Barracuda
Your journey, secured.

# Digitale Transformation im Gesundheitswesen

## Ihr Barracuda Schutz zur Bewältigung Ihrer Herausforderungen im modernen Gesundheitswesen

Solution Guide

NETWORK SECURITY

## Marktumgebung

### Herausforderungen an ein modernes Gesundheitswesen im Zeitalter der Digitalisierung

Die Ereignisse der letzten Jahre haben die Gesundheit in den Fokus der Öffentlichkeit, der Wissenschaft und der Politik gerückt. Die Gegenwart stellt wie selten zuvor enorme Anforderungen, die organisatorischen und logistischen Herausforderungen sind beispiellos und es gilt mit angespannten Ressourcen Großes zu leisten. Die fortschreitende Entwicklung von Gesundheitstechnologien und die zunehmende Digitalisierung von Medizinprodukten können zur Bewältigung der umfangreichen Aufgaben einen wertvollen Beitrag leisten, jedoch wird dadurch die ohnehin schon weitläufige digitale Umgebung noch komplizierter.

Die Rettung von Leben und die bestmögliche Versorgung von Patienten stehen bei Leistungserbringern im Gesundheitswesen an erster Stelle, aber neben den medizinischen Kernaufgaben muss auch eine geschützte, leistungsfähige und ausfallssichere IT-Infrastruktur bereitgestellt und eine Reihe von Gesetzen, Datenschutzbestimmungen und Dokumentationspflichten berücksichtigt werden. In der heutigen digitalen und vernetzten Welt spielen die IT-Experten im Gesundheitswesen eine ebenso wichtige Rolle wie das medizinische Personal.

## IT-Herausforderungen

### Gefahren und Risiken für die IT im Gesundheitswesen

Das Gesundheitswesen steht aufgrund seiner Bedeutung und des Werts der dort verarbeiteten Daten besonders im Visier von Angriffen. Cyberkriminellen ist wohl bewusst, dass Ausfallzeiten und Störungen des Klinikbetriebs Menschenleben gefährden können und ihnen dieser Umstand ein starkes Druckmittel, zum Beispiel bei der Erpressung, mittels Ransomware, an die Hand gibt. Aber auch Gesundheitsinformationen aus Patientenakten und Finanzdaten, die sich in den Systemen dieser Einrichtungen befinden, sind für Hacker von großem Wert.

Da der Vernetzungsgrad von Medizinprodukten in Krankhäusern steigt – was im Ergebnis für eine schnell wachsende Angriffsfläche und eine steigende Anzahl von Drittnutzern, die auf Netzwerk-Ressourcen zugreifen führt – ist Cyber-Security sowohl für Medizinproduktehersteller wie auch für Betreiber zu einem wichtigen Thema geworden. Heute kommen vermehrt Systeme aus dem Bereich Internet-of-Medical-Things (IoMT) für unterschiedlichste Therapien zum Einsatz – von denen viele nur unzureichende Sicherheitsfunktionen bieten. Hersteller und Betreiber müssen angesichts einer globalen und schnelllebigen Bedrohungslage angemessen auf diese neuartigen Risiken reagieren.

**Zu den wichtigsten Sicherheitsvorfällen gehören:**

- Phishing-Angriffe **(57%)**
- Credential Harvesting-Angriffe **(21%)**
- Social-Engineering-Angriffe **(20%)**
- Ransomware oder andere Malware **(20%)**
- Diebstahl oder Verlust **(16%)**
- Angriffe auf Websites oder Webanwendungen **(14%)**
- Fahrlässige Insider-Aktivitäten **(13%)**
- Sicherheitslücke oder Datenverlust **(11%)**
- Böswillige Insider-Aktivitäten **(10%)**

Source: 2020 HIMSS Cybersecurity Study

**Nachfolgend einige Sicherheitsrisiken in Überblick:**

### Gefährliche E-Mails

Kommunikation ist besonders in Krisenzeiten von enormer Bedeutung. E-Mail wird intensiv genutzt und stellt deshalb für Cyberkriminelle ein häufig genutztes Einfallstor für Angriffe dar. Die hierbei zum Einsatz kommenden Angriffstechniken wie Malware, Phishing, Brand-Impersonation, Extortion, Account-Takeover, und andere – insgesamt lassen sich 13 Bedrohungstypen benennen – werden zunehmend raffinierter. Eine einfache „Spam & Virus Firewall“ reicht deshalb längst nicht mehr für einen effizienten Schutz aus. Heute ist ein umfassendes KI-gestütztes Sicherheitskonzept nötig.

### Ransomware

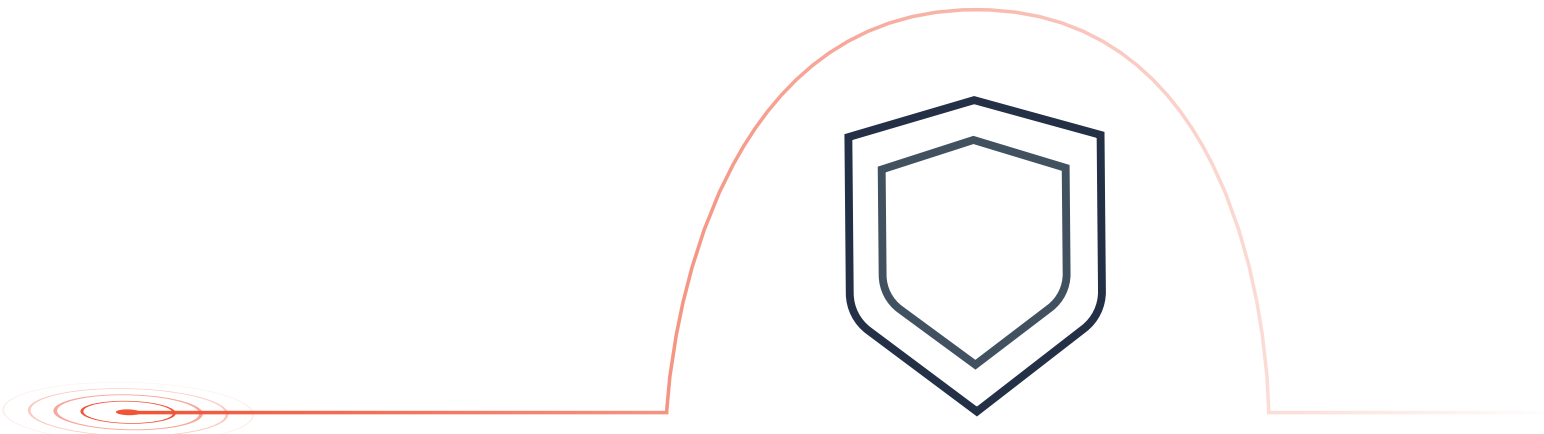
Die Zahl der Ransomware-Angriffe auf Gesundheitseinrichtungen ist 2020 deutlich angestiegen. Zu den bekanntesten Ransomware-Varianten zählen hier etwa Locky oder WannaCry. Diese Attacken verschlüsseln Dateien auf dem Computer, für die anzunehmen ist, dass sie für den Besitzer sehr wichtig und möglicherweise unwiederbringlich sind. Um die von der Ransomware verschlüsselten Daten wieder entschlüsseln zu können, wird der Geschädigte aufgefordert, ein Lösegeld zu bezahlen, damit er eine Software zur Entschlüsselung erhalte. Im Gesundheitswesen sind Vorfälle dieser Art absolut inakzeptabel und ein effizienter Schutz der alle Angriffsvektoren abdeckt deshalb unerlässlich.

### Zunehmende Vernetzung – Stichwort: Internet der Dinge

Die Digitalisierung ermöglicht erstaunliche Fortschritte im Gesundheitswesen und in der vernetzten Medizintechnik, dabei hat das Internet der Dinge einen bedeutenden Anteil. Der Schutz und die sichere Konnektivität dieser Systeme ist von größter Bedeutung, doch die Vielzahl der unterschiedlichen Gerätetypen erschwert diese Aufgabe erheblich. Überdies sind diese Geräte oft nur unzureichend abgesichert und übertragen Daten über das öffentliche Mobilfunknetz oder das WLAN. Deshalb muss diese Medizintechnik in die gesamte Sicherheitsarchitektur der Gesundheitseinrichtung integriert werden, eine Überprüfung der Gerätenutzer erfolgen und Zugriffsbeschränkungen auf diejenigen, die ein Gerät wirklich benötigen durchgesetzt werden.

### Nicht gepatchte Betriebssysteme und VLAN-Problematik

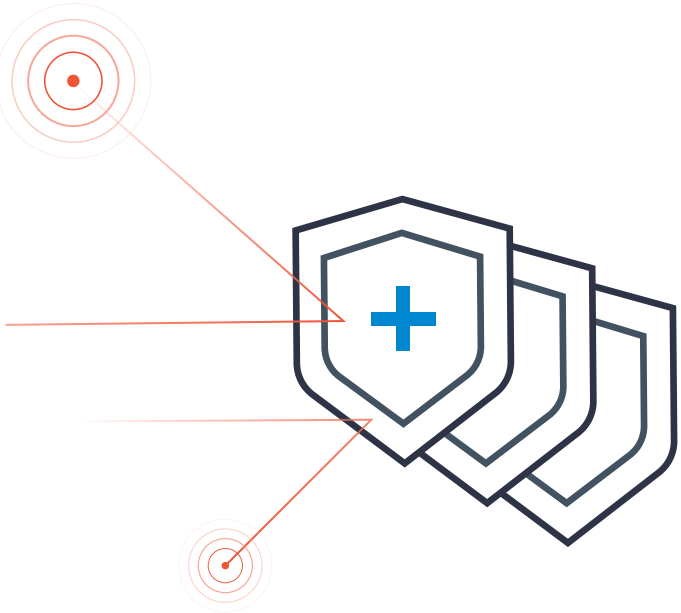
Eine für Einrichtungen im Gesundheitswesen spezifische Gefahrenquelle ist die Anzahl der Geräte mit veralteten, nicht mehr unterstützten Betriebssystemen. Gerade diese Geräte gehören meist zu den wichtigsten innerhalb der jeweiligen Organisationen, das davon ausgehende Risiko muss man von daher sehr ernst nehmen. Auch ist die Netzwerkinfrastruktur im Gesundheitswesen nach wie vor oft ein wunder Punkt. In der Mehrzahl der VLANs (logisches Teilnetz) sind sowohl medizinische Geräte als auch klassische IT-Geräte zugeordnet. Hier lässt sich schon durch verhältnismäßig einfache Maßnahmen einer effektiven Netzwerksegmentierung das Sicherheitsniveau deutlich erhöhen.



## Barracuda Networks – Barracuda Produktlinien

### Barracuda Networks – Ihr verlässlicher Partner für IT-Sicherheit

Barracuda Networks, mit seinem internationalen Hauptsitz im Silicon Valley, bietet ein umfangreiches Produktportfolio zum Schutz vor Bedrohungen, die auf E-Mail, Web-Applikationen und Netzwerk-Infrastrukturen abzielen, sowie Produkte, die die Anwendungsbereitstellung, den Netzwerkzugang und die Datensicherheit verbessern. Diese leistungsstarken, benutzerfreundlichen und erschwinglichen Lösungen werden bereits von mehr als 200.000 Unternehmen weltweit genutzt.



### Barracudas Lösungsportfolio

| EMAIL PROTECTION | APP & CLOUD SECURITY | NETWORK SECURITY | DATA PROTECTION |
|---|---|---|---|
| Über 91 % der gezielten Cyber-Angriffe beginnen mit einem E-Mail. Diese E-Mail-basierten Angriffe unterbrechen den Geschäftsbetrieb, verursachen finanzielle Schäden und beeinträchtigen die Integrität des Unternehmens. Barracuda bietet ein vollständiges Sortiment, von der physischen Appliance bis zur SaaS-Lösung, mit mehreren Schutzebenen, die alle Aspekte Ihrer E-Mail-Infrastruktur umfassen. | Sichern Sie all Ihre Webanwendungen. Barracuda Cloud Application Protection ist eine integrierte Plattform, die eine umfassende Reihe von ineinandergreifenden Lösungen und Funktionen vereint, um vollständige Anwendungssicherheit zu gewährleisten. Barracuda Web Application Firewall ist sowohl als Appliance, die vor Ort implementiert oder in der Cloud gehostet werden kann, als auch in Form einer innovativen SaaS-Lösung verfügbar. | Barracuda CloudGen Firewall schützt Ihre Benutzer, Applikationen und Daten - unabhängig davon, wie Ihre Infrastruktur aussieht und gewährleistet sichere und zuverlässige Konnektivität zwischen mehreren Standorten und in der Cloud. Barracuda CloudGen Firewall als physische oder virtuelle Appliance und auch für die Cloud verfügbar. Spezielle Lösungen für das Internet der Dinge runden das Sortiment ab. | Wegen der zunehmend komplexer werdenden Infrastrukturen und angesichts gezielter Cyberangriffe ist eine umfassende Backup-Strategie zum Schutz Ihrer Daten unerlässlich. Barracudas All-in-One-Ansatz zur Datensicherung macht es einfacher denn je, Ihr Unternehmen vor Datenverlust und -diebstahl zu schützen. Daten können an jedem Ort, einschließlich der Cloud, gesichert werden und Sie können sogar Ihre Office-365-Daten wie E-Mails effektiv sichern. |

**Weitergehende Informationen finden Sie hier:**
de.barracuda.com


Barracuda Networks AG
Prime Center 1
Flughafenstrasse
CH-8060 Zürich

Barracuda Networks AG
Eduard-Bodem-Gasse1
A- 6020 Innsbruck

**So erreichen Sie uns:**
dachsales@barracuda.com
Tel: CH: +41 31 528 04 87

dachsales@barracuda.com
Tel: A: +43 508 100

## Referenzen

**Barracudas Sicherheitslösungen werden weltweilt erfolgreich eingesetzt**

Humanitas DMH

Humanitas DMCH stellt die Barracuda CloudGen Firewall über Microsoft Azure bereit, wodurch die Netzwerksicherheit und die Patientenpflege erheblich verbessert werden.

Humanitas DMH - CloudGen Firewall for Azure

Mount Sinai

Mount Sinai wendet zum Schutz von sensibler Patientendaten die Barracuda CloudGen WAF für Azure an.

Mount Sinai - CloudGen WAF for Azure

Primary Care Network Calgary Foothills

Calgary Foothills schützt ihre Office 365 Daten mit der cloud-basierten Barracuda Backup Lösung.

Primary Care Network - Calgary Foothills - Backup and Cloud-to-Cloud Backup

King Edward VII's Hospital

Führende Privatklinik konsolidiert E-Mail-Schutz, um die Daten der "Crown Jewels" der VIP-Gäste zu sichern.

King Edward VII's Hospital - Total Email Protection

Pine Belt Mental Healthcare Resources

Barracuda Web Security Gateway beseitigt Viren bei Pine Belt Mental Healthcare und bietet gleichzeitig eine sichere Browsing-Umgebung

Pine Belt Mental Health - CloudGen Firewall, Web Security Gateway, Email Security Gateway

tirol kliniken

Verfügbarkeit, Sicherheit & Effizienz als zentrale Herausforderung

Tirol Kliniken - CloudGen Firewall

Barracuda
Your journey, secured.