

# Cybersicherheit vernetzter Medizinprodukte

Sicherheit von vernetzten Medizinprodukten in Zeiten zunehmender Cyberkriminalität: Wie begegnen wir den Gefahren der Zeit?

Heilmittelgesetz und Medizinprodukteverordnung verlangen von den Gesundheitseinrichtungen die Anwendung sicherer Medizinprodukte. Um diese Forderungen zu erfüllen, werden Medizingeräte geprüft, Geräteableitströme gemessen und Wartungstermine abgearbeitet.

## Standards und Praxis, die sich verändern müssen

Seit den 70er-Jahren haben Medizintechniker:innen Standards entwickelt, die aufzeigen, wie man sichere Technik im Umfeld der Patient:innen erzeugt. Auch in den Richtlinien «Schweizerische Gute Praxis für die Instandhaltung von Medizinprodukten (GPI)» kann bei Swissmedic nachgelesen werden, wie man in diesem Kontext Sicherheit erzeugt. Doch wie begegnen wir den Risiken, denen unsere vernetzten Medizinprodukte, unsere Softwares oder unsere Patientendaten-Management-Systeme (PDMS) ausgesetzt sind? Und wie erfüllen wir die Forderungen des MepV, Artikel 74, angemessene Massnahmen zur Gewährleistung der Cybersicherheit umzusetzen?

In seinem Vortrag zum Thema Cybersicherheit hat Ullrich Römmelt, Leiter Medizintechnik Servicecenter im Kantonsspital Aarau, an der IHS-Jahresfachtagung in Baden eine Umsetzungsvariante zur Erfüllung der gesetzlichen Forderungen aufgezeigt. Er hat dargestellt, worauf der Stand der Technik basiert und welche Massnahmen umgesetzt werden müssen, um diesen Stand im Umgang mit vernetzten Medizinprodukten zu erreichen.

Leider gibt es kein Rezeptbuch für Cybersicherheit. Gängige Normen zum Risikomanagement vernetzter Medizinprodukte liefern den Medizintechniker:innen und Spitalinformatiker:innen wenig konkrete Schutzmechanismen. Sie stellen Anforderungen an Strukturen und Prozesse, welche die Gesundheitseinrichtungen etablieren müssen.

## Risikomanagement im Lebenszyklus

Ziel muss es sein, alle Prozesse des Medizinprodukte-Lebenszyklus immer auch aus der Perspektive des Risikomanagements zu betrachten. Erst wenn es gelingt, von der Beschaffung bis zur Entsorgung alle Be-

teiligten an einen Tisch zu bringen wird es gelingen, in jeder Phase angemessene Sicherheitsmassnahmen zu finden und diese konsequent umzusetzen. Eine Kernaussagen von Ullrich Römmelt ist: «Auch wenn wir alle diese Massnahmen umsetzen, können wir nicht ausschliessen, dass es zu Cyber-Angriffen und in der Folge zu Beeinträchtigungen klinischer Prozesse kommt. Im Falle eines Schadens können wir aber zeigen, dass wir unsere vernetzte Medizintechnik auf dem Stand der Technik schützen und NICHT fahrlässig handeln.»

## Ein letzter Tipp: Die Klinikleitung muss ins Boot

Das Risikomanagement vernetzter Medizinprodukte verlangt einen klaren Auftrag und die Rückendeckung der Klinikleitung. Nur wenn die Führungsebene mit einbezogen ist, können die notwendigen Strukturen, Ressourcen und Prioritäten geschaffen werden, um die Cybersicherheit wirksam umzusetzen.

Die Präsentation von Ullrich Römmelt kann auf der IHS-Website heruntergeladen werden: <https://www.ihs.ch/Cyber-Security.pdf>

## ULLRICH RÖMMELT

Leiter Medizintechnik Servicecenter  
Kantonsspital Aarau AG  
[ullrich.roemmelt@ksa.ch](mailto:ullrich.roemmelt@ksa.ch)

## IHS: Offizielles Organ des IHS / Infrastruktur Hospital Schweiz Organe officiel de l'IHS / Infrastructure Hôpital Suisse

Herausgeber: IHS Geschäftsstelle,  
Postfach, 8302 Kloten

[www.ihs.ch](http://www.ihs.ch)  
[office@ihs.ch](mailto:office@ihs.ch)  
Redaktion: Sabrina Keinersdorfer  
[sabrina.keinersdorfer@ihs.ch](mailto:sabrina.keinersdorfer@ihs.ch)