

SCHUTZ VOR SCHÄDLICHER SOFTWARE

Die Vernetzung im Gesundheitswesen schreitet voran – und damit die Anforderungen an die Daten- und Systemsicherheit für vernetzte Medizinprodukte. Ein ZVEI-Arbeitskreis hat dazu ein Papier erarbeitet.

Bei der immer stärker werdenden Vernetzung von Medizinprodukten mit dem Internet und auch der Geräte untereinander tauchen in letzter Zeit vermehrt Meldungen auf, die sich mit Viren, Würmern und Trojanern beschäftigen. Diese sogenannte schädliche Software hat im vernetzten Gesundheitswesen unter Umständen Einfluss auf Diagnose, Therapie und die Gesundheit von Patienten.

Vor diesem Hintergrund haben die Mitglieder des Arbeitskreises Medical

IT & Communications Systems – kurz MICS – ein Informationsschreiben verfasst, welches die Anwender und Betreiber von Medizinprodukten über die Gefahren und die Verantwortung informieren soll.

Viele Unternehmen im Gesundheitswesen haben ihre Anlagen und Geräte automatisiert und vernetzt. Die Vorteile liegen auf der Hand: Offenheit zwischen Administration und Leistungserbringung sowie verbesserte Transparenz der Datenströme ermöglicht effizientere Leistungserbringung. Diese Automatisierung und Vernetzung birgt allerdings auch Risiken, was sich bei der Betrachtung der verschiedenen Installationen in den unterschiedlichsten Umgebungen zeigt.

Typischerweise wird zwischen externen IT-Systemen, internen IT-Systemen sowie Systemen mit integrierten Medizinprodukten unterschieden. Allen ist gemeinsam, dass sie durch ihre Offenheit potentielle Einfallstore für

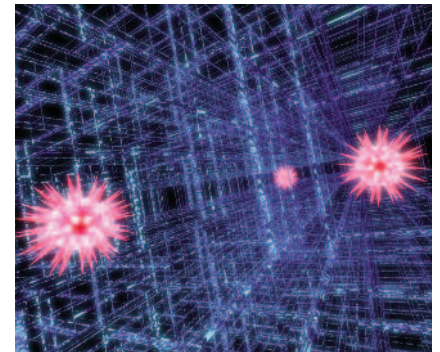
Schadsoftware sind und diese aufgrund automatischer Vernetzung auch schnell und leicht weiterverbreiten können.

Schadsoftware kann auf verschiedenen Wegen in ein medizinisches Netzwerk gelangen. Häufig wird sie sogar durch den Anwender selbst eingebracht, z.B. über CDs/DVDs, USB-Speichermedien, E-Mail-Anhänge oder Internet-Verbindungen ohne ausreichenden Virenschutz. Besteht keine sichere Trennung des medizinischen Netzwerks von der übrigen IT-Infrastruktur oder zu externen Systemen, kann Schadsoftware auch von dort in das medizinische Netzwerk gelangen.

Um diesen Gefahren zu begegnen, ergreifen Betreiber häufig eigene Schutzmaßnahmen, ohne sich bewusst zu sein, dass gerade solche Maßnahmen das ordnungsgemäße Funktionieren der IT-Systeme gefährden können. Unkontrollierte oder automatische, vom Medizinproduktehersteller nicht autorisierte Software-Updates können die ins Netzwerk eingebundenen Medizinprodukte in ihrer Funktion beeinträchtigen und somit möglicherweise Patienten gesundheitlich schädigen.

Hersteller von Medizinprodukten, die Software beinhalten oder reine Software-Produkte sind, müssen bereits während des Designs mögliche Risiken, die an den Schnittstellen denkbar sind, hinsichtlich ihres Gefährdungspotentials bewerten und entsprechende Minimierungsmaßnahmen definieren und implementieren. Sollte dies technisch nicht möglich sein, dann muss der Anwender bzw. der Patient hinreichend über diese Gefährdung informiert werden.

Betreiber dieser Medizinprodukte sind verpflichtet, bereits bei der Installation und Inbetriebnahme sich über



Computerviren können zur Bedrohung für medizinische Netzwerke werden.

eventuelle Gefährdungen hinsichtlich Fremdsoftware aller Art beim Hersteller zu informieren und geeignete Maßnahmen in ihrer eigenen Organisation umzusetzen. Dazu gehören sowohl technische Maßnahmen als auch organisatorische Maßnahmen, zum Beispiel die Festlegung und Implementierung von Richtlinien zur Nutzung der IT.

Hilfestellung für eine risikobewusste Integration der Medizinprodukte in das IT-Netzwerk gibt neben der Norm IEC 27002 auch die Norm IEC 80001-1. In der Norm IEC 80001-1 wird beschrieben, wie eine Risikoanalyse und die daraus abgeleiteten Maßnahmen das Risiko für Schadsoftwarebefall und -ausbreitung minimieren beziehungsweise wie Prozesse für den Ernstfall definiert werden.

Besondere Vorsicht ist geboten bei der Definition und Implementierung von Sicherheitskonzepten. Diese müssen zunächst individuell erarbeitet und implementiert werden und müssen dann regelmäßig gewartet, überprüft und, wo notwendig, verbessert werden, um ihren Anforderungen kontinuierlich zu genügen.

Weitere Informationen unter www.zvei.org/medtech

ZVEI-Fachverband
Elektromedizinische
Technik, Lyoner Straße 9
D-60528 Frankfurt am Main