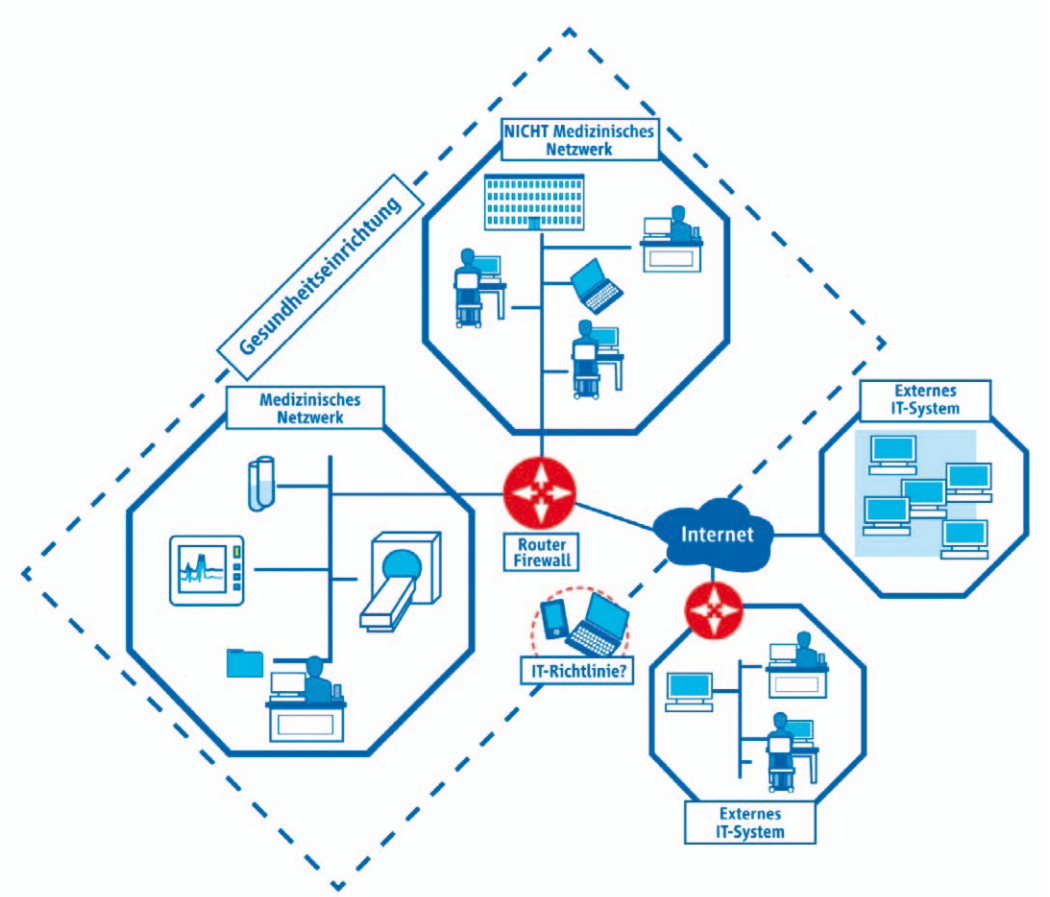
Cybersicherheit im Krankenhaus



Automatisierte und vernetzte Medizintechnik bietet große Vorteile für die Patientenversorgung. Denn die Offenheit zwischen Administration und Leistungserbringung sowie eine verbesserte Transparenz und Durchgängigkeit der Datenströme ermöglichen effizientere Prozesse in der Versorgung. Vernetzte Geräte sind jedoch auch eine potenzielle Einfallspforte für Schadprogramme. Deshalb ist es wichtig, geeignete Maßnahmen zur Erhöhung der Cybersicherheit zu ergreifen. Das gilt sowohl für interne IT-Systeme (z. B. Verwaltungssysteme) als auch externe IT-Systeme (z. B. IT-Geräte mit Remotezugriff, externe Speichermedien) sowie für Systeme mit integrierten Medizinprodukten (z. B. PC-basierte Medizinprodukte, medizinische Software-Produkte).

Gesetzliche Anforderungen und Zweckbestimmung versus sichere IT-Netze

Schadsoftware kann auf verschiedenen Wegen in ein medizinisches Netzwerk gelangen. Häufig wird sie sogar durch den Anwender selbst eingebracht, zum Beispiel 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 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 von vernetzten Medizinprodukten gefährden können. Unkontrollierte oder automatische, vom Medizinproduktehersteller nicht autorisierte Softwareupdates (z. B. für Virenschutz, Betriebssystem oder sonstige Anwendungssoftware) können die ins Netzwerk eingebundenen Medizinprodukte in ihrer Funktion beeinträchtigen und somit möglicherweise Patienten schädigen. Hersteller stehen hier also in einem Spannungsfeld zwischen gesetzlichen Anforderungen an die Sicherheit von Medizinprodukten bzw. dem Rahmen der Zweckbestimmung der Medizinprodukte einerseits und dem sicheren Betrieb von IT-Netzen andererseits.

IT-Netzwerke im Krankenhaus richtig sichern

Wie lassen sich IT-Infrastruktur und Geräte also schützen, ohne die gesetzlichen Vorgaben für Medizinprodukte zu verletzen? Sowohl bei organisatorischen Schritten, als auch bezüglich einer Anpassung in der Netzwerkarchitektur und der Systemabsicherung bieten sich Maßnahmen an, mit denen der Bedrohung des IT-Netzwerks effektiv begegnet werden kann. Dazu gehören unter anderem:

- Mitarbeiter regelmäßig schulen, um die Wahrscheinlichkeit für Schadsoftwarebefall zu reduzieren
- Klare Strukturierung des Netzwerks, um medizinische von nicht-medizinischen Netzwerkbereichen zu trennen. Die notwendigen Verbindungen sollten über wenige, aber gut gewartete Gateways erfolgen
- Schutzsoftware auf nichtmedizinischen Systemen installieren, um deren Infektion und die nachfolgende Verbreitung von Schadsoftware im medizinischen Netz zu verhindern.

Autor:
Hans-Peter Bursig,
Geschäftsführer des
ZVEI-Fachverbands
Elektromedizinische Technik
ZVEI
www.zvei.org/gesundheit

Hersteller und Betreiber: Wer ist wofür zuständig?

Hersteller, die für ihre Medizinprodukte die Verwendung in IT-Netzwerken erwarten oder vorhersehen, müssen bereits während des Designs mögliche Risiken, die an den Schnittstellen denkbar sind, hinsichtlich ihres Gefährdungspotentials bewerten und entsprechende Maßnahmen zur Risikominimierung definieren und implementieren. Sollte dies technisch nicht möglich sein, müssen Anwender bzw. Patienten hinreichend über diese Gefährdungen informiert werden, beispielsweise in der Gebrauchsanweisung. Betreiber dieser Medizinprodukte und IT-Netzwerke sind verpflichtet, sich bereits bei der Installation und Inbetriebnahme über mögliche Gefährdungen aller Art bei den involvierten Herstellern zu informieren und geeignete Maßnahmen in ihrer eigenen Organisation zu entwickeln, festzulegen und umzusetzen. Dazu gehören sowohl technische als auch organisatorische Maßnahmen, zum Beispiel die Festlegung und Implementierung von Richtlinien zur Nutzung der IT.

Bei Cybersicherheit im Krankenhaus ist Teamwork gefragt

IT-Systeme und ihre Vernetzung sind sowohl aus dem Alltag, wie auch aus dem Gesundheitswesen nicht mehr wegzudenken. Im klinischen Umfeld können damit jedoch besondere Risiken und potenzielle Gefährdungen für Patienten und Anwender verbunden sein. Deshalb sollte Cybersicherheit insbesondere bei Betreibern von medizinischen Einrichtungen einen hohen Stellenwert einnehmen. Sicherheitskonzepte, die auf lokalen Regelungen und Initiativen beruhen, sind allerdings mit Vorsicht zu betrachten. Denn sie bergen die Gefahr, dass die inhärente Sicherheit von Medizingeräten abgeschwächt wird oder diese inkompatibel zu anderen Regelungen werden. Stattdessen sollten Sicherheitskonzepte transparent und in Zusammenarbeit aller betroffenen Parteien erarbeitet werden. Danach müssen sie regelmäßig gewartet, überprüft und, wo notwendig, verbessert werden, um den Anforderungen kontinuierlich zu genügen. Das erforderliche Sicherheitsniveau kann nur erreicht werden, wenn alle Beteiligten ihrer Verantwortung gerecht werden und gemeinsam dran arbeiten, Cybersicherheit zu gewährleisten.

Weitere Informationen stehen in den ZVEI-Positionspapieren „IT-Sicherheit in Medizintechnik und Krankenhaus-IT" und „Sichere medizinische Subnetze" zur Verfügung. ◄