Security in der Wertschöpfungskette medizinischer Anwendungen

Die Produktpiraterie ist das Geschwür der heutigen Wirtschaft. Es handelt sich um eine fortschreitende Krankheit, die unbemerkt wuchert und mit rasanter Geschwindigkeit wächst. Kopiert oder nachgebaut wird heute nahezu alles. Die Medizintechnik stellt hierbei keine Ausnahme dar. Es gibt aber professionelle und langzeiterprobte Lösungen.

Fachartikel von Günther Fischer

Produktpiraterie ist das Geschwür der heutigen Wirtschaft. Es handelt sich um eine fortschreitende Krankheit, die unbemerkt wuchert und mit rasanter Geschwindigkeit wächst. Kopiert oder nachgebaut wird heute nahezu alles. Medizintechnik stellt hierbei keine Ausnahme dar. Ganz im Gegenteil, allein deutsche Unternehmen reinvestieren jährlich 8 bis 10 Prozent des Umsatzes der Medizintechnikindustrie in Forschung und Entwicklung, um sich durch den damit erarbeiteten Wissensvorsprung und die besonders hohe Produktqualität am Weltmarkt zu behaupten. Das Einsparpotential dieser Investitionen treibt die Plagiate-Industrie unaufhaltsam an. Die Bedrohungsszenarien der Originalhersteller sind dabei sehr vielfältig.

Die Schutztechnologie CodeMeter schützt Software und Daten bei medizinischen Anwendungen.
(Bild: Custo Med)

Es fängt bei rückläufigen Absatzzahlen der eigenen Produkte an und geht über die Kooperation mit Zulieferern weiter. Denn auch das Verarbeiten gefälschter Komponenten von Lieferanten birgt das Risiko, später in die für den Hersteller teure Gewährleistung zu gehen. Danach helfen nur noch juristische Maßnahmen und das kann teuer und zeitaufwendig sein. Physische Güter lassen sich heute leider schwer schützen. Das Know-how heutiger Produkte, wie Röntgengeräte, Kernspintomographen oder Geräte in der Dentaltechnik, steckt zum Großteil in der mit den Geräten gelieferten Software und die lässt sich durchaus schützen.

ECK-DATEN

Beim Einsatz medizinischer Geräte gibt es immer mindestens zwei Interessengruppen mit unterschiedlichen Anforderungen an die Sicherheit. Der Hersteller des Systems möchte seine Software gegen Kopieren, Reverse Engineering und unautorisierte Modifikation schützen. Der Betreiber oder Nutzer hat hingegen ein besonderes Interesse an der Integrität der Software und den Daten, da dies Einfluss auf die funktionale Sicherheit des Systems hat. Er möchte sicherstellen, dass sich das medizinische Gerät genauso verhält, wie es getestet und zertifiziert wurde, und somit ausschließen, dass unautorisierte Änderungen oder Manipulationen an Programm oder Betriebsparametern vorgenommen wurden.

Technisch-präventiver Schutz von Software und Daten

Professionelle und langzeiterprobte Lösungen zum Kopier-, Know-how- und Integritätsschutz in Verbindung mit flexiblen Lizenzierungssystemen aus der klassischen IT-Landschaft können helfen, dieses Schutzziel auch in der Medizintechnik zu erreichen.

Im Zentrum steht dabei immer die Software – ob als PC-Software zur Diagnose oder als Embedded-Anwendung im medizinischen Gerät – als auch die von der Software generierten und zu verarbeitenden Daten. Solche Daten können beispielsweise Betriebsparameter oder Patientendaten sein.

Die Schutzziele sind recht vielfältig. Für Medizintechnikhersteller ist dabei entscheidend, dass ihre Geräte bis hin zur Code-Ebene vor Reverse Engineering, Manipulation der Betriebsparameter und Sabotage geschützt sind.

Software- und Know-how-Schutz durch Verschlüsselung

Priorität hat für die meisten Hersteller der Schutz des eigenen geistigen Eigentums. Bereits vor über 3500 Jahren wurden Verschlüsselungsverfahren zum Schutz von Betriebsgeheimnissen eingesetzt. Die Methoden haben sich zwar geändert, das grundlegende Prinzip ist aber das gleiche geblieben. Die Vorgehensweise sieht dabei wie folgt aus: Die ausführbare Anwendung wird vor der Auslieferung in geeigneter Form verschlüsselt. Hierbei kann die gesamte Anwendung verschlüsselt oder es können einzelne Funktionsblöcke unterschiedlich verschlüsselt sein. Alle Kunden erhalten anschließend dieselbe geschützte Software.

Verschlüsselung der gesamten Anwendung.
(Bild: Wibu-Systems)

Jeder einzelne Kunde erhält jedoch eine individuelle Lizenz mit den nötigen Schlüsseln, um die von ihm käuflich erworbenen Funktionen frei zu schalten. Die Art des Nutzungsrechts, ob Einzelplatzversion, Netzwerklizenz oder zeitlich limitierte Nutzung, modelliert das Produktmanagement. Durch den Einsatz professioneller Werkzeuge entfällt sogar die Notwendigkeit, die Anwendung entsprechend anzupassen. Die Code-Meter-Technologie von Wibu-Systems zeigt, wie Hersteller ihre Software schützen und verschlüsseln können.

Durch den Einsatz dieser Technologie reduziert sich die Anzahl der Anwendungen, die individuell gepflegt müssen, erheblich. Am Ende entsteht im Idealfall eine einzige Applikation, die das Unternehmen an alle Kunden identisch ausliefert. Die individuell geschützten Funktionsblöcke sind durch eine Lizenz und den dahinter liegenden Schlüsseln freigeschaltet. Das wiederum vereinfacht den Produktionsprozess durch Modelreduzierung, die Lagerhaltung sowie den Auslieferungs- und Bestellprozess. Bei geeigneter

Kombination des Softwareschutz- und Lizenzierungstoolsets ergeben sich somit neben dem Schutz des geistigen Eigentums Möglichkeiten, die Produktkosten zu verringern und sogar neue Geschäftsmodelle zu etablieren.

Sicherer Schlüsselspeicher

Die eingesetzten Verschlüsselungsverfahren sind typischerweise gemäß Kerckhoffs Prinzip öffentlich zugänglich und dokumentiert. Das einzige Geheimnis stellt der jeweilige Schlüssel dar. Das bedeutet, dass die Schlüssel in einem besonders gesicherten Speicher abgelegt sein sollten. Den höchstmöglichen Schutz bieten hier hardwarebasierende Schlüsselspeicher mit integrierter Verschlüsselungskomponente, sogenannte Smart Card Chips, die sogar Angriffen wie Seitenkanal-Attacken/Differential Power Analysis (DPA) standhalten.

Die im Smart Card Chip gespeicherten Schlüssel verlassen den sicheren Speicher nie und alle wichtigen kryptografischen Operationen finden innerhalb des sicheren Hardware-Elements statt. Alternativ können verschlüsselte Lizenzdateien, die an einzigartige Eigenschaften des Geräts (zum Beispiel dessen Seriennummer) gebunden sind, zur Speicherung der Schlüssel zum Einsatz kommen.

Diese bieten zwar einen geringeren Sicherheitsgrad als die sicheren Hardware-Elemente, ermöglichen aber eine einfache Auslieferung des Lizenzspeichers zum Beispiel über das Internet. Einer hardwarebasierenden Lösung ist aber bei hohem Sicherheitsbedarf immer der Vorzug zu geben.

Bedarfsgerechte Wartungs- und Pay-per-Use-Modelle

Zusätzlich zum Schutz können Hersteller die Nutzung ihrer Geräte sicher und flexibel messen und abrechnen, weitere Optionen verkaufen oder zeitlich begrenzt Funktionen freischalten, damit Anwender Geräteoptionen vor dem Kauf testen können. Zusätzlich kann der Qualitätsstandard von Verbrauchsmaterial durch einen Verbrauchszähler in der Lizenz sichergestellt sein. Bei Auslieferung setzt und dekrementiert der Hersteller den Zähler, bis er einen definierten Schwellwert erreicht. Der Betreiber oder Nutzer weist bei Erreichen des Schwellwerts entweder darauf hin, dass er das Verbrauchsmaterial nachbestellen sollte, oder die Bestellung löst sich automatisch aus. Erreicht der Zähler den Wert 0, ist das Gerät nicht mehr nutzbar. Bei Lieferung des Verbrauchsmaterials setzt sich der Zähler erneut und ist ab da wieder dekrementierend. Auf diese Weise ist ausgeschlossen, dass Endkunden minderwertiges Verbrauchsmaterial auf dem Graumarkt erwerben und einsetzen. Lizenzen für Funktionen in einem Gerät, für Verbrauchsmaterial oder den Zugriff auf Dokumente und Daten sind dabei im Warenwirtschaftssystem genauso verwaltet wie jedes andere Einzel- oder Ersatzteil eines Geräts.

Zeitlich begrenzte Rechtevergabe für autorisierte Wartungstechniker

Um sicherzustellen, dass nur autorisiertes und entsprechend fachlich geschultes Personal Zugang zu Wartungsdokumenten und –Funktionen erhält, sind zeitlich limitierte Autorisierungslizenzen ausgestellt. Dadurch schließt man unsachgemäße Wartungsarbeiten oder Betriebsparameteränderungen aus. Die Rechtevergabe erfolgt somit über Lizenzen in festgelegten zeitlichen Intervallen mit Option auf Verlängerung. Für diesen Zweck gibt es typischerweise Dongles wie die Cm-Dongles der Code-Meter-Technologie. Diese steckt der Techniker an das Gerät bei Wartungsarbeiten.

Schutz vertraulicher Patientendaten vor Missbrauch durch Verschlüsselung

Der Gesetzgeber gibt zwar vor, wie mit Patientendaten umzugehen ist; die Umsetzung dieser Vorgaben liegt aber beim Medizintechnikhersteller oder Nutzer. Professionelle Softwareschutz- und Lizenzierungstools erleichtern eine sichere Umsetzung der Vorgaben. Generierte Patientendaten aus einer medizinischen Anwendung, automatisch verschlüsselt über die Assoziierung der Softwarelizenz, sind nur mit gültiger Lizenz wieder zu entschlüsseln. Dies kann transparent geschehen oder explizit unter Nutzung der Mechanismen, die das Schutz- und Lizenzierungssystem zur Verfügung stellt. Die Daten sind somit nur in Verbindung mit der zugehörigen Anwendung und entsprechend gültiger Lizenz nutzbar und weitestgehend vor unbefugter Einsicht oder Nutzung geschützt.

Zentrale Lizenzverwaltung

Unterschiedliche Verschlüsselung einzelner Funktionsblöcke.
(Bild: Wibu-Systems)

Kombination aus Verschlüsselung der gesamten Anwendung und unterschiedlicher Verschlüsselung einzelner Funktionsblöcke.
(Bild: Wibu-Systems)

Sichere Schlüssel-Speicherlösungen der Code-Meter-Technologie.
(Bild: Wibu-Systems)

CPU-Modul mit integriertem Schlüsselspeicher.
(Bild: Kontron)

Lizenzverwaltungssysteme erleichtern das Erstellen, Verwalten und Ausliefern von Lizenzen und unterstützen das Produktmanagement bei der Modellierung von Lizenzen. Um Datenredundanzen zu vermeiden, beschränkt sich die Datenhaltung auf lizenzspezifische Informationen. Das Erstellen der Aufträge erledigt wie gewohnt das führende ERP-oder CRM-System, welches das Erzeugen der zugehörigen Lizenzen über eine Automatisierungsschnittstelle auf dem Lizenzverwaltungssystem anstößt. Das Lizenzverwaltungssystem übernimmt dabei ausschließlich die Aufgabe der Verwaltung und Auslieferung der Lizenzen und ordnet sich ansonsten dem führenden ERP-oder CRM-System unter.
(hag)

Zentrale Lizenzverwaltung mit der Code Meter License Central.
(Bild: Wibu-Systems)

Weblinks

- Empfohlener Artikel

ÜBER DEN AUTOR

Günther Fischer

Senior Consultant Licensing and Protection bei Wibu-Systems

WEITERE INFOS

Wibu Systems

Rüppurrer-Straße 54

76137 Karlsruhe

Deutschland

Zum Firmenprofil >