Risikomanagement: IEC 80001-1 im medizinischen IT-Netz beschäftigt Hersteller und Betreiber

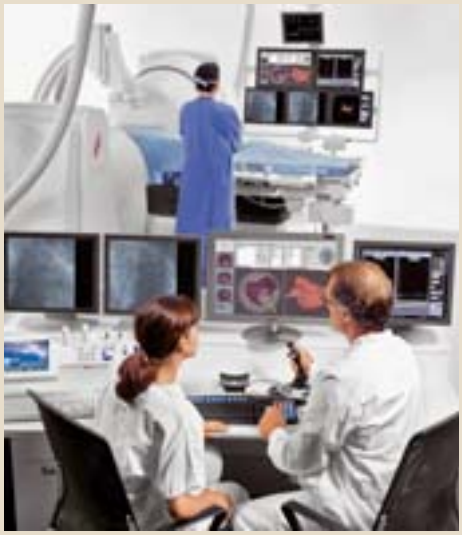
Kein Virus darf ins Netz

Im November 2011 ist die deutsche Übersetzung der IEC 80001-1 erschienen, die sich an die Betreiber von medizinischen IT-Netzwerken richtet. Je nach Betrachtung verbirgt sich in dieser Prozessnorm Kooperations- oder Konfliktpotenzial.

Ihr Stichwort

- Prozessnorm IEC 80001-1
- Medizinische IT-Netzwerke
- Risikomanagement
- Patientensicherheit an erster Stelle

Alle Geräte im medizinischen IT-Netzwerk müssen künftig der Norm IEC 80001-1 entsprechen. Auch die Hersteller sind in der Pflicht Bilder: Siemens



Sicherheit im OP: Ein strukturiertes Risikomanagement soll für problemlose Abläufe sorgen

Kaum ein medizinisches Gerät ist heutzutage ohne Netzwerk-Buchse zu bekommen, also ohne die Möglichkeit, es an ein IT-Netz anzuschließen. In den IT-Netzwerken von Krankenhäusern ist deshalb eine immer größere Zahl von medizintechnischen Geräten unterschiedlicher Hersteller integriert, die sich allerdings nicht gegenseitig stören oder negativ beeinflussen dürfen. Der nachhaltige Betrieb aller Geräte und Anwendungen ist sicherzustellen, und es müssen Maßnahmen für einen Ausfall vorbereitet sein. „Die Zeiten, in denen ein Arzt die IT ruft, um ein Gerät am Netzwerk anschließen oder eine Software aufzuspielen zu lassen, zu denen keine Informationen vorliegen, sind spätestens mit der IEC 80001-1 vorbei“, erklärt Jochen Kaiser, Sicherheitsbeauftragter am Universitätsklinikum Erlangen. „Denn mit Einführung eines strukturierten Risikomanagements müssen alle gravierenden Änderungen kontrolliert bewertet, implementiert und überprüft werden können.“ Dieses kontrollierte Vorgehen muss nicht nur bei der Inbetriebnahme von Geräten oder Anwendungen im Netz stattfinden, sondern bei jeder noch so kleinen Änderung, auch Software-Updates einzelner Komponenten oder des Betriebssystems. Im Extremfall bedeutet das, dass jeder Betriebssystem-Patch, der aufgespielt wird, von den einzelnen Medizinprodukte-Herstellern erst auf Wechselwirkungen überprüft und freigegeben werden muss. Insofern hat die Einführung der IEC 80001-1 auch weitreichende Konsequenzen auf die Perspektive der Hersteller: Waren sie bisher nur für diejenigen Vigilanz-Ereignisse zuständig, bei denen sich eine Störung unmittelbar auf die Patientensicherheit auswirkte, müssen sie nun noch systematischer darüber nachdenken, was hinter der Schnittstelle ihres Gerätes im Netzwerk vor Ort passieren könnte. Die Betreiber sind für ein Risikomanagement gemäß IEC 80001–1 gehalten, alle notwendigen Informationen für eine Beurteilung bei den Herstellern abzufragen, um anschließend entscheiden zu können, ob und in welcher Form ein Produkt das Gesamtsystem stören könnte – und die Hersteller müssen in der Lage sein, diese Informationen zu liefern. Markus Holzbrecher-Morys, Referent der Deutschen Krankenhausgesellschaft (DKG), dazu: „Die Zusammenarbeit bei dieser Informationsabfrage muss sich noch einspielen. Momentan bestehen hier Unsicherheiten sowohl auf Betreiber- als auch auf Herstellerseite. Doch diese Norm kann nicht einseitig umgesetzt werden, sie setzt die Kooperation der Beteiligten voraus.“

Im Vordergrund steht derzeit, sinnvoll zusammenzustellen, welche Informationen für das Risikomanagement tatsächlich relevant

Hilfe im Informationsdschungel

Die Umsetzungshinweise für Krankenhäuser ist als Arbeitshilfe der DKG erschienen: „Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten“. Sie ist erhältlich bei der Deutschen Krankenhaus Verlagsgesellschaft.
Auf der Website des ZVEI e.V., Fachverband Elektromedizinische Technik, gibt es eine FAQ-Liste zur Umsetzung der Norm. Zudem können Fragen an Marcus Wenzel (wenzel@zvei.org), gesendet werden, die bearbeitet und gegebenenfalls in einer aktualisierten FAQ-Liste veröffentlicht werden: www.zvei.org/medtech

sind. Der gedankliche Horizont geht dabei über die eigentliche Zweckbestimmung des Medizinproduktes hinaus; der Zweck der Vernetzung des Produktes rückt ins Rampenlicht.
Da ein medizinisches IT-Netzwerk ein sicherheitstechnisch sensibles Konstrukt ist, könnten einige Krankenhaus-ITler dazu verleitet sein, sich vom Hersteller jede erdenkliche Information geben zu lassen, um sich selbst abzusichern. Die Überschriften dazu lauten Sicherheit (safety), Daten- und Systemsicherheit (security) und Effektivität (effectiveness). Es geht also um eine ganze Bandbreite unterschiedlicher Aspekte, die abgedeckt werden wollen. Das beginnt bei der Sicherstellung der Netzverfügbarkeit, geht über die Sicherung patientenbezogener Daten und hört bei Alarmen, die sicher beim zuständigen Personal ankommen müssen, noch nicht auf. Doch Jochen Kaiser warnt seine Kollegen davor, einen – für beide Seiten – unnötigen Aufwand zu erzeugen: „Wir müssen mit gesundem Menschenverstand an das Thema herangehen und erkennen, wo Patienten gefährdet werden könnten. Darüber müssen wir gezielt mit dem Hersteller sprechen. Im Grunde wird mit dieser Prozessnorm der komplette Integrationsprozess von Medizintechnik zwischen Betreiber und Hersteller erst definiert.“ Dr. Georg Heidenreich, bei Siemens zuständig für Healthcare IT Standards, bestätigt das und ergänzt: „Viele Diskussionen um die IEC 80001-1 verlieren sich schnell in technischen Einzelheiten, obwohl doch klar der Prozess-Aspekt im Vordergrund steht. Betreiber müssen im Interesse der Verfügbarkeit wichtiger Daten sicher wissen, welche Daten wo entstehen, wie sie gesichert werden und wie sie zurückgespielt werden.“ Die Sicherung diagnostischer und therapeutischer Daten sei für ihn das wichtigste Thema. Checklisten, die Betreiber bei der Anschaffung oder bei Änderungen von Medizinprodukten als Vorlage verwenden können, sind in der druckfrischen Arbeitshilfe der DKG zur Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten, zu finden. Beispielsweise wird darin beschrieben, wie Aktualisierungen von Betriebssystemen vertraglich geregelt sein könnten, also wer im Einzelfall für die Aktualisierung des Betriebssystems auf dem vernetzbaren Medizinprodukt zuständig ist.
„Um den Krankenhäusern den Einstieg ins Risikomanagement zu erleichtern, haben wir in unseren Umsetzungshinweisen Anregungen, welche grundlegenden Informationen beim Hersteller sinnvoll abgefragt werden können“, so Markus Holzbrecher-Morys. „Eine abschließende Liste ist das allerdings nicht, sie muss vom Verantwortlichen an die lokalen Anforderungen angepasst und eventuell ergänzt werden.“ Dr. Georg Heidenreich rät indes seinen Hersteller-Kollegen, alle Fragen der Betreiber Ernst zu nehmen, denn „diese Fragen spiegeln den erlebten Bedarf des Betreibers wider. Über die produktspezifischen Dokumente hinaus, können die Hersteller durch eine systematische Beantwortung der Fragen ihre IT-Prozesskompetenz demonstrieren.“ Ob die Norm zwischen Betreibern und Herstellern eher zu Konflikten oder zu Kooperationen führt, wird am Ende von der Offenheit der jeweils beteiligten Akteure abhängen.

Ramona Riesterer
Fachjournalistin in Stuttgart