 [Quelle 20]

Durch das MDS² Formular für die Arbeitsstationen und den Server gibt der Hersteller verschiedene Microsoft Betriebssysteme frei. So ist es möglich, die Hardware und das Betriebssystem der Arbeitsstation beizustellen, auf dem der Hersteller dann sein Produkt (Sleepware) installieren kann.

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
Sleep Diagnostics	Philips Healthcare	v2.0	June 27, 2012
Device Model: Sleepware G3	Software Revision: 3.3.1	Software Release Date	June 21, 2012

Manufacturer or Representative Contact Information:	Company Name: Philips Healthcare	Manufacturer Contact Information
	Representative Name/Position: Product Security Manager	productsecurity@philips.com

ADMINISTRATIVE SAFEGUARDS	Yes No N/A	Note #
5. Does manufacturer offer operator and technical support training or documentation on device security features?	Yes	8
6. What underlying operating system(s) (including version number) are used by the device? See Note 7		
12. Level of owner/operator service access to device operating system: Can the device owner/operator		
a. Apply device manufacturer-validated security patches?	Yes	
b. Install or update antivirus software?	Yes	9
c. Update virus definitions on manufacturer-installed antivirus software?	Yes	11
d. Obtain administrative privileges (e.g. access operating system or application via local root or admin account)?	Yes	9

SECTION 2

EXPLANATORY NOTES (from questions 1 - 19)

IMPORTANT: Refer to Section 2.2.2 of this standard for the proper interpretation of information requested in this form

To view the full standard, please visit: http://www.nema.org/stds/hn1.cfm

7. Windows XP Pro, Vista Business, 7 Pro, Server 2003 & 2008.
8. At the customer's request, training sessions on the use of the device can address security features; during installation (instructions), the option to encrypt the ePHI is available.
9. Sleepware is software only. It is installed on a customer-owned, -maintained, and -secured computer.
10. Sleepware is software only. It is installed on a customer-owned, -maintained, and -secured computer, on a network managed by the customer. Remote system access is optional for software upgrades, user assistance and problem resolution. It is used with customer permission (audit trail data does not identify whether a given activity is done remotely).
11. Philips Respironics does not validate operating system patches. Owner/operator/customer is responsible for downloading operating system patches and antivirus software.

Abbildung 12: Auszug MDS² Formular Sleepware G3 [Quelle 21]

Klärungsbedarf mit dem Hersteller/Lieferanten besteht, weil der Betreiber zwar durch die Anmerkungen in Punkt 9 und 10 die Freiheit hat, zumindest die Arbeitsstation und den Datenbankserver selbst zu verwalten. Das Einspielen von Sicherheitspatches für die Basisstationen über die Sleepware Software ist nur für geschultes Personal erlaubt. Das Patchen des Betriebssystems kann also in Eigenleistung durchgeführt werden. Wie aus Punkt 12.a. ersichtlich ist, benötigt man dazu die Information, welcher Patchstand vom Hersteller validiert ist.

Fazit: Die Kommunikation mit dem Hersteller/Lieferanten vor der Beschaffung von Medizinprodukten erlaubt es, ein für beide Seiten tragfähiges Konzept aufzustellen. Dieses wird dann vertraglich fixiert.
Im konkreten Beispiel besteht die Möglichkeit, nach Information über den validierten Patchlevel und/oder die Übermittlung der Sicherheits-Patches durch den Hersteller oder Lieferanten, diese als Krankenhaus selbst einzuspielen oder den Lieferanten mit diesen Aufgaben zu beauftragen, ohne die Herstellerkonformität mit der Medizinprodukte-Richtlinie zu tangieren.

4. Beschaffungsprozesse von Medizinprodukten mit Betriebssystemen

Plant ein Krankenhaus die Beschaffung eines vernetzbaren Medizinproduktes, so muss es durch eine entsprechende Ablauforganisation und/oder Projektmanagement sicherstellen, dass Hersteller/Lieferanten über Abfragen und/oder Ausschreibungen Angaben dazu liefern, welches Betriebssystem das anzubietende Medizinprodukt enthält, in welchem voraussichtlichen Patchzustand das Produkt ausgeliefert werden kann bzw. wie der Hersteller das Patchmanagement über den Lebenszyklus des Medizinproduktes sicherstellt.
Eine solche Abfrage seitens der Krankenhäuser und Angaben seitens der Hersteller sind bis heute nicht selbstverständlich und müssen daher aktiv eingefordert werden, damit der Betreiber seine Sorgfaltspflicht bzw. Verkehrssicherungspflicht bei der Instandhaltung von Medizinprodukten aus **Gründen der Haftungsprävention** nachkommt.

4.1 Berücksichtigung der Betriebssysteme von Medizinprodukten/-systemen in Wartungsverträgen

Schließt ein Krankenhaus einen Wartungsvertrag für ein Medizinprodukt bzw. Medizinproduktesystem ab, so muss es unbedingt dabei berücksichtigen, das Patchmanagement des verwendeten Betriebssystems unter Einhaltung der Herstellerkonformität zu fixieren. Erforderlichenfalls sollten auch bereits bestehende Wartungsverträge bezüglich dieser Aspekte überarbeitet und mit dem Hersteller zusammen angepasst werden.
Nachfolgende Beispiele von aktuellen Wartungsverträgen einiger radiologischer Modalitäten aus dem St. Bonifatius Hospital zeigen, dass das Patchen der eingesetzten Betriebssysteme durch Hersteller **durchaus schon Berücksichtigung findet**. Die Schwachstelle findet sich im Bereich der Information. Der Betreiber

bekommt standardmäßig keinen Nachweis über die Durchführung des Patchens und kann nur darauf vertrauen, dass der Hersteller seinen Pflichten nachkommt.

Qualitätssicherung und Update

- *Durchführung der von Siemens zur Verbesserung der Nutzungssicherheit und Betriebsbereitschaft als notwendig erachteten technischen Änderungen (Updates) einschließlich der dazu benötigten Hard- und Software.*
- *Beseitigung von Programmfehlern[2] in der aktuellen oder früheren SW – Versionen durch kostenlose Bereitstellung von SW – Korrekturen (Updates und patches[3]) und Installation dieser SW – Korrekturen über Remoteanschluss, wenn möglich*
- *Dokumentation der Leistungen*

[2] Programmfehler sind Abweichungen von der im Benutzerhandbuch beschriebenen Funktionalität und Schwachstellen, die zu sicherheitsrelevanten Störfällen führen können. Fehler in diesem Sinne sind reproduzierbar.
[3] Soweit SW Updates verfügbar sind.

Auszug aus Siemens Dienstleistungsvereinbarung Performance Top für CT/MR [Quelle 22]

Technische Modifikationen die durch Rechtsvorschriften erforderlich werden.
Zusätzliche Leistungen bei rechnergestützten Anlagen:

- *Software-Updates des Betriebssystems zur Erhaltung der spezifizierten Funktion des Systems.*
- *Hardware-Updates zur Erhaltung der spezifizierten Funktionen des Systems auf dem Stand der Technik.*

End of Live

Erreichen Systeme bzw. deren Komponenten während der Dauer des Vertrags den Status "end of live", so ist dies von Philips schriftlich anzuzeigen. Befindet sich das System/ die Komponente im Vertragsstatus „Vollservice" so greift das bestmögliche Leistungsverfahren (Best effort). In diesem Fall wird das System / die Komponente weiterhin mit allen Serviceleistungen und Ersatzteilen betreut. Kann das System / die Komponente zu einem bestimmten Zeitpunkt von Philips nicht mehr instandgesetzt werden, so endet der Vollservicevertrag ab diesem Zeitpunkt.

Auszug aus einem Rahmenvertrag Philips Medizin Systeme Vertragstyp Silver für einen volldigitalen Buckyarbeitsplatz [Quelle 23]

4.2 Medizinprodukte ohne Wartungsverträge

Eine zwingende Verpflichtung, einen Dienstleistungsvertrag über das Patchmanagement abzuschließen, besteht nicht. Es obliegt dem Betreiber, zu entscheiden, wie der sichere Betrieb der Anlagen gewährleistet wird. Die Leistung kann extern vergeben oder durch das im Haus vorhandene Personal erbracht werden.
Für vernetzbare Medizinprodukte, die keinem Wartungsvertrag unterliegen, sollten in jedem Fall die folgenden Fragen mit dem Hersteller diskutiert und geklärt werden:

- Wie oft bietet der Hersteller validierte Patches für seine Systeme an?

- Können diese per Remote eingespielt werden oder sind Vor-Ort Einsätze nötig?
- Bietet der Hersteller Servicelehrgänge für Krankenhausmitarbeiter an?
- In welcher Weise wird das BS Windows XP auf Medizinprodukten genutzt? Welche Funktionen sind aktiv und welche nicht?
- Entstehen durch die Integration eines solchen Produktes in das IT-Netzwerk des Betreibers Gefährdungen und wenn ja, wie sind diese zu minimieren?
- Und andere Fragestellungen.

Es empfiehlt sich, diese Fragestellungen **systematisch** mit Herstellern zu klären.

5. Bedeutung der Ankündigung des Endes des Supports für die Betriebssysteme Windows XP, Windows XP embedded und Windows 7 ohne SP

Der kostenfreie Support durch Sicherheitspatches der Produkte Microsoft Windows XP Professional läuft am 08.04.2014, der für Microsoft Windows XP Embedded am 12.01.2016 und der für Windows 7 ohne Service Pack am 09.04.2013 [Quelle 24] aus.
EKG-, EEG-, Lungenfunktions-, Ultraschall- oder gefäßdiagnostische Systeme werden auch 2013 vereinzelt noch mit den Microsoft Software-Produkten Windows XP oder Windows XP embedded angeboten. Der Anschaffungspreis der Systeme liegt zwischen € 15.000 bis €25.000. Spezialsysteme können auch deutlich hochpreisiger sein. Bei geschätzten 3% Instandhaltungskosten fallen somit über zehn Jahre € 4.500 bis € 7.500 Instandhaltungskosten an.
Aus heutiger Sicht ist ein Krankenhaus gut beraten, wenn vor der Beschaffung eines vernetzbaren Medizinproduktes die Folgekosten für das Patchen eines Betriebssystems bzw. eine mögliche Migration auf ein Nachfolgebetriebssystem im Lebenszyklus des Medizinproduktes oder Medizinproduktesystems ermittelt werden.
In Anbetracht unterschiedlicher Lebenszyklen von Medizinprodukt und Betriebssystemen können sich durch die Notwendigkeit der Aktualisierung/Migration vernetzter Medizinprodukte auf ein Nachfolge-Betriebssystem zukünftig entweder die Nutzungszeiten drastisch verkürzen und/oder die Instandhaltungskosten über den Lebenszyklus deutlich erhöhen. Diese Auswirkungen sollten im Vorfeld der Beschaffung eines vernetzbaren Medizinproduktes betrachtet werden.

Soll die Herstellerkonformität erhalten bleiben, muss das Aufspielen eines aktuellen Nachfolge-Betriebssystems auf ein Medizinprodukt durch den Hersteller erfolgen, da anschließend die Applikationssoftware installiert und das Zusammenspiel geprüft werden muss.
Alternativ kann ein Hersteller auch dem Betreiber durch eine schriftliche Freigabe autorisieren, auf ein Nachfolgebetriebssystem zu migrieren, unter Beibehaltung der Herstellerkonformität.
Es ist davon auszugehen, dass Hersteller Betreibern weiteren Support von Medizinprodukten mit Windows XP Professional nach der Einstellung des Supports von MS anteilig in Rechnung stellen (werden).

6. Bedeutung für Krankenhäuser und Arztpraxen

Ein Betreiber sollte daher einen Überblick haben bzw. ermitteln, welche und wie viele Produkte eines Krankenhauses mit welchen Betriebssystemen, z. B. Windows XP u. a. betrieben werden. Dies bedeutet, dass sowohl die IT-Abteilung als auch die Medizintechnik ermitteln, wie viele und welche Produkte (Bürorechner als auch Medizinprodukte sowie Medizinproduktesysteme mit Rechner) mit Betriebssystem wie XP eingesetzt werden.

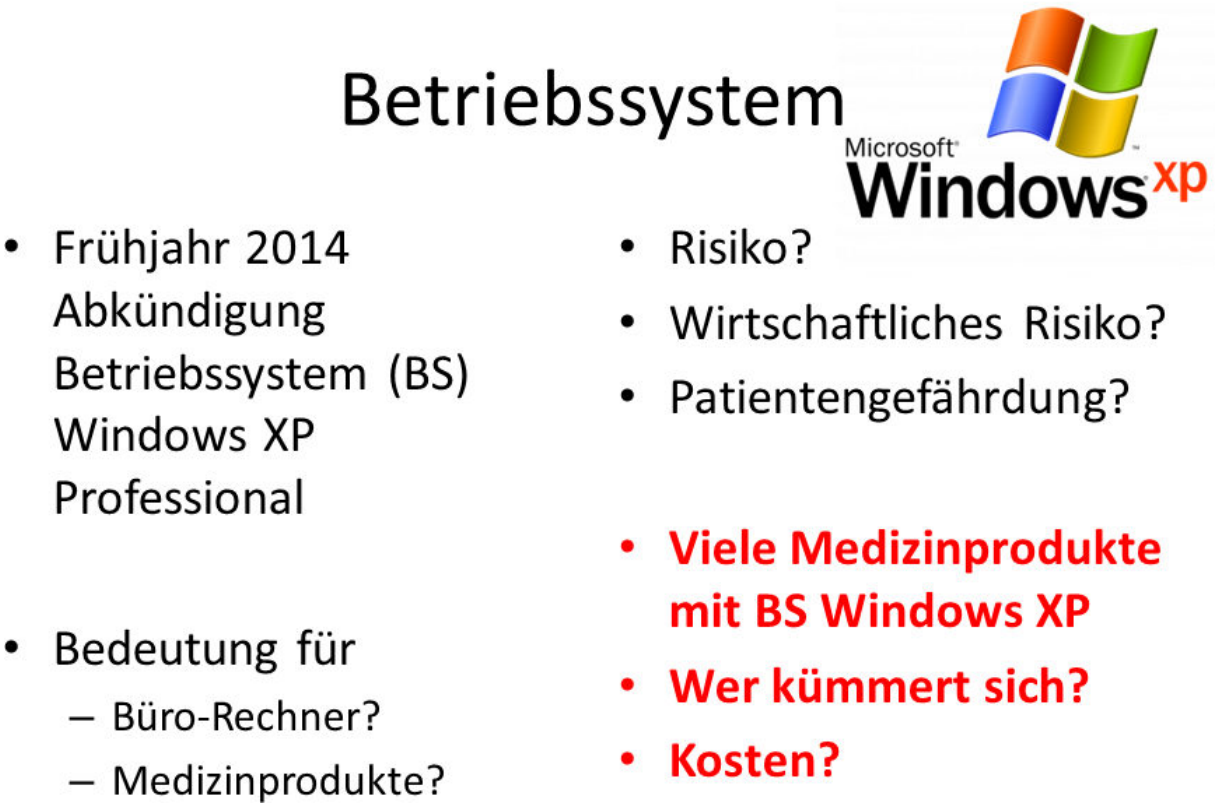


Abbildung 13: Mögliche Risikobetrachtung Betriebssystem Windows XP

Besteht ein solcher Überblick, muss mit den Herstellern von Medizinprodukten geklärt werden, ob und welche Gefährdungen und Risiken bestehen:

- Gefährdung der Patientenversorgung durch ein veraltetes, nicht mehr gepatchtes Betriebssystem?
- Wirtschaftliche Risiken bei Büro-Rechnern (Ersatzplanung)?
- Wirtschaftliches Risiko durch zukünftig nicht mehr durch den Hersteller kostenfrei gepflegte Betriebssysteme von Medizinprodukten?
- Weiterbetrieb von Medizinprodukten mit Windows XP mit erhöhten Betriebskosten durch Mehraufwand der Hersteller für den kostenpflichtigen Support nach Frühjahr 2014?
- In welcher Form wird das BS XP auf den Medizinprodukten betrieben? Welche Komponenten werden genutzt und welche nicht?

- Kann durch ein nicht mehr gepatchtes Betriebssystem Windows XP in irgendeiner Form eine Gefährdung für die Patientenversorgung entstehen?
- Besteht ein wirtschaftliches Risiko durch eine hohe Anzahl von zu ersetzenden alten Betriebssystemen?
- Kann auf ein Nachfolge-Betriebssystem mit einem anderen Sicherheitsstandard migriert werden?
- Besteht ein quantitativer Überblick über die betroffenen Produkte, kann ein Betreiber eine Strategie definieren, wie es mit dieser Situation umgeht, indem es Produkte mit Windows XP mit möglichen Mehraufwand weiterbetreibt oder aber die betroffenen Medizinprodukte weitestgehend auf ein neueres Betriebssystem konsolidiert, sofern dies möglich ist.

Wichtig: Auch wenn dies bisher nicht flächendeckend gesehen und betrieben wurde, das Patchen von Medizinprodukten und Rechnern in der Medizintechnik gehört aus juristischer Sicht zu den laufenden Instandhaltungspflichten eines Betreibers. Unterlässt ein Betreiber dies, verletzt er seine Sorgfaltspflichten bzw. die sogenannten Verkehrssicherungspflichten, um Patienten, Anwender und Dritte vor Schaden zu bewahren. Ein sorgfältiges Patchmanagement der eingesetzten Betriebssysteme nicht nur in der Medizintechnik gehört auch zur Haftungsprävention eines Betreibers.

Zumindest die Fachartikel in den einschlägigen Fachzeitschriften [Quelle 25] weisen darauf hin, dass Microsoft über April 2014 keine Sicherheitslücken des BS XP Professional mehr stopft. Das bedeutet, dass bei Weiternutzung mit jeder neu entdeckten Schwachstelle das BS XP immer unsicherer wird. Laut dem Verfasser des Artikels [Quelle 25] beruht Windows XP auf einer Sicherheitsarchitektur, die nicht mehr den heutigen Anforderungen entspricht
Aber nicht nur Sicherheitsgründe sollten den Betreiber veranlassen, sich mit dem Thema zu beschäftigen und eine Migrationsstrategie zu definieren: Mittlerweile entwickeln Hersteller von Peripherie-Hardware wie beispielsweise Drucker, keine aktuellen Treiber mehr für ihre neuen Modelle. Auch laufen neue Programme nicht mehr (unbedingt) auf Windows XP.
Allerdings zwingt die Migration auf ein neues Betriebssystem oftmals zu einem Update der Applikationen. Dies muss ebenfalls berücksichtigt werden.

7. Zusammenfassung

Betreiber von vernetzten Medizinprodukten sollten die Frage mit den Herstellern bzw. den Lieferanten klären, ob und in welcher Weise das Betriebssystem Windows XP oder Windows 7 ohne Servicepack auf den betreffenden Medizinprodukten eingesetzt wird und wie eine Migration auf ein aktuelles Betriebssystem erfolgen kann.
Parallel dazu sollten Betreiber bei Beschaffungen ab sofort die Thematik des eingesetzten Betriebssystems vernetzter Medizinprodukte im Vorfeld klären und eine verbindliche Patchstrategie mit den Herstellern festlegen, die auch in Wartungsverträgen über den Lebenszyklus eines Medizinproduktes wie Modalitäten

definiert sein muss, damit die Herstellerkonformität für ein zu patchendes Produkt erhalten bleibt.
Das Patchmanagement gehört zu den Instandhaltungspflichten des Betreibers. Führt er dies im Sinne einer Risikomanagementstrategie (auch nach DIN EN 80001-1) durch, erfüllt er seine Sorgfaltspflichten zu Haftungsprävention.

Stand 07.04.2013

8. Literatur und Quellenangaben

1. http://de.wikipedia.org/wiki/Betriebssystem, letzter Zugriff 25.02.2013
2. http://www.itwissen.info/definition/lexikon/DIN-44-300.html, letzter Zugriff 27.03.2013
3. Harte und weiche Echtzeitsysteme, Material zur Vorlesung Echtzeitsysteme an der Hochschule Niederrhein, Jürgen Quade, Kapitel 3. Realzeitbetriebssysteme https://ezs.kr.hs-niederrhein.de/lectures/ezs/html/c719.html, letzter Zugriff 06.04.2013
4. Microsoft Windows Embedded-Gesundheitslösungen, http://www.microsoft.com/windowsembedded/de-de/evaluate/windows-embedded-healthcare-oems.aspx , letzter Zugriff 15.02.2013
5. Eickenberg, R.; Auf verlorenem Posten – Windows XP vor dem Support-Aus, http://www.heise.de/ct/artikel/Auf-verlorenem-Posten-1771000.html, Heise Verlag, c´t, Ausgabe Nr. 2, 31.12.2012, S. 100 – 103, letzter Zugriff 22.03.2013
6. Wind River Education Services for Medical Applications http://www.windriver.com/education/solutions-medical.html letzter Zugriff 15.02.2013
7. Windows Embedded Betriebssystem; Auswahl; Medizin Geräte, http://www.microsoft.com/windowsembedded/de-de/evaluate/choose-a-windows-embedded-operating-system.aspx?DeviceTypeID=15, letzter Zugriff 22.03.2013
8. http://de.wikipedia.org/wiki/Eingebettetes_System, letzter Zugriff 25.02.2013
9. Gärtner, A.; Hersteller-Informationen gemäß DIN EN 80001 – Ein Vorschlag, 31.03.2011, http://www.e-health-com.eu/fileadmin/user_upload/dateien/Downloads/Gaertner_Hersteller-Informationen_zur_IEC_80001.pdf, letzter Zugriff 16.02.2013
10. DIN EN 62304:2007-03 Medizingeräte-Software - Software-Lebenszyklus-Prozesse
11. Sophos - In drei einfachen Schritten mehr Sicherheit beim Patch-Management erreichen, http://www.sophos.com/de-de/medialibrary/Gated%20Assets/white%20papers/sophosbetterpatchsecurity.pdf letzter Zugriff 16.02.2013

12. Microsoft Baseline Security Analyzer, http://technet.microsoft.com/de-de/security/cc184923.aspx, letzter Zugriff 22.03.2013
13. http://de.wikipedia.org/wiki/Exploit, letzter Zugriff 15.03.2013
14. DIN EN 80001-1:2011 Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten – Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten
15. Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Umsetzungshinweise für Krankenhäuser, (Hrsg.) Deutsche Krankenhausgesellschaft e. V, http://www.dkvg.de/product_info.php?info=p280_Anwendung-des-Risikomanagements-fuer-IT-Netzwerke--die-Medizinprodukte-beinhalten.html, letzter Zugriff 22.03.2013
16. Manufacturer Disclosure Statement for Medical Device Security, http://www.nema.org/standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx, letzter Zugriff 22.03.2013
17. GE Healthcare – Customer Product Security, http://www.gehealthcare.com/euen/customer-product-security/index.html, letzter Zugriff 15.02.2013
18. Philips Healthcare – Product Security, http://www.healthcare.philips.com/main/support/productsecurity/index.wpd, letzter Zugriff 15.02.2013
19. Philips Respironics, Benutzerhandbuch (REF 1083931) für Alice 6 Seite 23
20. Philips Healthcare, Manufacturer Disclosure Statement for Medical Device Security – MDS², Alice 6 - v2.0, 04.05.2012
21. Philips Healthcare, Manufacturer Disclosure Statement for Medical Device Security – MDS², Sleepware G3 - v2.0 27.06.2012
22. Dienstleistungsvereinbarung Performance Top für CT/MR Siemens mit dem St. Bonifatius Hospital Lingen, Stand 2009
23. Rahmenvertrag Typ Silver für einen volldigitalen Buckyarbeitsplatz der Firma Philips mit dem St. Bonifatius Hospital Lingen, Stand 2010
24. Letzter Support-Monat für Windows 7 ohne Service Pack, heise online http://www.heise.de/newsticker/meldung/Letzter-Support-Monat-fuer-Windows-7-ohne-Service-Pack-1825451.html, letzter Zugriff 22.03.2013
25. CIO, Zeitbombe Windows XP, http://www.cio.de/knowledgecenter/security/2906739/, letzter Zugriff 25.02.2013
26. Tanenbaum; Andrew S.: Moderne Betriebssysteme Pearson Studium, 3., aktualisierte Auflage, ISBN 978-3-8273-7342-7

Anschrift der Verfasser
Armin Gärtner
Ingenieurbüro für Medizintechnik
Ö. b. u. v. Sachverständiger der IHK Düsseldorf
Edith-Stein-Weg 8
40699 Erkrath
Armin.gaertner@t-online.de

Michael Voth
St. Bonifatius Hospital gGmbH
Hümmling Krankenhaus Sögel gGmbH
Marienkrankenhaus Papenburg - Aschendorf GmbH
Bereichsleiter Medizintechnik
Wilhelmstraße 13
49808 Lingen
michael.voth@bonifatius-lingen.de