Angriff aus dem Dunkeln: Auch in der Medizin sind Hacker-Attacken allgegenwärtig.

Bild: Pixabay

Cybersecurity für die Medizintechnik

Medizingeräte werden von – nur in Ausnahmefällen sicher erstellter – Software, Firmware oder mobilen Apps gesteuert. Diese Unsicherheit ist seit Jahren bekannt; auch, dass die Geräte gehackt werden (können). Die daraus resultierenden Schäden sind schockierend! In Zeiten von Medizin 4.0 sieht der Gesetzgeber das auch so: Mit der DSGVO und der geltenden MDR steigen die Anforderungen an die IT-Sicherheit weiter.

Sascha Böhm
Security Consultant, softScheck GmbH

Hartmut Pohl
Geschäftsführender Gesellschafter, softScheck GmbH

Überall treffen wir sie an: Roboter, die uns in alltäglichen Lebenslagen unterstützen. Auch als zum Teil ferngesteuerte Chirurgie-Roboter kennen wir sie aus Krankenhäusern – weltweit werden über 1000 jährlich neu installiert. Leider sind sie vielleicht »safe« – aber nicht immer sicher im Sinne von »secure«. Denn Roboterfunktionen können durch Angreifer fehlgesteuert werden. So lassen sich die Befehle der Chirurgen verändern, überschreiben, ignorieren oder verzögern. Auch können »Denial of Service«-Angriffe (Verweigerung des Dienstes) dazu genutzt werden, Roboter lahmzulegen und unbedienbar zu machen. Eine weitere Option wäre es, den Videostream abzugreifen, um bei einer Operation zuzusehen. Bei einem chirurgischen Eingriff können schon kleinere Störungen zu beträchtlichen körperlichen Risiken für die Patienten führen.

Darüber hinaus stellt das Abgreifen von Daten eine Verletzung der Privatsphäre (Datenschutz) dar, was jetzt mit der neuen DSGVO zu schwerwiegenden Folgen (auch finanziell) führen kann. Deswegen fordert auch die DSGVO IT-Sicherheit nach dem Stand der Technik. Bereits im Oktober 2016 hat das Unternehmen Johnson & Johnson vor einer Sicherheitslücke in seinen Insulinpumpen gewarnt. Bei Pumpen der Marke Animas (»OneTouch Ping«) hätte demnach der Chip von Dritten gehackt werden können. Zwar versicherte der US-Pharmahersteller damals, dass das Risiko extrem klein sei; ein Hacker hätte sich nicht weiter als 800 Meter entfernt von der Pumpe aufhalten dürfen und über ein gewisses technisches Wissen verfügen müssen. Das Problem lag in der unverschlüsselten Funkverbindung zwischen der Insulinpumpe und deren Fernbedienung.

AUF EINEN BLICK

Die 6 Methoden zur Identifizierung von Sicherheitslücken:

- SQUARE: Security QUALity Requirements Engineering – Risk Analysis
- Threat Modeling: Untersuchung des Security Designs auf Sicherheitslücken
- Static Source Code Analysis zur Quellcodeprüfung auf Sicherheitslücken – Code Reading
- Penetration Testing: Identifizierung bekannter Sicherheitslücken
- Dynamic Analysis – Fuzzing: Identifizierung von Sicherheitslücken durch Eingabe erfahrungsgemäß erfolgreicher Angriffsdaten
- Conformance Testing: Prüfung auf Übereinstimmung von Design und Implementierung sowie von Implementierung und ausführbarem Code zur Identifizierung von Hintertüren/Backdoors

SOFTSCHECK SECURITY TESTING PROCESS

softScheck arbeitet im Kontext aktiver Medizinprodukte mit dem Johner Institut für IT im Gesundheitswesen zusammen. Das Johner Institut unterstützt Medizinproduktehersteller dabei, die regulatorischen Anforderungen zum Beispiel der MDR, der IVDR oder der FDA zu erfüllen und so sicherere Produkte schnell und gesetzeskonform in den Markt zu bringen.

Mit dem »softScheck Security Testing Process« (sSTP) erreichen Entwickler vier Ziele:

- Hohes IT-Sicherheitsniveau der Entwicklungen in Hardware und Software: Angreifbare Sicherheitslücken werden von softScheck identifiziert.
- Produkt-Lebensdauer – Zukunftssicherheit: Software, Firmware, Apps, Systems und Hardware entsprechen den nationalen und den europäischen Gesetzen und Verordnungen sowie den US Regelungen der FDA.
- Kostengünstige Software-Entwicklung: Sicherheitsrelevante Fehler werden bereits während der Entwicklung identifiziert und müssen nicht erst nach Auslieferung an den Kunden kostenaufwendig korrigiert und gepatcht oder sogar die Produkte im Feld ausgetauscht werden.
- Verkürzung der Time-to-Market durch parallel zur Entwicklung durchgeführte Security-Tests und Erhöhung des Sicherheitsniveaus während der gesamten Lebenszeit.

Das System war zwar nicht ans Internet angebunden, konnte aber mit der entsprechenden technischen Expertise aus der Nähe gekapert werden. Generell gelten drahtlose Verbindungen ins Internet als riskant; natürlich sollte die Verbindung verschlüsselt sein, aber das reicht noch lange nicht aus, weil sich in der Implementierung der Verschlüsselung Software-Sicherheitslücken befinden können.

Auch immer wieder im Focus stehen Herzschrittmacher, weil eine Fehlfunktion unmittelbar lebensbedrohend wirkt: Ist der Herzschlag zu langsam oder setzt aus, bekommt der Mensch zu wenig Sauerstoff. So wurde 2017 eine weltweite Rückrufaktion für Herzschrittmacher des US-Pharmakonzerns Abbott notwendig. Anlass war die Identifizierung einer Sicherheitslücke: Angreifer können durch diese Sicherheitslücke unerlaubten Zugriff erlangen und das Gerät lahmlegen oder die Batterie leeren. Ein beängstigender Gedanke für Patienten, dass Hacker in ihren Körper eingreifen können. Nach Angaben des Konzerns waren weltweit etwa 750.000 Patienten betroffen.

Hersteller und Betreiber ziehen an einem Strang

Die Digitalisierung im Medizinbereich ist natürlich unverzichtbar, aber sie sollte auch korrekt und unter Berücksichtigung aller tatsächlichen Risiken durchgeführt werden. Hier müssen Hersteller und Betreiber (Praxen, Labore, Krankenhäuser) gemeinsam an einem Strang ziehen, um IT-Sicherheit zu gewährleisten. Ein erster Schritt sind die 2017 vom EU-Parlament beschlossenen – für alle EU-Staaten unmittelbar wirksamen – Verordnungen für Medizinprodukte: Medical Device Regulation (MDR) und die In-Vitro-Diagnostika Device Regulation (IVDR). Diese beiden Verordnungen lösen die bisherigen Medizinprodukte-Richtlinien MDD, AIMD und IVD ab.

In beiden neuen Verordnungen wird das Thema Cybersecurity deutlich stärker adressiert, sodass Medizin-Produkte nicht mehr ohne Sicherheitsmaßnahmen in den Verkauf kommen: Ein IT-Angriff (Virus, Wurm, direkter Angriff) auf lebenserhaltende Geräte und Systeme kann direkt Geräte stören oder abschalten. Fällt ein medizinisches Gerät aus, können Patienten vielleicht noch aufgenommen, aber nicht behandelt werden. Mit Ransomware werden Daten der Geräte (Steuerdaten, Patientendaten) so manipuliert (zum Beispiel unlesbar verschlüsselt), dass die Geräte nicht mehr korrekt arbeiten und auch Patienten falsch behandelt werden.

Darüber hinaus können personenbezogene Daten kopiert, manipuliert oder gelöscht werden. Mit stark zunehmender Häufigkeit auch, um Einrichtungen zu erpressen. Dazu gehören Labordaten, die zwar pseudonymisiert sind, aber den betroffenen Patienten durchaus zugeordnet werden können. Einschlägig ist hier auch die EU-Datenschutz-Grundverordnung (EU-DSGVO) mit ihrer Meldepflicht von Angriffen und Vorfällen. Abgesehen von strafrechtlicher Verfolgung können Bußgelder in Höhe von bis zu 20 Millionen Euro beziehungsweise bis zu 4 % des gesamten weltweit erzielten Konzern-Jahresumsatzes festgesetzt werden.

Stand der Technik umsetzen

Für die Software- und Geräteentwicklung fordert die MDR ausdrücklich IT-Sicherheit auf dem »Stand der Technik«. Dies erfordert Maßnahmen, die allgemein bekannt sind wie die Anwendung und Einhaltung des Grundschutzes des Bundesamts für Informationssicherheit (BSI) mit technischen Richtlinien, internationalen Normen wie die ISO 15408, IEC 62443, ISO 27034 oder auch die UL 2900-2-1.

So fordert die ISO 25010 (früher ISO 9126) Qualitätseigenschaften für Software-Security wie Vertraulichkeit, Integrität und Authentizität. Um dies zu erreichen, sind Security-Tests unverzichtbar, um potenzielle Angriffspunkte (Sicherheitslücken) zu identifizieren. Angriffe sind nur dann erfolglos, wenn der (oder die) Angriffspunkt(e) – also die Sicherheitslücken – behoben, korrigiert und gepatcht sind. Dazu existiert die ISO 27034 Application Security. Diese Norm entspricht dem Stand der Technik und erhöht die Sicherheitsqualität der Software. Sie beinhaltet einige Methoden zur Vermeidung bzw. Identifizierung von Angriffspunkten: Sicherheitslücken.

Dabei werden sechs Methoden zur Identifizierung der Sicherheitslücken ein-

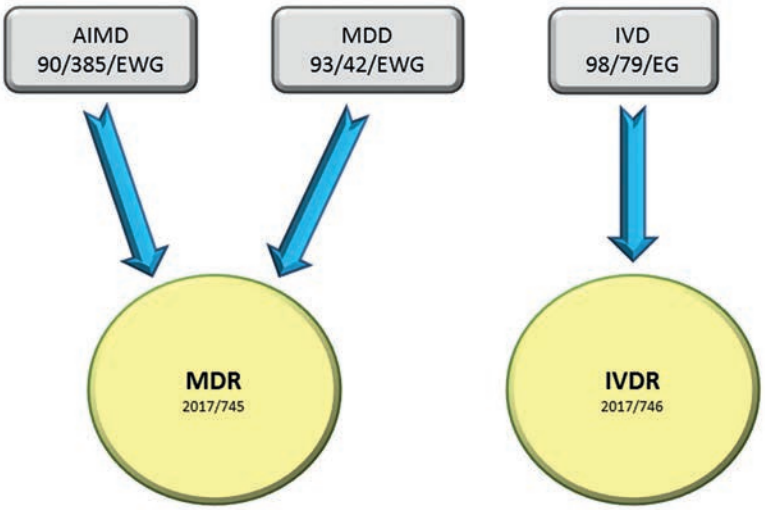
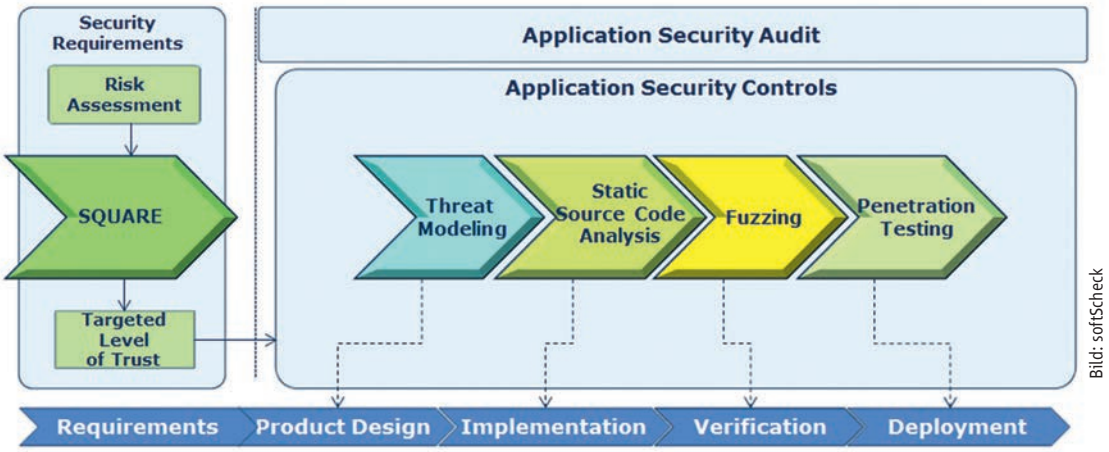


Bild: Nach Johner-Institut

Übergang MDD, AIMD und IVD in die neuen Verordnungen MDR und IVDR.



Security Testing Process von softScheck.

gesetzt (siehe auch *Kasten* S. 43), jede in einer bestimmten Entwicklungsphase (Security Requirements, Security Design, Implementierung bis zum ausführbaren Code). So lassen sich bereits während der Entwicklung kritische Sicherheitslücken beheben. Die Wirksamkeit der hier eingesetzten Tools können durch den Einsatz in der Cloud verstärkt werden.

SQUARE ist hierbei der erste Schritt. Mit dieser Methode werden zu Projektbeginn die IT-Security spezifischen Anforderungen definiert.

Threat Modeling unterstützt die methodische Entwicklung eines sicheren Systementwurfs und einer Architektur in der Designphase der Softwareentwicklung – die Fehlerbehebungskosten sind in dieser Entwicklungsphase noch gering. Es hilft beim Aufbau einer vollständigen Sicherheitsarchitektur mit einem angemessenen Sicherheitsniveau und trägt damit dazu bei, die Angriffsfläche des untersuchten Systems zu minimieren.

Static Source Code Analysis analysiert semi-automatisch den Quellcode auf Sicherheitslücken, ohne ihn auszuführen (im Gegensatz zur Dynamic Analysis, wozu u. a. Fuzzing zählt). Um False-Positives auszuschließen, werden die Ergebnisse manuell überprüft und Behebungsvorschläge erarbeitet. Die Qualität und Quantität des Analyse-Resultats hängt somit maßgeblich von der Auswahl geeigneter Tools (und geschultem, spezialisiertem Fachpersonal) ab. Static Source Code Analysis wird Tool-gestützt automatisiert bzw. semi-automatisiert durchgeführt; die Befunde der Tools werden gesammelt und »manuell« ausgewertet.

Im Rahmen eines **Penetration Tests** werden kontrollierte Angriffe durchgeführt, ähnlich wie ein Angreifer vorgehen würde. Es werden systematisch und methodisch gezielt Sicherheitslücken identifiziert. Ziel ist, relevante Sicherheitslücken, z. B. durch Konfigurationsfehler oder fehlende Security-Patches, im Produkt zu identifizieren.

Dynamic Analysis/Fuzzing stellt eine halb-automatisierte Methode zur Identifizierung von (mit Angriffen ausnutzbaren) Sicherheitslücken in Software und Hardware/Firmware dar: Tool-gestützte Eingabe von Testdaten in ein Target-System (Programm, Firmware) werden verwendet, um unvorhergesehene Eingabedaten zu erkennen. Falsche oder unzureichende Verarbeitung dieser Daten führt zu einem unerwarteten Verhalten (Crash, hoher Verbrauch an Ressourcen wie Rechenzeit, Speicher) des Zielprogramms. Dieses Verhalten wird mit Hilfe eines Monitoring-Tools protokolliert, voranalysiert und dargestellt. Durch die Analyse der Monitorergebnisse können falsche Hinweise (False-Positives) ausgesondert werden. Sicherheitslücken werden durch Reproduzierung der Anomalien und Erstellen von Exploits nachgewiesen.

Mit Hilfe von **Conformance Testing** wird überprüft, ob auch wirklich nur das implementiert wurde, was designt wurde und nicht etwa zusätzlicher (Schad-)Code wie Backdoors etc. hinzugefügt wurde.

Ausblick: Verschärfung der Risikobewertung

Zukünftig sollen auch bereits im Markt befindliche Medizinprodukte auf IT-Sicherheitslücken überprüft werden. Die zuständige Food and Drug Administration (FDA) der USA fordert das bereits. Dabei werden naturgemäß auch bereits erfolgte Zulassungen nachträglich in Frage gestellt.

Darüber hinaus müssen gleichermaßen funktionale Updates bereits im Markt befindlicher Produkte auf Angriffspunkte untersucht und auf Security getestet werden. Um dies zu gewährleisten hat die FDA mehrere Guidelines und Dokumente herausgebracht. Unter anderem zur Risikobewertung. Zusätzlich hat die FDA den proprietären Standard UL 2900 anerkannt. Sie behandelt ebenfalls das Thema Software-Cybersicherheit im Medizinbereich. Es ist zu erwarten, dass sich diese amerikanischen Anforderungen über kurz oder lang auch in der EU durchsetzen werden. ■

Anzeige