# Absicherung medizinischer Endgeräte in medizinischen Einrichtungen

Wie Sie mit Zscaler sensible Patientendaten schützen und Ihre Security auf ein neues Level heben

# Einleitung

Deutsche Krankenhäuser stehen im Zuge der Digitalisierung und Restrukturierung vor komplexen IT-Sicherheitsherausforderungen. Die neue Krankenhausreform (KHVVG) wird viele Konsolidierungen mit sich bringen, zudem erfordern weitere gesetzliche Vorgaben wie die DSGVO, KRITIS, ISO 27001, DIN EN IEC 80001-1:2023, DIN EN ISO 11073 und das IT-Sicherheitsgesetz (IT SiG 2.0) Maßnahmen zum Schutz sensibler Patientendaten. Diese Anforderungen ziehen nicht nur technische sondern auch grundlegende organisatorische Maßnahmen mit sich (z. B. ISMS, MPG und weitere). Außerdem erhöhen digitale Entwicklungen wie ePA, Telemedizin und die Vernetzung der Medizingeräte die potenzielle Angriffsfläche erheblich. Neben einer geforderten hohen Verfügbarkeit und einem immer breiteren digitalen medizinischen Angebot sollen trotzdem moderne Zugriffskontrollen und Verschlüsselungen ermöglicht werden. Cyber-Attacken wie Ransomware und Phishing-Angriffe sind mittlerweile eine alltägliche Bedrohung, vor allem im Gesundheitswesen. Eine Vielzahl von Einzellösungen, welche das Management komplexer werden lassen, gehen einher mit eingeschränkten Budgets und fehlenden Ressourcen. Dies alles führt zu Lücken in der Sicherheitsarchitektur von medizinischen Versorgern und Dienstleistern. Ein ganzheitlicher Ansatz, der die Vielschichtigkeit verringert und das Sicherheitsniveau erhöht, ist somit unausweichlich für eine nachhaltige Planung der Architekturen von medizinischen Infrastrukturen.

Im Krankenhaus und den Arztpraxen nehmen die Anzahl medizinischer Endgeräte mit Vernetzung ebenso wie das Internet of Medical Things (IoMT-Geräte) stetig zu. Die Medizingeräte sind häufig nicht oder nur ungenügend in die Gesamtarchitektur integriert, sondern werden auch aus infrastruktureller Sicht meist getrennt von der Betriebs-IT betrachtet. Dies wiederum führt zu mangelnder Visibilität und fehlendem Management der Sicherheitslösungen. Das daraus entstehende Risiko wirkt sich besonders auf die Patientensicherheit, Behandlungseffektivität und auf die Reputation aus.

Traditionelle Netzwerke können die Anforderungen und Innovationen im Gesundheitswesen kaum noch effektiv abbilden. Eine stetig steigende Angriffsfläche führt vermehrt zu Sicherheitsvorfällen.

Somit müssen IT- und Sicherheitsteams sich mit einer großen Auswahl an Cybersicherheitslösungen auseinandersetzen. Einzellösungen müssen dann jeweils betrachtet, getestet, beschafft und implementiert werden.

Im Nachgang muss das Produktmanagement durch Fachpersonal geschult, die Lösung in das bestehende Gesamtkonzept integriert und die Interoperabilität zwischen weiteren Sicherheitslösungen gewährleistet werden. Kurzum: Es wird mit jeder neuen Lösung komplexer und aufwendiger.

## Die Herausforderung

Im Bereich der Cybersicherheit sind besonders Medizingeräte unzureichend geschützt. Die Hauptgründe sind:

- Investitionsschutz durch lange Laufzeiten (Abschreibung) und eine einhergehende Nutzung veralteter Betriebssysteme wie z. B. embedded OS. Viele Medizingeräte dürfen nicht eigenständig gewartet werden, lediglich durch unzureichend geschützte Fernzugriffe, meist ohne Überwachung und granulare Steuerung.
- Die Funktionalitäten der Medizingeräte beschränkt sich meist allein auf den klinischen Anwendungsfall, jedoch werden Sicherheitsstandards vernachlässigt.
- Medizinische Geräte werden oft als eigene Infrastruktur gesehen und werden meistens getrennt von der KH-IT betrachtet.
- Fehlende Kooperation und Kommunikation zwischen Medizingeräte-Herstellern und Regulierungsbehörden.

## Die Folgen

**Mangelnde Sichtbarkeit**
Schatten-IT, BYD und Geräte außerhalb der bestehenden Asset-Liste sind nicht oder nur sehr schwer für die interne KH-IT verwaltbar und kontrollierbar. Die Inventarisierung stellt häufig eine Herausforderung dar.

**Betriebliche Komplexität**
Die Interoperabilität zwischen Anwendungen und Geräten ist mitunter nicht oder nur unzureichend gegeben. Ein Know-How-Transfer zwischen IT-Teams und Mitarbeitern lässt sich bei der Arbeitslast und einer häufig angespannten Personalsituation nicht durchführen.

## Allgemeine Bedrohungslage

Medizinprodukte sind ein beliebtes Ziel für Cyberkriminalität. 2020 fand das BSI über 150 Schwachstellen mit unterschiedlichem Schweregrad. Dabei wurden implantierbare Herzschrittmacher, Insulinpumpen, Beatmungsgeräte, Infusionspumpen und Patientenmonitore untersucht. Bei einem Cyberangriff können nicht nur sensible Patientendaten gestohlen, sondern auch das Verhalten der Geräte beeinflusst werden. Ein kritischer Gesundheitszustand bis hin zum Tod kann die Folge sein.

Der aktuelle Bericht der Zscaler Threatlabz aus 2024 zeigt das Gesundheitswesen weltweit auf Platz 2 der Ransomware-Angriffe. Patientendaten sind ein sehr wertvolles Gut.

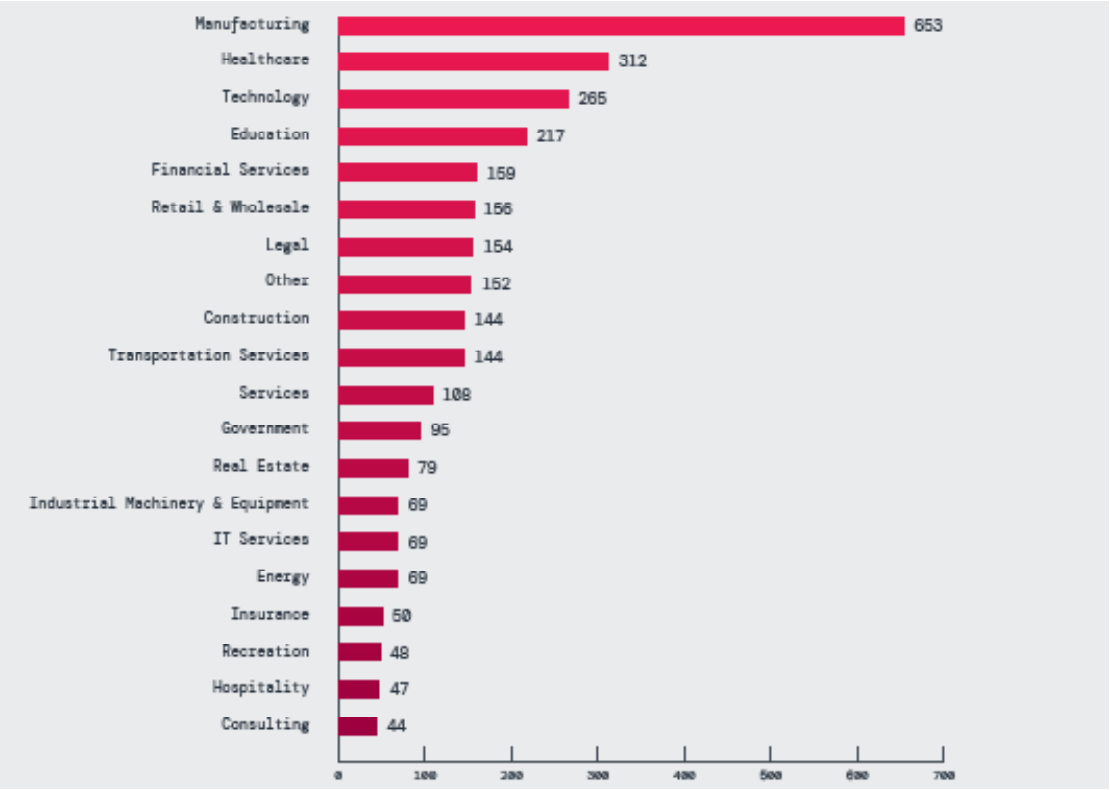
Täglich wird in deutschen Medien über Cyberangriffe berichtet. Ein paar Beispiele:

- Cyberangriff in Bayern: Krankenhaus mit Ransomware infiziert. 300 GB sensibler Daten im Darknet.
- Ransomware-Attacke in Berlin: Notfallbetrieb ausgelöst. Zugriff auf Systeme nicht mehr möglich.
- Ransomware-Attacken und deren Gefahren für Leib und Leben

### Branchen, die am stärksten von Ransomware betroffen sind

Top 10 Branchen mit den meisten Ransomware-Angriffen basierend auf Data-Leaks-Websites

1. Fertigung
2. Gesundheitswesen
3. Technologie
4. Bildung
5. Finanzdienstleistungen
6. Einzel- & Großhandel
7. Rechtswesen
8. Sonstiges
9. Bildungswesen
10. Transportdienstleistungen



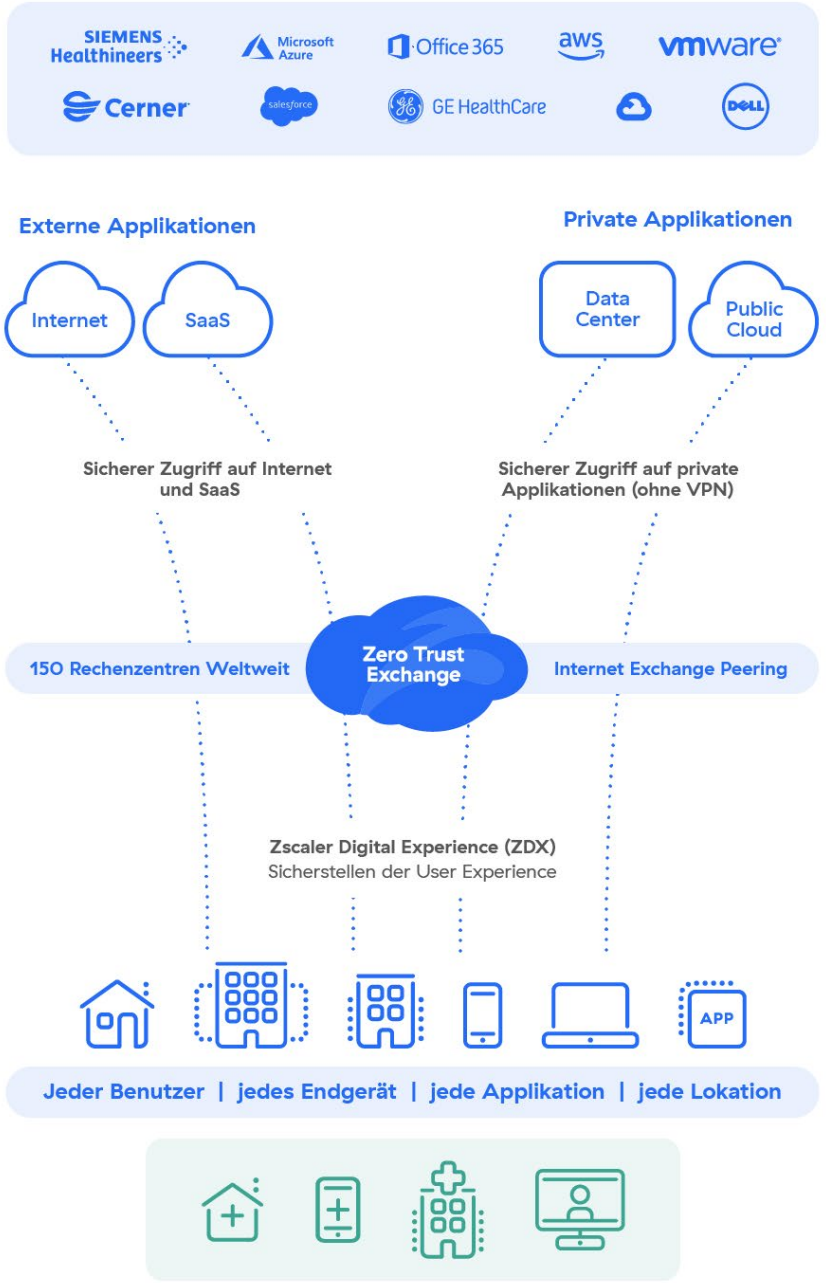
## Zero-Trust-Architektur

Zscaler Zero Trust Exchange unterstützt im Gesundheitswesen eine Vielzahl von Anwendungsfällen, die über die Sicherung des Mitarbeiterzugangs hinausgehen. Dazu gehören die Sicherung von SaaS-Daten wie z. B. bei KIS-Anwendungen, Patientendienstleistungen, IoMT-Geräten und die Verbindung mit MVZs, Fachärzten oder Arztpraxen. Die Flexibilität der Plattform ermöglicht es, diverse klassische Netzwerkkomponenten wie Web-Gateways und VPNs zu ersetzen, und erleichtert eine schnelle, einheitliche Bereitstellung und eine hohe Verfügbarkeit unter Berücksichtigung der Sicherheitsanforderungen und gesetzlichen Vorgaben.

Den traditionellen Netzwerk- und Sicherheitsmodellen stehen Herausforderungen gegenüber, um moderne Bedrohungen effektiv abzuwehren und die eigene Infrastruktur zu schützen. Diese Architekturen, die für eine Rechenzentrums-zentrierte Welt entwickelt wurden, schaffen heute mitunter zusätzliche Schwachstellen und sind zunehmend aufwändig und damit kostspielig.

Zscaler hat die Sicherheitsarchitektur mit seinem Zero-Trust-Ansatz neu definiert und als einheitliche SaaS-Plattform entwickelt. Der gesamte Datenverkehr wird dabei über die Plattform geleitet, wo Sicherheitsrichtlinien konsequent durchgesetzt werden:

- Konnektoren verbinden sämtliche Geräte, einschließlich medizinischer Geräte in Krankenhäusern, MVZs oder Arztpraxen, mit der Plattform. Unautorisierter Zugriff ist ausgeschlossen.
- Sicherer Zugriff auf kritische Anwendungen wie KIS, Radiologie und mehr. Diese Anwendungen sind von außen nicht sichtbar, was die Angriffsfläche deutlich reduziert.
- Schnelle Integration oder Zusammenlegung anderer Einrichtungen in Tagen oder Wochen statt Monaten oder Jahren.
- Keine Agenteninstallation an den Standorten erforderlich, außer bei mobilen Endgeräten wie Notebooks, Tablets oder Smartphones (ohne Z-SIM).
- Ablösung von VDI-Lösungen (Virtual Desktop Infrastructure) in Bereichen wie Radiologie oder Nuklearmedizin. Dies reduziert Kosten, schafft Transparenz und erhöht die Sicherheit, indem die Lösungen Teil der Sicherheitsarchitektur werden.



- Integration von medizinischen Cloud-Anwendungen wie Google Medical oder AWS Health Services.
- Sichere Einbindung aller medizinischen Geräte: Die Z-SIM versorgt mobile Medizingeräte wie Insulinpumpen oder Patientenüberwachungssysteme.
- Privilegierter Remotezugriff ermöglicht ausschließlich autorisierten Drittanbietern den Zugriff auf Infrastruktur oder Medizinprodukte zu Wartungszwecken. Eine Aufzeichnung der Sitzungen ist ebenfalls möglich.
- Segmentierung von Benutzern, Anwendungen und Netzwerk reduziert Komplexität und Kosten, wodurch teure Hardware eingespart werden kann.
- Kontinuierliche Überwachung der Benutzererfahrung stellt einen reibungslosen Krankenhausbetrieb sicher und ermöglicht dem Personal, mehr Zeit für die Patienten zu haben.

## Privilegierter Remotezugriff für IoMP

Krankenhausbetreiber verfügen außerhalb der eigenen IT-Netze über wenig Kontrolle bei der Fernwartung von Medizinprodukten. Insbesondere im Bereich der Radiologie, wo häufig eigene Wartungszugänge zumeist über VPN-Verbindungen der jeweiligen Hersteller genutzt werden. Ein privilegierter Remotezugriff stellt notwendige Konsolen bereit und sichert einen Zugriff auf dedizierte Systeme für autorisierte Benutzer. Die Nutzung wird protokolliert und Sitzungen können aufgezeichnet werden.

## Zscaler SIM (Z-SIM)

In vielen modernen Medizingeräten wie Patientenmonitoring oder OP-Instrumenten ist eine SIM-Karte implementiert, um Mobilität und Flexibilität zu gewährleisten. Folgen sind eine erschwerte Verwaltbarkeit und Implementierung in die Sicherheitsarchitektur.

Zscaler stellt eine vorbereitete SIM-Karte mit Anbindung an die eigene Zero-Trust-Landschaft bereit. Dabei ist keine Installation eines Agenten erforderlich. Nachfolgende Merkmale werden dabei erfüllt:

- Schutz der Endgeräte
- Direkte Verbindung über den Provider, dadurch niedrigere Latenzen
- Durchsetzung der Unternehmensrichtlinien
- Durchgänge Überwachung und Sichtbarkeit durch Analyse der Authentifizierung und Aufdeckung nicht autorisierter Geräte
- Eingrenzung eines Betriebes auf Ebene des Krankenhausgeländes durchsetzbar

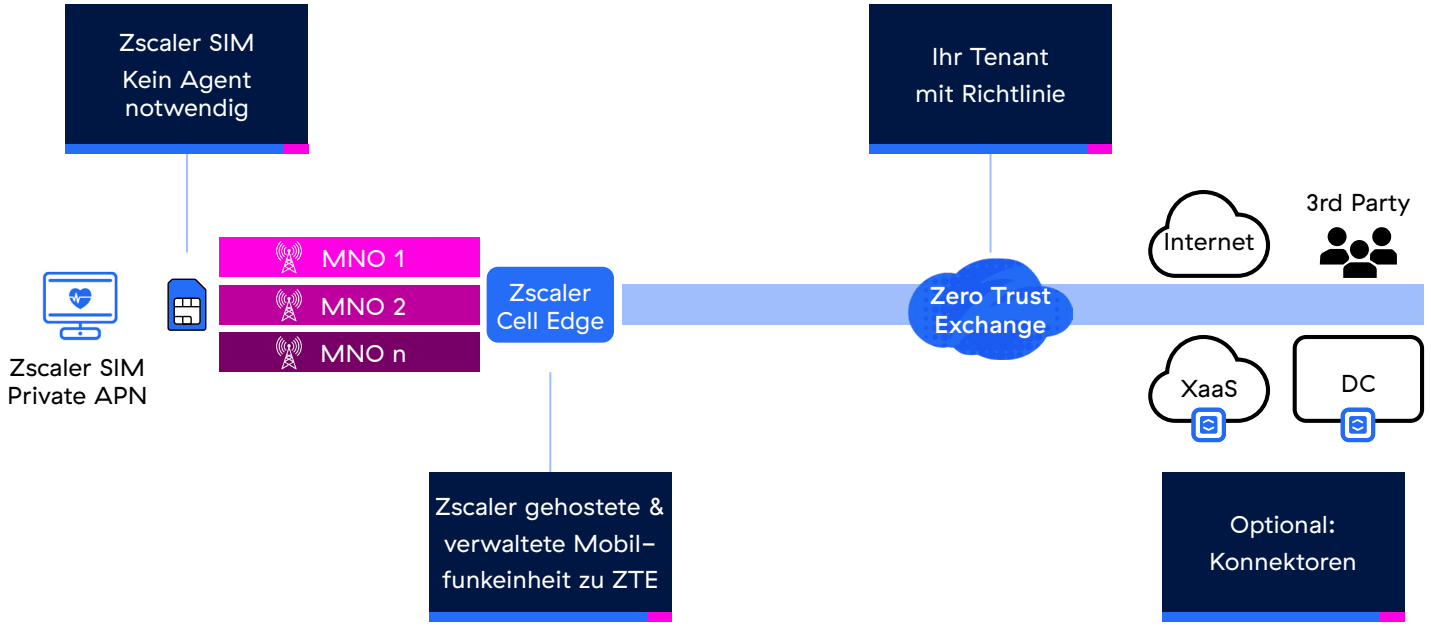
**Vorteile der Zscaler-Lösung im Krankenhausumfeld**

**Cloud-native Architektur**
Keine Abhängigkeit von lokalen Appliances – somit keine weiteren Kosten für Anschaffung und Verwaltung.

**Skalierbarkeit**
Flexible Anpassung der Sicherheitsinfrastruktur bei wachsenden Anforderungen, „KHVVG-Ready“ – für Konsolidierungen und Umstrukturierungen.

**Erhöhte Resilienz**
Schutz vor modernen Bedrohungen durch kontinuierliche Bedrohungsanalyse.

**Compliance**
Unterstützung bei der Einhaltung gesetzlicher Vorgaben und Dokumentationspflichten.



## Fazit

Durch die Implementierung von Zscaler-Lösungen können deutsche Krankenhäuser und Anbieter von Gesundheitsleistungen ihre IT-Sicherheit erheblich verbessern. Die Cloud-basierte Sicherheitsarchitektur kann die operationellen Kosten reduzieren, die Risiken minimieren und die kontinuierliche Verfügbarkeit von Gesundheitsdiensten sicherstellen.

Mehr dazu, erfahren Sie hier:
https://www.zscaler.com/de/industries/public-sector-germany-healthcare

## Noch Fragen?

Kontaktieren Sie uns für weitere Informationen oder vereinbaren Sie ein Security Assessment.

## Ihr Zscaler Public Sector Team


**Markus Ocker**

Solution Engineer Healthcare
mocker@zscaler.com

**Leon Wimmer**

Sales Development Representative Healthcare
lwimmer@zscaler.com


zscaler™ | Experience your world, secured.™

**Über Zscaler**
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, zuverlässiger und sicherer arbeiten können. Die Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an beliebigen Standorten vor Cyberangriffen und Datenverlust. Die SSE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.de** oder folgen Sie uns auf Twitter unter **@zscaler**.