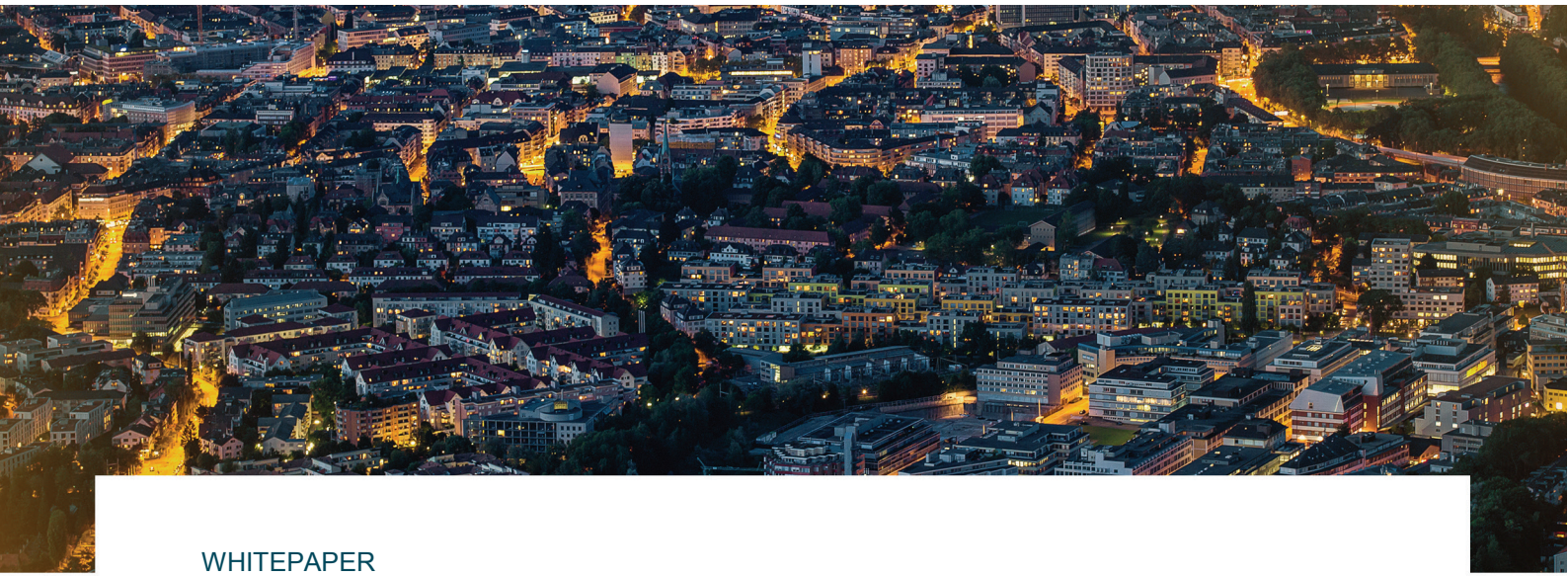
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WHITEPAPER

Software im Kontext der Medical Device Regulation (MDR)

Adrian Helfenstein | Leiter Entwicklung | Steinhausen, 14. Januar 2020

Wer in der Schweiz oder einem EU-Vertragsstaat ein Medizinprodukt in Verkehr bringt oder es ohne Inverkehrbringen betreiben will, muss dessen Konformität zur Medical Device Regulation (MDR) nachweisen. In einem Bewertungsverfahren muss die Konformität des Produktes beurteilt und festgestellt werden. Was bedeutet dies für Software? Wie wird Software im Kontext der MDR eingestuft und bewertet? Was wird insbesondere für Software-Updates verlangt? Wir geben Ihnen einen Überblick und sagen, worauf es ankommt.

Wann gilt eine Software als Medizinprodukt?

Als Medizinprodukte werden Instrumente, Geräte, Implantate, Software oder andere Objekte bezeichnet, die allein oder in Kombination mit anderen einen oder mehrere medizinische Zwecke erfüllen und gemäss Hersteller für Menschen bestimmt sind. Für eine weitere Präzisierung des Begriffs Medizinprodukt sei an dieser Stelle auf die MDR verwiesen.

Eine Software mit medizinischem Verwendungszweck und dem Anwendungsbereich Mensch wird demzufolge als Medizinprodukt eingestuft, sei es allein oder in Kombination mit einem anderen Medizinprodukt.

Software wird nach den Risiken des Verwendungszwecks klassifiziert

Unter Berücksichtigung des medizinischen Verwendungszwecks und der damit verbundenen Risiken werden Medizinprodukte in die Klassen I, IIa, IIb und III eingeteilt. Nach den Klassifizierungsregeln gemäss MDR wird Software, die ein Medizinprodukt steuert oder dessen Anwendung beeinflusst, derselben Klasse zugeordnet wie das Produkt selbst. Ist sie hingegen von anderen Medizinprodukten unabhängig, wird sie für sich allein klassifiziert. Das hierzu notwendige Vorgehen sowie die zu treffenden Entscheidungen sind in folgendem Diagramm dargestellt:

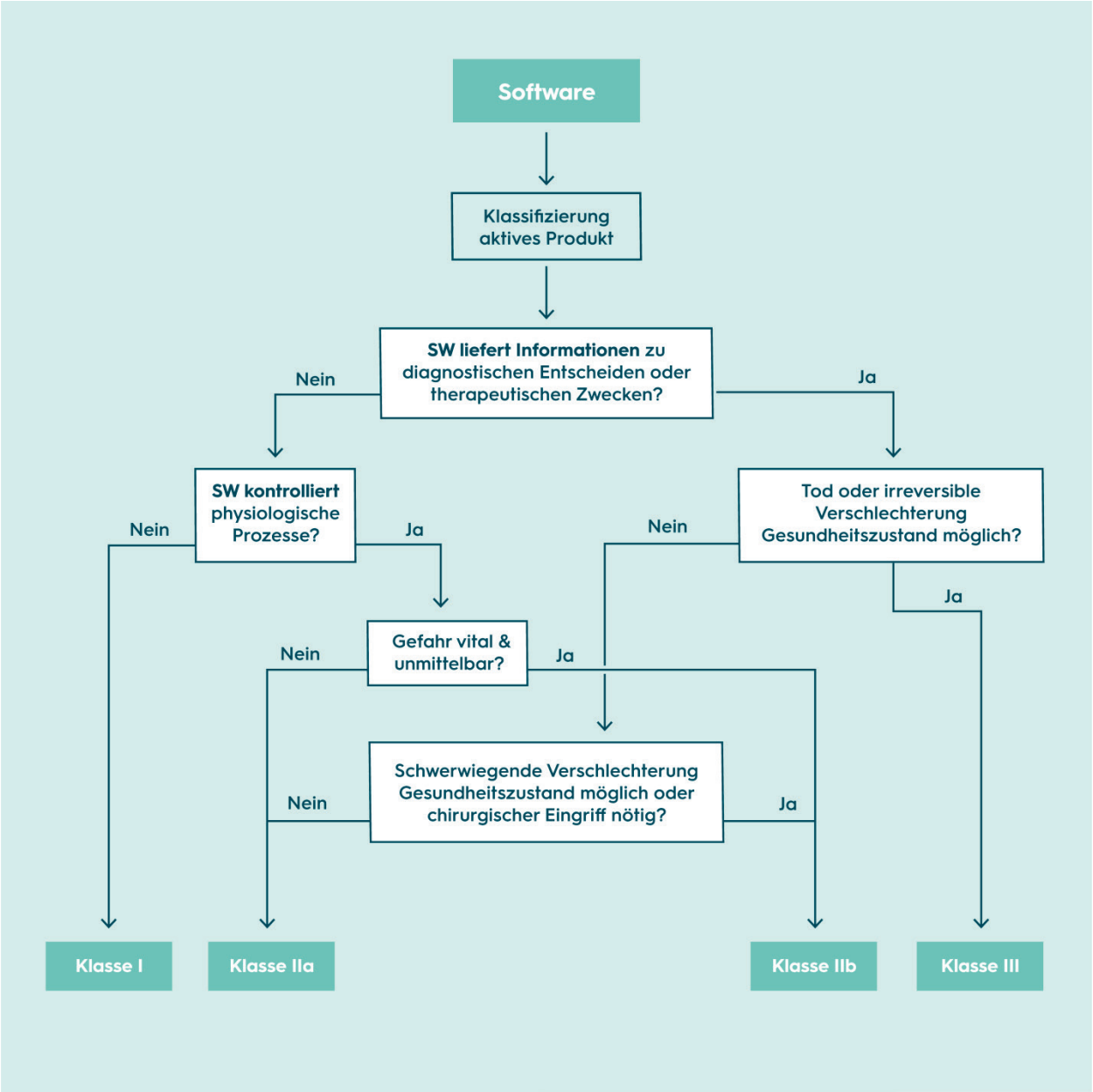


Abbildung 1: Eigenständige Klassifizierung von Software nach MDR

Software gilt als aktives Produkt. Dies bedeutet, dass für den Betrieb von Software von einer externen Energiequelle – beispielsweise Strom aus Akku, Batterie oder durch Umwandlung von thermischer/kinetischer Energie – ausgegangen wird.

Eingeschränkt verwendbar © CyOne Security AG. Alle Rechte vorbehalten

Konformitätsbewertung von Software – das Verfahren ist abhängig von deren Klassifizierung

Je nach Klassifizierung eines Medizinproduktes müssen die Hersteller eine Konformitätsbewertung durchführen. Die Verfahren hierzu sind ebenfalls in der MDR festgelegt und gelten explizit auch für als Medizinprodukt eingestufte Software.

Aktuell sind drei unterschiedliche Konformitätsbewertungsverfahren definiert. Deren Anforderungen und Vorgehensweisen sind in den Anhängen IX, X und XI der MDR geregelt und unterscheiden sich aufgrund nachfolgender Bewertungsgrundlagen:

- Qualitätsmanagementsystem und technische Dokumentation
- Baumusterprüfung
- Produktkonformitätsprüfung (Produktionsqualitätssicherung, Produktprüfung)

Alle drei Beurteilungsverfahren verlangen vom Hersteller einen der jeweiligen Grundlage entsprechenden Antrag auf Bewertung der MDR-Konformität. Dieser muss bei der dafür vorgesehenen benannten Stelle, in der Schweiz bei einer Konformitätsbewertungsstelle, eingereicht werden. Diese wiederum prüft den Antrag und teilt dem Hersteller ihre begründete Entscheidung zur Ausstellung der entsprechenden Bescheinigung mit.

Die folgende Zusammenstellung gibt einen groben Überblick über die je nach Klassifizierung anzuwendenden Konformitätsbewertungsverfahren:

Klasse III	Die Bewertung basiert auf der Grundlage eines Qualitätsmanagementsystems (QMS) und der technischen Dokumentation des Produkts. Alternativ kann eine Bewertung basierend auf Baumusterprüfung und Produktkonformitätsprüfung vorgenommen werden.
Klasse IIb	Die Bewertung basiert auf der Grundlage eines QMS und der technischen Dokumentation des Produkts – zumindest eines repräsentativen Produkts **pro generische Produktgruppe**. Sofern eine Software in einem implantierbaren Produkt zum Einsatz kommt, muss die Bewertung der technischen Dokumentation für jedes Produkt vorgenommen werden. Alternativ kann eine Bewertung basierend auf Baumusterprüfung und Produktkonformitätsprüfung vorgenommen werden.
Klasse IIa	Die Bewertung basiert auf der Grundlage eines QMS und der technischen Dokumentation des Produkts – zumindest eines repräsentativen Produkts **jeder Produktkategorie**. Alternativ können sich die Hersteller entschliessen, eine technische Dokumentation gemäss MDR-Anhängen II und III zu erstellen, in Kombination mit einer Konformitätsbewertung basierend auf der Produktkonformitätsprüfung (Anhang XI, Abschnitt 10 oder 18). Hierbei muss die Bewertung der technischen Dokumentation für zumindest ein repräsentatives Produkt jeder Produktkategorie durchgeführt werden.

Eingeschränkt verwendbar © CyOne Security AG. Alle Rechte vorbehalten

Klasse I	Für Produkte der Klasse I kann der Hersteller selbst die Konformität mittels Ausstellung einer EU-Konformitätserklärung bestätigen. Die Rahmenbedingungen hierzu sind in Art. 19 und die Anforderungen an die zu erstellende technische Dokumentation in den Anhängen II und III der MDR geregelt. Bei Produkten mit Messfunktion, welche in sterilem Zustand in den Verkehr gebracht werden oder bei welchen es sich um wiederverwendbare chirurgische Instrumente handelt, wendet der Hersteller das Verfahren zur Bewertung des Qualitätsmanagementsystems oder der Produktkonformitätsprüfung (Teil A: Produktionsqualitätssicherung) an. Die Beteiligung der Konformitätsbewertungsstelle an diesen Verfahren ist jedoch begrenzt. So ist beispielsweise bei Produkten mit Messfunktion die Beteiligung auf Aspekte beschränkt, welche mit messtechnischen Anforderungen zusammenhängen.

Sonderanfertigungen und Prüfprodukte sind jedoch von den oben beschriebenen Regelungen ausgenommen. Es gelten andere, spezielle Vorschriften, die ebenfalls in der MDR geregelt sind.

Konsultationsverfahren für bestimmte Produkte der Klasse III und IIb

Für implantierbare Produkte der Klasse III und aktive Produkte der Klasse IIb, die dazu bestimmt sind, Arzneimittel an den Körper abzugeben und/oder aus diesem zu entfernen, wendet die Konformitätsbewertungsstelle das sogenannte Konsultationsverfahren an. Hierzu erstellt sie zuhanden eines Expertengremiums einen Bericht über die Begutachtung der klinischen Bewertung, über die medizinische Zweckbestimmung und zum Plan für die klinische Nachbeobachtung nach dem Inverkehrbringen. Ein angerufenes Expertengremium entscheidet und begründet, anhand festgelegter Kriterien, spätestens nach 21 Tagen, ob es innerhalb von 60 Tagen ein wissenschaftliches Gutachten erstellen wird oder nicht. Falls es kein wissenschaftliches Gutachten vorlegen wird oder die 60-tägige Frist abläuft, kann die Konformitätsbewertungsstelle das Zertifizierungsverfahren fortsetzen. Wird in einem Expertengutachten ein Mangel beim klinischen Nachweis, der medizinischen Zweckbestimmung und/oder dem Plan für die klinische Nachbeobachtung festgestellt, rät die Konformitätsbewertungsstelle dem Hersteller zu entsprechenden Anpassungen und/oder Einschränkungen, oder sieht – gegebenenfalls im Konformitätsbewertungsbericht – Einschränkungen vor.
Folgt die Konformitätsbewertungsstelle in ihrem Bericht dem Expertengutachten nicht, legt sie eine umfassende schriftliche Begründung vor. Diese Begründung sowie das Expertengutachten werden von der EU-Kommission über die Eudamed-Datenbank veröffentlicht.

Konformitätsbewertung anhand eines repräsentativen Produktes

Wie obenstehender Übersicht zu entnehmen ist, sind Konformitätsbewertungen ganzer Produktkategorien und generischer Produktgruppen anhand eines repräsentativen Produktes und unter gewissen Voraussetzungen (Klassenzugehörigkeit und Bewertungsgrundlagen) vorgesehen. Hierdurch bietet sich eine Möglichkeit, Aufwand und Durchlaufzeit für die Beurteilung mehrerer Produkte zu reduzieren. Es stellt sich daher die Frage, wie die Begriffe generische Produktgruppe und Produktkategorie definiert sind.
Unter generischer Produktgruppe wird eine Gruppe von Produkten mit gleicher oder ähnlicher Zweckbestimmung oder technologischen Gemeinsamkeiten verstanden, die ohne Berücksichtigung spezifischer Merkmale klassifiziert werden können. Der Begriff Produktkategorie ist in der MDR, nach bestem Wissen, nicht näher präzisiert. Da dieser auf die tiefere Risikoklasse IIa angewendet

Eingeschränkt verwendbar © CyOne Security AG. Alle Rechte vorbehalten

wird, ist nicht von einer engeren Definition als derjenigen für die generische Produktgruppe (IIb) auszugehen.

Software-Updates – Nachtrag oder neue Zertifizierung?

Software-Updates stellen eine Änderung am zugelassenen Produkt dar. Daher unterliegen solche Änderungen ebenfalls der Genehmigungspflicht. Hierbei gelten die nachfolgenden Regelungen:

- Beinhaltet ein Software-Update eine Änderung an einem Baumuster, muss die Konformitätsbewertungsstelle, welche die EU-Baumusterprüfbescheinigung ausgestellt hat, in jedem Fall vorab angefragt werden.
- Geht es jedoch um ein Produkt, für welches eine Bewertung der technischen Dokumentation ausgestellt wurde, muss die Konformitätsbewertungsstelle, welche die EU-Bewertung der technischen Dokumentation ausgestellt hat, lediglich informiert werden, sofern die geplanten Änderungen dessen Sicherheit, Leistungsfähigkeit oder Anwendungsbedingungen beeinträchtigen könnten.

In beiden Fällen bewertet die Konformitätsbewertungsstelle, ob die geplanten Änderungen in einem Nachtrag zur entsprechenden EU-Bescheinigung genehmigt werden, oder ob diese eine neue Konformitätsbewertung nach sich ziehen.

Fazit

Steuert eine Software ein Medizinprodukt oder beeinflusst sie dessen Anwendung, wird sie derjenigen Risikoklasse zugeordnet, der das Medizinprodukt angehört.

Andernfalls wird Software für sich allein klassifiziert. Hierzu sind in der MDR entsprechende Einstufungsregeln festgelegt.

Die im Rahmen der Zulassung (Zertifizierung und Re-Zertifizierung) durchzuführenden Konformitätsbewertungsverfahren sind über die Risikoklassifizierung des Medizinproduktes geregelt. Hierbei gilt: je höher die Risikoklasse, desto höher die zu erwartenden Verfahrensaufwände. Dies geht von der Selbstdeklaration durch den Hersteller, bei Produkten der Klasse I, bis hin zur zwingenden Bewertung des Qualitätsmanagementsystems und der technischen Dokumentation für Produkte der Klasse III durch eine Konformitätsbewertungsstelle. Für Produkte der Klasse IIa und IIb, welche auf solche Art und Weise beurteilt werden, muss die Konformitätsbewertung der technischen Dokumentation nur für ein repräsentatives Produkt je Produktgruppe (Klasse IIb) resp. je Produktkategorie (Klasse IIa) vorgenommen werden. Hierdurch kann der Verfahrensaufwand, über mehrere Produkte einer Kategorie oder Gruppe betrachtet, reduziert bzw. amortisiert werden.

Bei Änderungen an einem zugelassenen Medizinprodukt, wie dies beispielsweise ein Software-Update darstellt, beurteilt die zuständige Konformitätsbewertungsstelle, ob diese Änderung mit einem Nachtrag zur bestehenden Bescheinigung genehmigt werden kann, oder ob eine neue Konformitätsbewertung notwendig ist. Hierbei gilt:

- Liegt der Zulassung eine Baumusterprüfbescheinigung zugrunde, ist die Konformitätsbewertungsstelle vor geplanten Änderungen immer beizuziehen.
- Basiert die Zulassung hingegen auf der Bewertungsgrundlage der technischen Dokumentation, ist die Konformitätsbewertungsstelle zwingend anzufragen, sofern die angestrebten Änderungen die Sicherheit und Leistungsfähigkeit oder die Anwendungsbedingungen des zugelassenen Produkts beeinträchtigen könnten.

Da bei einem Nachtrag von kürzeren Verfahrensdurchlaufzeiten und somit von geringeren Aufwänden ausgegangen werden kann als bei einer neuen Konformitätsbewertung, stellt sich die Frage, wie

Eingeschränkt verwendbar © CyOne Security AG. Alle Rechte vorbehalten

Medizinprodukte gebaut sein müssen, damit zumindest gewisse Arten von Software-Updates als Nachträge bewilligt werden.

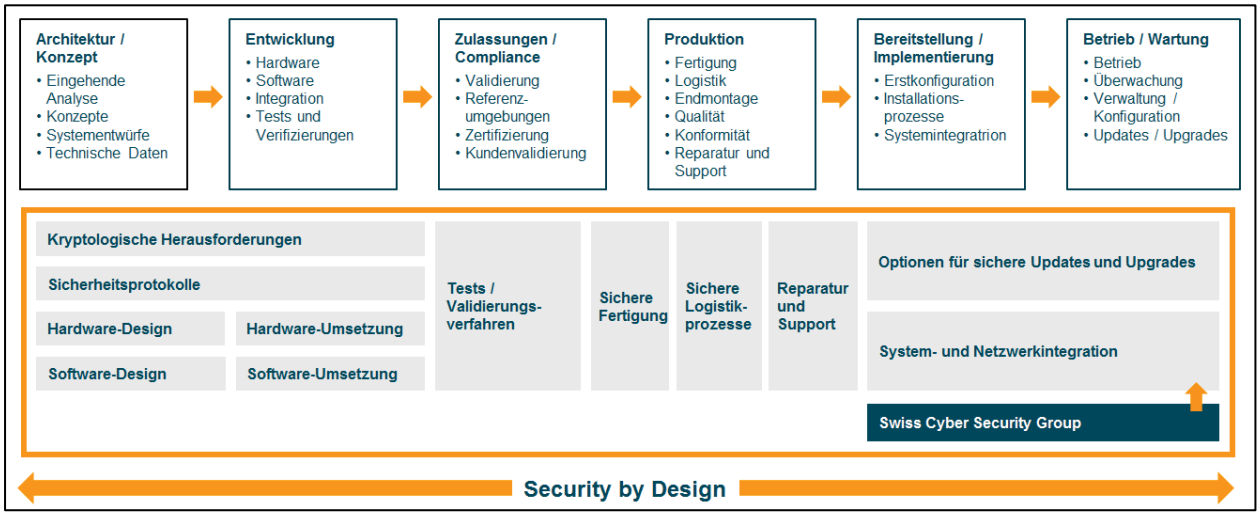
Oder besser: Wie müssen Medizinprodukte gebaut sein, so dass möglichst viele Arten von Software-Updates weder deren Sicherheit und Leistungsfähigkeit noch deren Anwendungsbedingungen beeinträchtigen können?

Produkte, die nachweislich auf solche Art und Weise gebaut sind, müssen nicht neu beurteilt werden – auch nicht über einen Nachtrag –, sofern deren Zulassung auf der Bewertung der technischen Dokumentation oder einer Baumusterprüfung beruht.

CyOne Security ist der kompetente Partner

Bei der Entwicklung von vernetzten Medizinprodukten wie auch beim Einsatz von bis anhin standalone-betriebenen Geräten in einem grösseren IT-Netzwerk bleibt die Sicherheit oft auf der Strecke. Deshalb müssen bisherige Sicherheitsansätze grundlegend überdacht werden. Verfügbarkeit, Verhinderung von Zweckentfremdung und Wahrung der Datensicherheit sind zwingende Voraussetzungen für eine seriöse Nutzung des enormen Potenzials, das die neuen digitalen Welten für uns bereithalten.

Informations- und Datensicherheit ist ein substanzieller Bestandteil der Entwicklung von Medizinaltechnik. Um die vernetzten Produkte und Systeme vor Cyber-Attacken zu schützen, bringt die CyOne Security tiefes Expertenwissen in Cipher- und Cyber Security in die Sicherheitskonzepte und -lösungen ein, die auf der 360°-Sicherheitskompetenz von Product Security, System Security und Operational Security basieren.



Beginnen Sie heute und schützen Sie Ihre vernetzten Medizinprodukte vor Cyber-Risiken.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Cyber-Security-Experten Ihre aktuellen und zukünftigen Sicherheitsbedürfnisse Ihrer vernetzten Medizinprodukte, damit wir mit Ihnen über zielgerichtete Sicherheitslösungen diskutieren können.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.

Eingeschränkt verwendbar © CyOne Security AG. Alle Rechte vorbehalten