Rohde & Schwarz Cybersecurity

IT-SICHERHEIT IM GESUNDHEITSWESEN

Investitionen in das „smarte“ Krankenhaus der Zukunft

ROHDE&SCHWARZ

Make ideas real

INHALT

EINLEITUNG

Diese Broschüre befasst sich mit dem umfangreichen „Ökosystem IT-Sicherheit im Gesundheitswesen", zu dem Infrastruktur, Software, Systeme und Endgeräte gleichermaßen gehören. Die Cybersecurity bezieht sich dabei auf die Sicherung der dazugehörigen Komponenten. Mitarbeitende im Gesundheitsbereich sollen mit Hilfe dieser Broschüre einen profunden Überblick erhalten, wie Cybersicherheitsziele erreicht – und gehalten werden können. Es werden mehrere Themenfelder und Richtlinien behandelt, die sich im steten Wandel befinden – und die dabei nur so gut sind, wie die Personen, die diese umsetzen und anwenden.

Wir adressieren Beschäftigte im Gesundheitswesen, die in technischen Positionen arbeiten und vor allem Führungspersonal wie CIO, CISO, CTO und IT-Teams sowie jene, die mit der Beschaffung in Gesundheitsorganisationen betraut sind.

Krankenhäuser leisten ärztliche und pflegerische Leistungen, um Verletzungen und Erkrankungen zu versorgen. Als Einrichtung mit herausragender Bedeutung zum Schutz der Bevölkerung zählen sie zu den Kritischen Infrastrukturen (KRITIS) in unserer Gesellschaft. Deren Ausfall, Beeinträchtigung oder Störungen gilt es zu vermeiden, um die Verfügbarkeit der Dienste und Prozesse zu garantieren. Moderne medizinische Versorgung und digitale Lösungen gehören dabei zusammen. Die Digitalisierung bietet dem Gesundheitssektor effizientere, leistungsfähigere Systeme. Diese sind allerdings auch angreifbar und können damit gleichermaßen das Gemeinwohl bedrohen.

Krankenhäuser sind auf vielfältige Weise angreifbar. Der Ausfall wichtiger Energie- und Versorgungsquellen wie Wasser oder Strom, aber auch Naturkatastrophen beeinflussen ihre Verwundbarkeit[1]. Moderne medizinische Versorgung mittels IT-Anwendungen und EHR-Systemen gehört zum Arbeitsalltag von Medizinern. Ziel ist die optimale Versorgung von Patienten. Der Schutz dieser Anwendungen wird zu einem zentralen Anliegen, denn sie müssen in lebensbedrohlichen Situationen ausfallsicher funktionieren. Dies betrifft beispielsweise die Kommunikation zwischen Computertomographen Beatmungsgeräten, Anästhesiegeräten oder Geräten bei der Medikationssteuerung. „Die Digitalisierung" birgt im Idealfall Potenzial, den Ablauf im Krankenhaus kostensensitiv und effizient zu gewährleisten.

Je mehr Bereiche innerhalb eines Krankenhauses durch IT-Systeme optimiert werden, desto mehr werden sie potenziell zu einem Angriffsziel. Krankenhäuser sind in den letzten Jahren gezielt angegriffen worden, Sicherheitsvor- und -ausfälle machen vor dem Gesundheitssektor keinen Halt.

[1] http://www.tagesspiegel.de/weltspiegel/ueberschwemmungen-chaos-inmittelhessen/753824.html

FEBRUAR 2016

Lukaskrankenhaus Neuss in Nordrhein-Westfalen **(Trojaner)**

48 weitere Kliniken in Nordrhein-Westfalen **(Virus Locky)**

MAI 2017

Gesundheitsdienst „National Health Service" (NHS): 40 Krankenhäuser und zahlreiche Arztpraxen in Großbritannien **(WannaCry)**

SEPTEMBER 2018

3 AMEOS-Kliniken in Bremerhaven und Geestland **(Phishing Mail mit infiziertem Anhang)**

NOVEMBER 2018

Klinikum Fürstenfeldbruck in Bayern **(Trojaner)**

Abbildung 1:

Das Electronic Medical Records Adoption Model (EMRAM) ist ein Modell, um den Digitalisierungsgrad in Krankenhäusern zu beschreiben. Es unterscheidet dabei in 7 Stufen von begrenzten, ergänzenden Abteilungssystemen bis hin zum vollständig papierlosen EMR-Umfeld.[2]

In Europa gibt es insgesamt 66 Krankenhäuser mit EMRAM-Stufe 6 oder 7, davon 6 im DACH-Gebiet.[3]

STUFE 7	Lückenlose ePA integriert alle klinischen Bereiche (z. B. Ambulanz, Intensivstation, Notaufnahme) und ersetzt alle (medizinischen Papierakten); Einsatz von Standards zum Datenaustausch für die integrierte Versorgung; Data Warehouse als Basis für klinische und betriebliche Analysen
STUFE 6	Klinische Dokumentation interagiert mit intelligenter klinischer Entscheidungsunterstützung (basierend auf diskreten Datenelementen) UND Vorhandensein eines IT-gestützten, geschlossenen Medikationsgabeprozesses (closed loop medication)
STUFE 5	Integrierte Bildmanagementlösung (z. B. PACS) ersetzt alle filmbasierten Bilder
STUFE 4	Elektronische Verordnung mit klinischer Entscheidungsunterstützung (basierend auf einer Rules-Engine) in mindestens einem klinischen Bereich und für Medikation
STUFE 3	IT-gestützte klinische Dokumentation sowie Einsatz elektronischer Verordnungen durch Ärzte bzw. Pflegepersonal; dies beinhaltet auch die Dokumentation der Medikamentengabe (eMAR)
STUFE 2	Eine Elektronische Patientenakte (bzw. ein Clinical Data Repository) ermöglicht die Zusammenfassung und Normalisierung von Daten aus verschiedenen klinischen Quellen im gesamten Krankenhaus
STUFE 1	Informationssysteme für die großen diagnostischen und versorgenden Abteilungen (Labor, Radiologie, Apotheke) sind installiert bzw. Daten von externen Dienstanbietern können elektronisch verarbeitet werden
STUFE 0	Informationssysteme für die großen diagnostischen und versorgenden Abteilungen (Labor, Radiologie, Apotheke) sind nicht installiert bzw. Daten von externen Dienstanbietern können nicht elektronisch verarbeitet werden

[2] https://www.himss.eu/himss-taxonomy-topics/electronic-health
[3] https://www.himssanalytics.org/europe/stage-6-7-achievement
[4] https://www.sueddeutsche.de/digital/patientendaten-netz-sicherheit-1.4604064

JULI 2019
DRK Trägergesellschaft Süd-West: Krankenhäuser und andere DRK-Einrichtungen in Rheinland-Pfalz und im Saarland **(Schadsoftware)**

SEPTEMBER 2019
Millionen Radiologische Bilddaten ungeschützt online angreifbar (Trojaner)[4]

OKTOBER 2019
GZO Spital Wetzikon, Zürcher Oberland, Schweiz **(Emotet)**

DEZEMBER 2019
Klinikum Fürth in Bayern **(Emotet)**

MÄRZ 2020
Universitätsklinikum Brno in Tschechien **(Emotet)**

1 DIE REGULIERUNG DER IT-SICHERHEIT IN KRANKENHÄUSERN

VERORDNUNGEN UND RICHTLINIEN

Ein Angriff auf Geräte, Anwendungen und die Infrastruktur der Gesundheitsversorgung hätte ohne Zweifel desaströse Folgen auf die medizinische Versorgung von Gesellschaften. Eine Konsequenz besteht in der Anpassung und verpflichtenden Umsetzung gesetzlicher Vorgaben an die IT-Sicherheit und den Datenschutz. Hierzu gehören die Entwicklung von Verfahren zur Verarbeitung und Speicherung personenbezogener Daten sowie die Sicherung von Netzwerken und Endpunkten, Clouds und Tools der Zusammenarbeit.

Es gilt, die Versorgung der Patienten ausfallsicher zu gewährleisten und neben dem Schutz der IT-Infrastruktur auch für Patientensicherheit und Datenschutz zu sorgen. Im Folgenden werden die für Krankenhäuser als besonders wichtig definierten gesetzlichen Anforderungen erläutert.

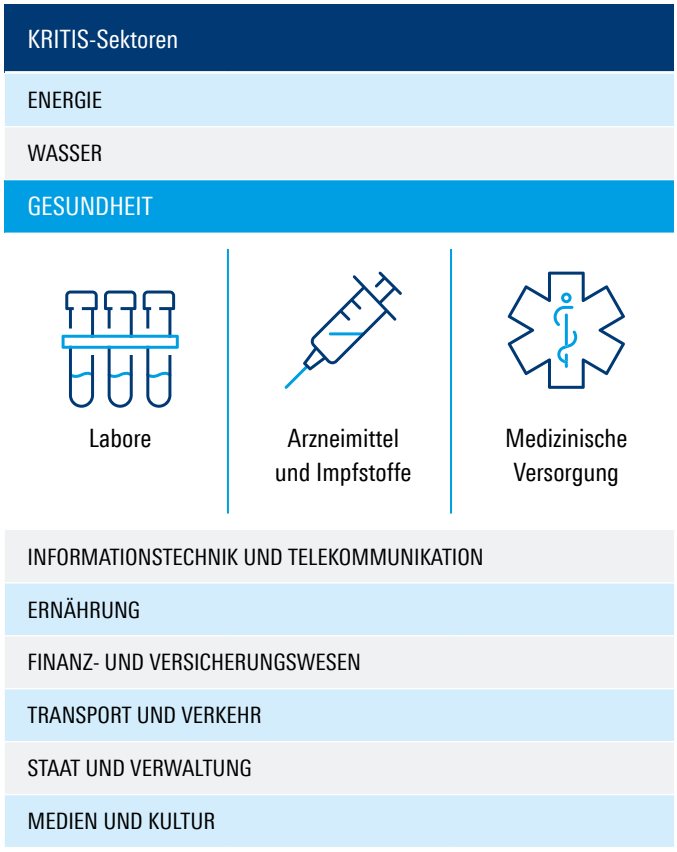
Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus (B3S)

Die Deutsche Krankenhaus Gesellschaft (DKG) legte dem Bundesamt für Sicherheit in der Informationstechnik (BSI) den Sicherheitsstandard B3S[5] Krankenhaus als Leitfaden vor, der für Krankenhäuser ab 30.000 vollstationären Patienten pro Jahr gilt. Hierin beschrieben sind technische wie organisatorische Prozesse sowie mehr als 160 Maßnahmen, die eine resiliente IT und dadurch sichergestellte Patientenversorgung gewährleisten, wie etwa ein Informationssicherheits-Managementsystem (ISMS) mit Risikomanagement oder prozessorientierte Notfallplanung im Rahmen eines Business Continuity Managements.

Der B3S dient vorwiegend dem Schutz der technischen Infrastruktur, das Erreichen der Schutzziele erhöht aber ebenso die Patientensicherheit und Behandlungseffektivität.

Die aufgeführten Handlungsempfehlungen richten sich nach BSI-Vorgaben und orientieren sich an den Anforderungen der internationalen Normen für Informationssicherheit ISO 27001 und ISO 27799. Der Standard hat Gültigkeit bis zum 16.08.2021. Das Dokument zum B3S kann auf der DKG-Website heruntergeladen werden.[6]

Abbildung 2:
Sektoren und Branchen Kritischer Infrastrukturen[7]



[5] https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Was_tun/Stand_der_Technik/B3S/B3S.html;jsessionid=756D3A0E6D47BEF4A4D194ADE2C33DDB.1_cid360?nn=6776460#doc8140926bodyText10

[6] https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/2019-04-02_B3S_KH_v1.0_-_Gesamtdokument.pdf

[7] https://www.kritis.bund.de

Laut Definition der „Nationalen Strategie zum Schutz Kritischer Infrastrukturen“ zählen laut Bund jene Einrichtungen, „deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen“ bedeutete.[8]

KRITIS | Einordnung in das Thema Krankenhaus

Der Gesetzgeber sieht eine Selbstidentifizierungspflicht vor, die besagt, dass Krankenhausbetreiber selbst entscheiden, ob sie als von dem Gesetz betroffener Bereich Gesundheit zu den lebensnotwendigen kritischen Infrastrukturen gehören. Für versorgungskritische Infrastrukturen wurden 30.000 vollstationäre Behandlungsfälle pro Jahr für Krankenhäuser festgelegt. In Deutschland sind das einige Hundert Krankenhäuser.

Patienteninformationen als personenbezogene Daten sind besonders schützenswert und der Datenschutz im Krankenhaus essenziell. Im Fokus der öffentlichen Wahrnehmung sind daher Themen wie digitale Patientenakten, wenn es um IT-Sicherheit im Krankenhaus geht. Betrachtet man Krankenhäuser aus KRITIS-Perspektive, steht Datenschutz jedoch nicht an erster Stelle, sondern vielmehr die Gewährleistung gesicherter medizinischer Versorgung.

Für Krankenhausbetreiber besteht daraus eine besondere Verpflichtung, ihren Versorgungsauftrag der Bevölkerung gegenüber sicherzustellen. Hierzu gehört Kenntnis über Abläufe – z. B. Notfallpläne – im Falle eines Ausfalls der Funktionsfähigkeit.

EU-DSGVO

Die europäische Datenschutzgrundverordnung (EU-DSGVO) ist seit mehr als zwei Jahren in Kraft und im Gesundheitssektor gelten grundsätzlich dieselben datenschutzrechtlichen Regeln wie im Datenschutzrecht. Dennoch sind die Anforderungen an medizinische Einrichtungen und Krankenhäuser in Sachen Verschwiegenheit und Datenschutz hier höher.

Die Verarbeitung personenbezogener Daten ist essenzieller Bestandteil der Arbeit in Krankenhäusern und Gesundheitseinrichtungen. Aus Sicht des Datenschutzes gehören diese nach Artikel 9 Datenschutzgrundverordnung zur besonderen Kategorie personenbezogener Daten und sind daher besonders schutzbedürftig. Dies bedeutet, dass jene Daten in der Regel nur nach Einwilligung der Betroffenen verarbeitet werden dürfen. Um ein angemessenes Schutzniveau zu gewährleisten, müssen nach Artikel 32 der EU-DSGVO (Sicherheit der Verarbeitung) „geeignete technische und organisatorische Maßnahmen“ getroffen werden.

[8] https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html

Technisch-organisatorische Auswirkungen der Digitalisierung in Krankenhäusern EU-DSGVO (Auszug):

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
- Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen
- Fähigkeit, die Verfügbarkeit der Daten und den Zugang bei physischem oder technischem Zwischenfall rasch wiederherzustellen
- Keine unbefugte Systembenutzung, sichere Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern
- Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen
- Trennungskontrolle
- Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z. B. Mandantenfähigkeit, Sandboxing
- Weitergabekontrolle
- Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z. B.: Protokollierung, Dokumentenmanagement
- Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z. B.: Backup-Strategie (online/ offline; on-site/ off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne
- Belastbarkeit = „Resilience“

Werden die Anforderungen nicht erfüllt, beträgt der Bußgeldrahmen der EU-DSGVO bis zu 20 Millionen Euro oder im Fall eines Unternehmens bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr, je nachdem, welcher Wert der höhere ist sowie 50.000 Euro für NIS-Verletzungen in Deutschland.

Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie)

Um Regulierungen im Bereich Cybersicherheit innerhalb der Europäischen Union zu harmonisieren, wurde 2016 die „Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit“ (NIS-Richtlinie) verabschiedet. Ziel ist es, technische Ausfälle und Angriffe durch ein hohes Sicherheitsniveau informationstechnischer Systeme, das den aktuellen Stand der Technik abbildet, zu begrenzen.

Alle wesentlichen Informationssysteme innerhalb des Krankenhauses müssen in einem getrennten Bereich des Informationssystems geschützt werden.

Wenn diese Anwendungen außerhalb des Krankenhauses gespeichert werden, müssen sie authentifiziert, in Bewegung befindliche Daten verschlüsselt und gespeicherte Daten ebenfalls verschlüsselt werden.

Als Betreiber sogenannter „wesentlicher Dienste“ ist das Gesundheitswesen, also Krankenhäuser wie Privatkliniken von der NIS-Richtlinie betroffen. Die bereits eingangs genannte Verordnung zur Bestimmung Kritischer Infrastrukturen (KRITIS) ergänzt hier und definiert konkretere Anwendungsbereiche. Alle wesentlichen Informationssysteme innerhalb des Krankenhauses müssen in einem getrennten Bereich des Informationssystems geschützt werden. Werden diese Anwendungen außerhalb des Krankenhauses gespeichert, müssen diese authentifiziert werden. Data in motion (bewegte Daten) wie Data at rest (ruhende Daten) müssen verschlüsselt werden.

Cloud Act

Der US-Kongress verabschiedete Anfang 2018 den Clarifying Lawful Overseas Use of Data Act (Cloud Act). Der Schutz persönlicher Daten ist in diesem „Gesetz zur Klarstellung des rechtmäßigen Umgangs mit Daten im Ausland“ als nachrangig wichtig definiert, vielmehr handelt es sich um eine Datenherausgabe an (Dritt-)Länder

– auch dann, wenn diese in Ländern außerhalb der Vereinigten Staaten von Amerika gespeichert sind.

Dies steht im Widerspruch zur EU-DSGVO, die besagt, dass personenbezogene Daten als hohes Schutzgut gelten. Um nicht dagegen zu verstoßen, sollten Krankenhäuser und alle Gesundheitseinrichtungen, die Cloud-Computing und SaaS-Dienste nutzen, auf europäische Anbieter setzen, bzw. auf Anbieter, die nicht dem Cloud Act unterliegen.

Technisch-organisatorische Auswirkungen der Digitalisierung in Krankenhäusern NIS

Krankenhausbetreiber müssen Sicherheitsmaßnahmen gemäß dem Stand der Technik umsetzen, was auch die Nutzung von Cloud-Computing-Diensten umfasst und deren Störungen mit erheblichen Auswirkungen auf die Verfügbarkeit melden. Jeweilige Sicherheitsmaßnahmen werden auf nationaler Ebene definiert.

Im Gegensatz zur regelmäßigen Prüfung der Einhaltung der NIS-Richtlinie bei KRITIS-Betreibern alle zwei Jahre gilt für Anbieter digitaler Dienste eine Überwachung Ex-post, also erst nach konkreten Hinweisen auf eine Nicht-Einhaltung der Sicherheitsanforderungen.

In Deutschland sind Notfallteams bei Störungsfällen als Mobile Incident Response Teams (MIRT) dem Bundesamt für Sicherheit in der Informationstechnik (BSI) angesiedelt. KRITIS-Betreiber müssen diese in „herausgehobenen Fällen“ um Unterstützung bei der Wiederherstellung der Sicherheit und Funktionsfähigkeit ihrer IT-Systeme anfragen. Das BSI kann von Hard- und Softwareherstellern eine Mitwirkung bei der Wiederherstellung von IT-Systemen verlangen.

Für Krankenhäuser gelten zudem der BSI IT-Grundschutz oder die ISO 27001 sowie ISO 80001. Jede Anforderung beinhaltet Maßnahmen, die umgesetzt werden müssen. Diese Anforderungen der Informationssicherheit, des Datenschutzes sowie der IT-Notfallplanung stellen Projektverantwortliche im Gesundheitsbereich vor große Herausforderungen.

2 RISIKEN FÜR DIE IT-SICHERHEIT IN EINEM KRANKENHAUS

Krankenhausbetreiber müssen Maßnahmen zur IT-Sicherheit „nach dem Stand der Technik" ergreifen, einem unbestimmten Rechtsbegriff. Zur Einordnung haben wir Ihnen eine Übersicht der IT-Sicherheitsrisiken zusammengestellt:

- Jedes vernetzte Endgerät in einem Krankenhaus wird zu einem potenziellen Einfallstor für Angreifer
- Über Jahre gewachsene Netzwerke und Systeme, bei denen IT-Sicherheit eine nachrangige Rolle spielt
- Updates von Firmware, die nicht bei laufendem Betrieb eingespielt werden können – oder die schadhaften Code enthalten
- IT-Systeme, die online angreifbar sind[9] [10]
- Fehlendes Budget, IT-Sicherheit als essenzielles Bindeglied zwischen Medizin- und IT-Technik zu implementieren
- Fehlendes Bewusstsein über den „kritischen" Kontext des eigenen Betriebs im Kliniknetz – und der Grundversorgung an sich, aber auch: unzufriedene Mitarbeiter
- Sowie aus den Top 10 Health Technology Hazards for 2018[11]
  - Ransomware
  - Verpasste Sicherheitsalarme durch fehlerhaft konfigurierte sekundäre Benachrichtigungsgeräte und -systeme

Abbildung 3:
Betroffene Webanwendungen aus dem Gesundheitssektor

CLOUD-WEBSITES UND APPS	WEBMAIL UND KOLLABORATIVE ANWENDUNGEN	GESCHÄFTS-ANWENDUNGEN	WEBDIENSTE UND API
			
Terminplanung Treffen Voraufnahmen Bilder Testergebnisse	Nachrichtenübermittlung SharePoint™	Verzeichnisse Bilder Biologie Pathologie elektronische Patientenakte (ePA)	mobile Apps regionaler ePA-Feed Gesundheits-Hoster medizinisch-technische Systeme

[9] https://www.heise.de/security/meldung/Tausende-medizinische-Geraete-aus-dem-Internet-angreifbar-2831620.html
[10] https://www.golem.de/news/it-sicherheit-lebenswichtige-medizinische-geraete-ungeschuetzt-im-internet-1509-116563.html
[11] https://www.ecri.org/Resources/Whitepapers_and_reports/Haz_18.pdf

Der Krankenhausstudie von Roland Berger (2017) zufolge sind 64 % der deutschen Krankenhäuser bereits Opfer eines Hacker-angriffs geworden. Dies umfasst sowohl aktive „Angriffe" durch das Internet als auch durch unachtsame Nutzung eingeschleuster Viren / Trojaner.[12]

Anwendungsschutz im Gesundheitswesen

IT-Sicherheitslücken in Anwendungen aus dem Gesundheitssektor können verheerende Folgen haben. Je mehr Anwendungen zum Einsatz kommen, desto höher die potenzielle Bedrohung jener, die über das Web angesteuert werden und so von außen angreifbar sind.

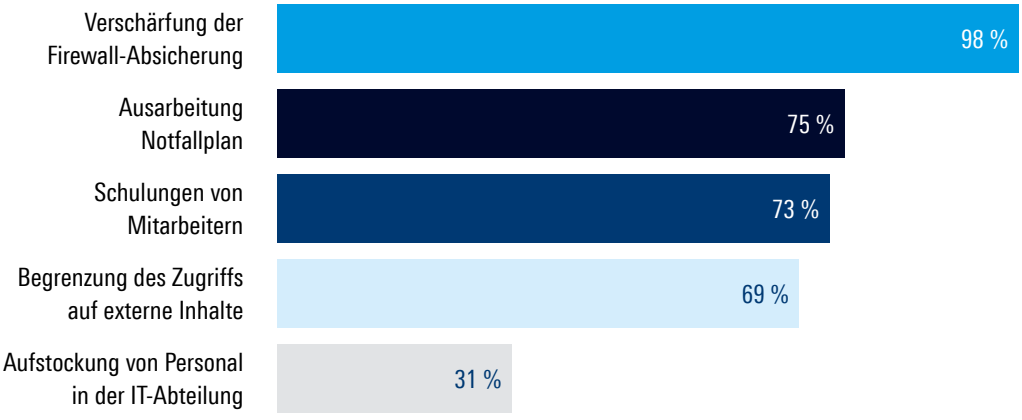


Abbildung 4:

Ergriffene Maßnahmen deutscher Krankenhäuser, um sich vor unberechtigtem Datenzugriff zu schützen[13]

[12] https://www.rolandberger.com/publications/publication_pdf/roland_berger_krankenhausstudie_2017.pdf
[13] https://www.rolandberger.com/publications/publication_pdf/roland_berger_krankenhausstudie_2017.pdf

TYPISCHE SCHWACHSTELLEN

#1 BETRIEBSSYSTEMBEFEHLE

Befehle auf dem Host-Betriebssystem werden über eine anfällige Webanwendung ausgeführt

#2 BYOD (BRING-YOUR-OWN-DEVICE)

BYOD ohne Richtlinien bildet ein Zusatzrisiko

#3 CROSS-SITE SCRIPTING

Angreifer fügen ein schadhaftes Skript in eine anfällige Webanwendung ein, das anderen Benutzern angezeigt wird. Dieses Skript kann Nutzer zu anderen Websites umleiten oder auch Anmeldeinformationen stehlen

#4 CYBERSPIONAGE

Das Interesse konkurrierender Interessengruppen an klinischen Forschungsergebnissen und/ oder Patientendaten

#5 DISTRIBUTED DENIAL OF SERVICE (DDOS)-ANGRIFFE

Autorisierten Usern wird der Zugriff zum Dienst verweigert. DDoS-Angriffe versuchen, Ressourcen wie Server, auf denen Webanwendungen oder Websites gehostet werden, zu verlangsamen oder sogar zum Absturz zu bringen. DDoS-Angriffe werden mitunter als Ablenkung für eigentliche Angriffe auf Netzwerke eingesetzt – die weitaus schädlicher ausfallen können

#6 DIEBSTAHL VON DATEN UND ENDGERÄTEN

Medizinische Geräte haben sehr hohe Anschaffungskosten, Diebstahl ist weit verbreitet. Kleine bis mittelgroße tragbare Geräte wie Ultraschallgeräte, EKG, Defibrillatoren, Infusionspumpen oder Vitalparameter-Monitore sollten idealerweise keine medizinischen Daten speichern

#7 DIRECTORY TRAVERSAL (PATH TRAVERSAL ODER AUCH FORCEFUL BROWSING)

Diese „Überquerung“ (Deutsch von: Traversal) erfolgt, wenn ein Angreifer, mittels manipulierter Pfadangaben, eine HTTP-Anfrage stellt, um zu nicht autorisierten übergeordneten Verzeichnissen zu gelangen und den Inhalt vertraulicher Dateien anzuzeigen

#8 HIJACKING (CRYPTOJACKING & MEDJACKING)

Beim Cryptojacking verwenden Angreifer Computer, Smartphones, Tablets oder sogar Server ohne die Zustimmung oder das Wissen der Benutzer, um Kryptowährung auf Kosten des Opfers zu „schürfen“. Unterschied Cryptojacking & Medjacking: universelle IT-Infrastruktur vs. IT-basierte medizinische Geräte

#9 IDENTITÄTSDIEBSTAHL

Die Identität der Mitarbeitenden oder die der Patienten kann gestohlen werden. Die Annahme einer Identität eines Arztes oder einer Krankenschwester ermöglicht z. B., gefälschte Rezepte auszustellen oder birgt die Gefahr von Fehldiagnosen. Im zweiten Fall könnte Sozialbetrug geschehen oder falsche Diagnosen „provoziert“ werden

#10 INFORMATIONSLECKS

Diese Angriffe zielen auf vertrauliche Informationen ab, die vom System angezeigt werden, wie etwa Fehlermeldungen und Kommentare im HTML-Code

#11 INSIDER-ANGRIFFE

Ärzte, Krankenschwestern, Verwaltung, Wartung, das gesamte Krankenhauspersonal kann als Insider Informationen weitergeben, aber auch Patienten oder Besucher, da ein Krankenhaus 24/7 geöffnet ist, Zugang kann nicht vollumfassend kontrolliert werden

#12 IT-SYSTEME

In Krankenhäusern sind IT-Systeme stark miteinander vernetzt & nur schwer zu trennen, ohne Funktionen zu stören

#13 LOCAL FILE INCLUSION (LFI)

Angreifer verschaffen sich Zugang zu fremden Servern. Angreifer stellen eine HTTP-Anfrage, um auf nicht autorisierte Dateien zuzugreifen. Anstatt den Inhalt der Datei anzuzeigen, wird schadhafter Code auf dem Zielsystem ausgeführt

#14 RANSOMWARE

Infiziert Gesundheitsinfrastrukturen
1) Softwareinfrastruktur ist schwer auf dem neuesten Stand zu halten/ Ausfallzeit-Slot erhalten
2) Computer, auf denen Legacy-Software ausgeführt wird, die nur unter speziellen Betriebssystemen/ Treiberversionen funktioniert, sind leichtes Angriffsziel.
Veraltete Geräte, die kaum aktualisiert werden können, funktionieren wie ein Reservoir für Malware, die im Netzwerk verteilt wird

#15 SOCIAL ENGINEERING (PHISHING)

Kompromittierte E-Mails (Phishing, Spam und Spear-Phishing) sind ein Hauptangriffsvektor für Malware-Infektionen. Viele Gesundheitseinrichtungen erlauben den Zugriff auf private E-Mail-Webkonten auf Krankenhausrechnern.
E-Mail-Adressen von Ärzten können einfach über öffentliche Verzeichnisse von Krankenhäusern und vorhandene Präsentationen in Erfahrung gebracht werden. Hinzu kommt die Verwendung beruflicher E-Mail-Konten für persönliche Angelegenheiten sowie die Verwendung persönlicher E-Mail-Konten für berufliche Angelegenheiten

#16 SQL-INJECTION

SQL ist eine Programmiersprache zur Kommunikation mit Datenbanken zum Abfragen oder Ändern von Daten und findet daher häufig Verwendung in Webanwendungen. Angriff äußert sich durch SQL-Eingaben in Textfeldern, zum Beispiel in einem Online-Formular. Ziel ist es, Daten abzugreifen oder Daten zu manipulieren

#17 WEBBASIERTE ANGRIFFE

Aktualisierungen, bei denen versucht wird, Systemkonfiguration beizubehalten, um Ausfallzeiten zu reduzieren, erleichtern Angreifern das Ausnutzen von Schwachstellen

#18 XML-INJECTION

Ähnlich wie bei SQL-Angriffen manipuliert die XML-Injection eine Webanwendung, indem sie schadhaften XML-Code anstelle legitimer Formulardaten einfügt

Folgen:

- **Reputationsschäden durch nicht/ gestört verfügbare Systeme**
- **Umsatzeinbußen und Versorgungs-engpässe durch Ausfallzeiten kritischer Services**

3 ROHDE&SCHWARZ CYBERSECURITY-LÖSUNGEN

Betreibern von Gesundheitseinrichtungen, insbesondere Krankenhäusern, ist die Wichtigkeit eines funktionierenden Cyberabwehrsystems für medizinische Geräte bewusst, dennoch geht es mit der operationalen Realisierung nicht so schnell voran wie gewünscht.

Durch eine Stärkung ihrer IT-Sicherheitspolitik können Gesundheitseinrichtungen jedoch Konformität mit behördlichen Auflagen nachweisen und steigende Erwartungen von Dienstleistern sowie ihrer Patienten gleichermaßen erfüllen.

Die Lösungen von Rohde&Schwarz Cybersecurity ermöglichen, alle Aspekte der Anwendungssicherheit, des Zugangs zu Gesundheitsapplikationen und des Schutzes gesundheitsbezogener Daten abzudecken.

Sie gewährleisten eine einfache Integration ohne Auswirkungen auf die Produktivität bestehender Systeme. Rohde&Schwarz Cybersecurity garantiert mit Lösungen aus einer Hand die Umsetzung nationaler und europäischer gesetzlicher Vorgaben.

Rohde&Schwarz Cybersecurity kann Krankenhäuser in vier Bereichen in Bezug auf die oben genannten Bedrohungen konkret unterstützen.


DR. T. J
GENERAL PRACTITIONER

APPLICATION SECURITY: R&S®WEB APPLICATION FIREWALL

Spielt eine Schlüsselrolle bei der Erstellung und Implementierung einer Applikationssicherheitsstrategie im Gesundheitssektor. Sie schützt kritische Webanwendungen (Legacy-Anwendungen), Webdienste (Microsoft® Outlook Web Access™, Exchange™, SharePoint™, SAP) und API vor bekannten und unbekannten Angriffen, darunter die OWASP Top 10. Zertifiziert von der französischen Cybersicherheitsbehörde ANSSI.

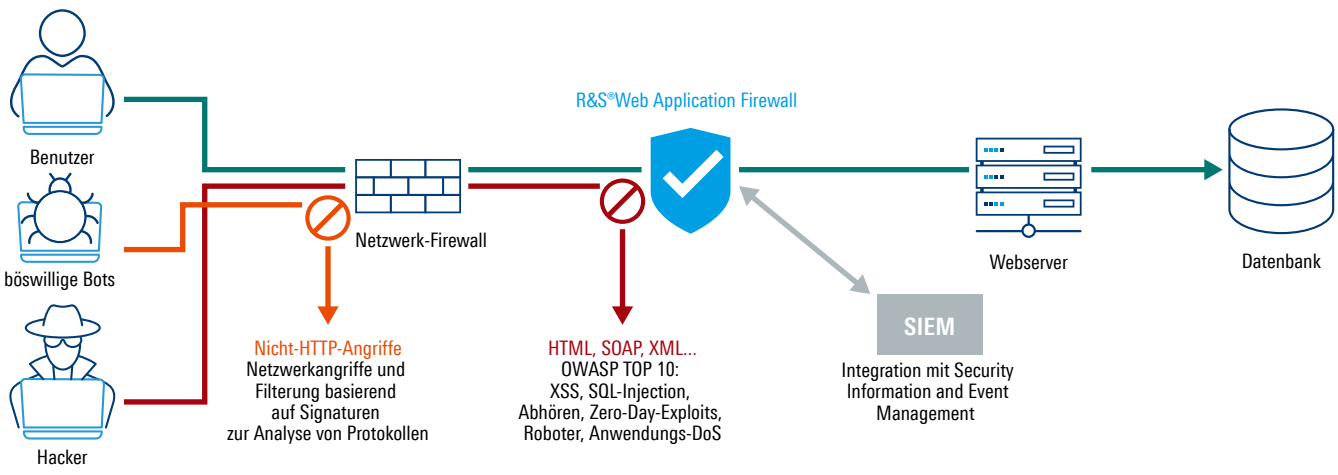
Ihr „Pooling-Mode“ ermöglicht es, kritische Krankenhausdienste und -systeme in einem abgeschotteten Bereich mit erhöhter Sicherheit zu betreiben (NIS-konform). Die Lösung ist komplett skalierbar, kann vor Ort oder in der Cloud implementiert werden, sorgt dafür, dass gesundheitsbezogene Daten nach hohen Vertraulichkeits- und Integritätsstandards gespeichert werden und die Absicherung von Webanwendungen sowie des API-Austauschs gewährleistet bleibt.

Abbildung 5:

Effektive Sicherheit gegen eine Vielzahl von Angriffen, einschließlich automatisierter Angriffe (Bots)

VORTEIL:

- Schutz der Protokollschicht 7
- Technologieunabhängig; ermöglicht die Nutzung von Multi-Cloud oder hybriden Cloud-Deployments
- Erweiterte API-Sicherheit ermöglicht es, die Vorteile agiler, API-gestützter Entwicklung zu nutzen und parallel sicher und compliant zu bleiben
- Schutz gegen OWASP Top 10



NETWORK SECURITY: R&S®SITLINE ETH

Schützt sensible Daten im Gesundheitsbereich vor Spionage und Manipulation. Die Layer 2-Verschlüsselung nach modernsten Methoden und Standards erlaubt es, Kommunikation und Daten per Ethernet über Festnetzleitungen, Richtfunk und Satellitenverbindungen abzusichern. Der Verschlüsseler reduziert die Betriebskosten signifikant und sorgt gleichzeitig für ein erhöhtes Sicherheitsniveau.

Ideal zu Telediagnosezwecken (Echtzeitanwendung) oder als Alternative zur Datenverschlüsselung beim Austausch zwischen verschiedenen Krankenhausstandorten.

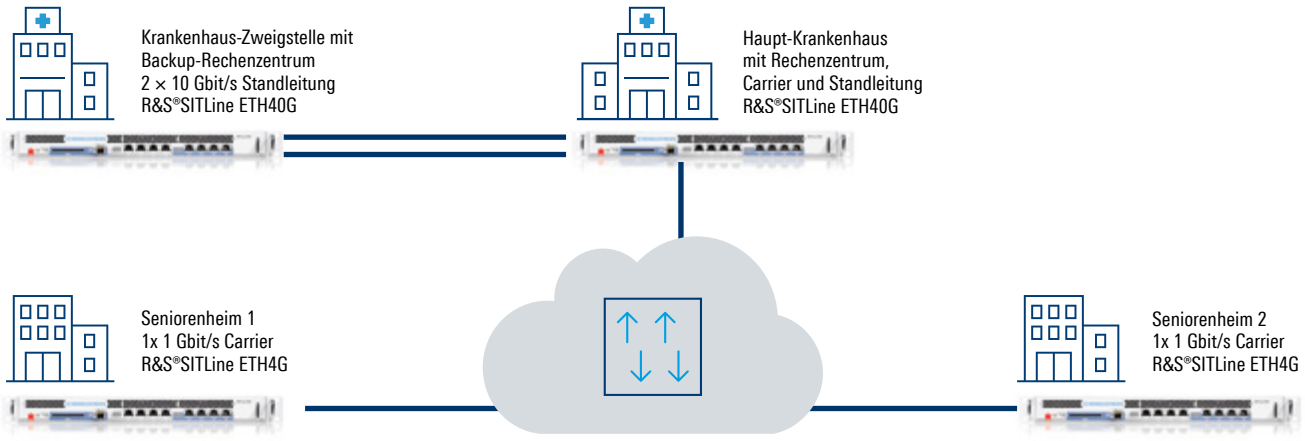
Die Geräte sind vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen bis VS-NfD, NATO-Restricted und EU-Restricted.

VORTEIL:

- Hochgeschwindigkeits-Verschlüsselung auf Layer 2
- Hochmoderne kryptografische Verfahren und Standards
- Zentrales Netzwerkmanagement und -monitoring
- Geringer Energieverbrauch und niedrige Systemkosten

Abbildung 6:

Vorkonfigurierte Verschlüsselung für Standleitungen, die beim Start automatisch verschlüsselte L2-Verbindungen über Fast Ethernet herstellt



CLOUD SECURITY: R&S®TRUSTED GATE

Garantiert die Sicherheit und den Schutz der Daten in öffentlichen Clouds und Kollaborationstools. Viele Gesundheitseinrichtungen haben sich für Microsoft® Office 365™ entschieden, um die Vorteile der Cloud zu nutzen.

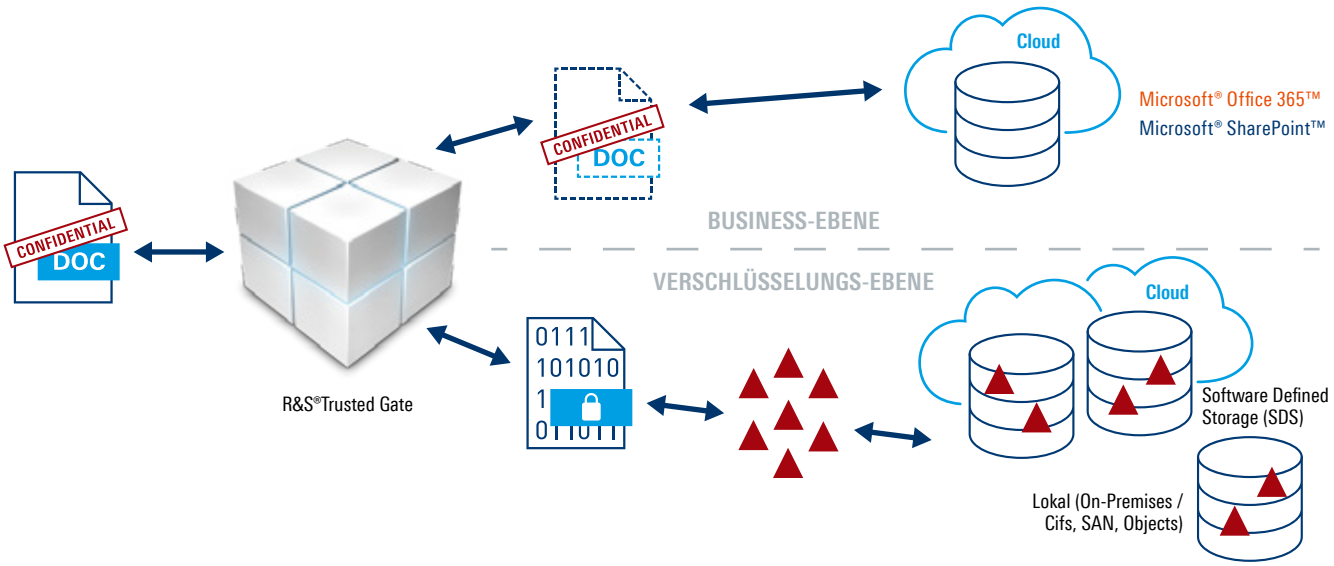
Dank dynamischer Verschlüsselungstechnologien und Virtualisierung entspricht die Lösung den höchsten Sicherheitsstandards für den Schutz gesundheitsbezogener Daten und kann in Krankenhäusern und anderen Gesundheitseinrichtungen gemäß geltender Datenschutzregelungen und ohne Einbußen bei Performance (sichere Volltextsuche) und Flexibilität genutzt werden.

Die Verschlüsselungsmechanismen von R&S®Trusted Gate werden nahtlos in Office 365™-Lösungen eingebunden. Mitarbeitende im Gesundheitsbereich verwenden ihre Apps in Office 365™ wie gewohnt.

Abbildung 7:
Sichere Zusammenarbeit in der Cloud – Originaldaten landen verschlüsselt und fragmentiert im konfigurierbaren Speichersystem

VORTEIL:

- Einhaltung von Datenschutzanforderungen bei der Arbeit in der Public Cloud
- Effektives und sicheres Arbeiten in Cloud-Anwendungen
- Lösungen für Public Clouds und Collaboration-Tools
- Optimierung der Infrastruktur durch virtuelle Spiegelung On-Premises oder Multi-Cloud



DESKTOP SECURITY: R&S®BROWSER IN THE BOX

Stellt eine virtuelle Umgebung zum sicheren Surfen im Web bereit. Internetbrowser gehören zu einer der größten Schwachstellen von Endpunkten und Netzwerken innerhalb von Gesundheitseinrichtungen. Schadsoftware kann über E-Mails, Anwendungen und Tools zur Zusammenarbeit, mit denen Mitarbeiter ihren Arbeitsalltag organisieren, ins Krankenhaus geschleust werden – was nicht nur für die Datensicherheit fatale Folgen haben kann.

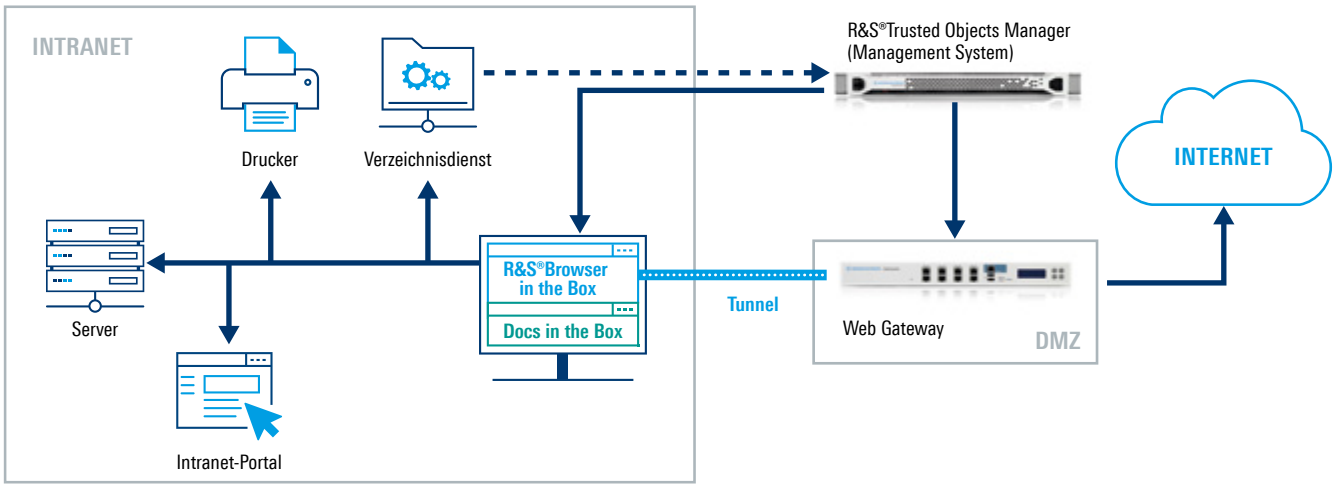
R&S®Browser in the Box sichert Krankenhaussysteme vor Datenabfluss durch Telemetriedaten in Microsoft® Office™ und Windows 10™ ab und das Feature Docs in the Box ermöglicht mittels Viewer-Funktion, alle Anhänge gängiger Office-Anwendungen und Applikationen mit Internet-Zugriff wie Skype in einer geschützten virtualisierten Umgebung zu prüfen.

VORTEIL:

- „Der sicherste Browser der Welt“
- Hohe Sicherheit durch Virtualisierung und Trennung von Internet und Intranet
- Granulare Rechtevergabe & spezifizierte Nutzereinstellungen wie barrierefreies Browsen
- Proaktive Blockierung aller Telemetriedienste

Abbildung 8:

Netzwerktrennung bietet „ geschützten Raum“, in dem Schadsoftware nicht auf lokale Rechner/ in Unternehmensnetzwerke gelangt



4 AUS DER PRAXIS: IT-SICHERHEITSSTRATEGIEN IM EINSATZ

Webanwendungen erfordern Sicherheit auf mehreren Ebenen. Insbesondere in Krankenhäusern, bei der Arbeit mit Gesundheitssystemen geht es darum, wichtige Bestandteile von Webanwendungen zu isolieren und einzeln zu sichern.

So kann gewährleistet werden, dass einzelne Protokolle, Server, Datenbanken und Dienste sicher arbeiten.

Nachfolgend stellen wir Ihnen ausgewählte Praxisbeispiele und Tipps unserer Kunden vor:

– Verschaffen Sie sich einen Überblick sämtlicher im Einsatz befindlicher Webanwendungen

– Erstellen Sie Sicherheitsrichtlinien und führen Sie interne Audits durch

– Verschlüsseln Sie diesen Datenverkehr

KUNDE

- Ein Klinikverbund mit 4 Krankenhäusern und 3.400 Betten
- Beschäftigt sind mehr als 12.000 Personen des medizinischen und nichtmedizinischen Personals sowie 2.000 Ärzte
- 125.000 stationäre Aufnahmen, 900.000 Konsultationen und 200.000 Notfälle pro Jahr

HERAUSFORDERUNG

- Ermittlung des Sicherheitsniveaus der wichtigsten Geschäftsanwendungen
- Identifizierung potenzieller Sicherheitslücken der IT-Infrastruktur, die durch diese Anwendungen unterstützt werden
- Dabei: Einhaltung der EU-DSGVO und Rahmenbedingungen für Qualität und Wirtschaftlichkeit in der gesundheitlichen und pflegerischen Versorgung
- SSL-Verschlüsselung von mobilen Anwendungen (Apps)

LÖSUNG

- R&S®Web Application Firewall
- 4.000 IP-Adressen & 100 Anwendungen
- Compliance und Sicherstellung der Datenintegrität

KUNDE

- Lokales Krankenhaus-Gesundheitsunternehmen
- Über 4.000 Mitarbeiter

HERAUSFORDERUNG

- Sichern kritischer Webanwendungen gegen OSWAP Top 10-Angriffe
- Absicherung intern entwickelter Anwendung zur Bedarfsplanung und Bestellung von Mahlzeiten aus der Krankenhauskantine. Die Anwendung wechselte vom Intranet ins Internet
- E-Learning-Anwendung sichern

LÖSUNG

- R&S®Web Application Firewall
- (mittels) Virtual Machine Ware mit 20 Anwendungen und Web Access Manager-Modul

KUNDE

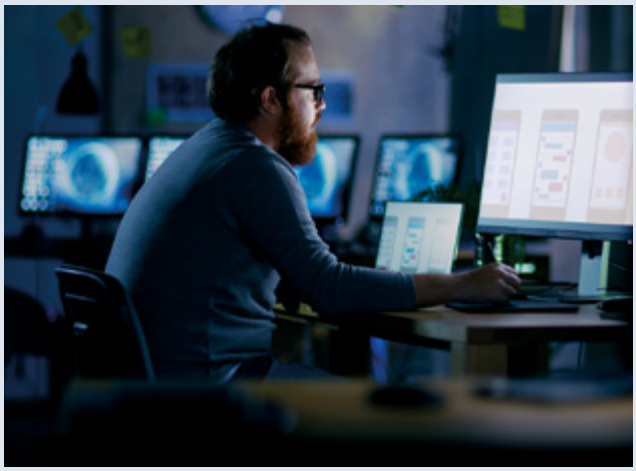
- Über 2.500 medizinische und nichtmedizinische Vertreter
- 845 Betten und Plätze
- 148.437 volle Krankenhaustage

HERAUSFORDERUNG

- Sichere Kommunikation zwischen dem Rechenzentrum und den CHPG-EHPADs
- Betreiber Monaco Telecom mit Einschränkungen im Zusammenhang mit dem MPLS-Netzwerk und der von Orange betriebenen Glasfaser
- Technische Herausforderung: mehrere VRF, Multicast-Routing

LÖSUNG

- R&S®SITLine ETH
- Einsatz von 4 Ethernet-Verschlüsselern in Glasfaser- und MPLS-Netzwerken
- Garantierte Sicherheit für die Kommunikation zwischen EHPAD-Standorten



KUNDE

- Öffentliches Krankenhaus
- 845 Betten
- Mehr als 2.500 Mitarbeiter

HERAUSFORDERUNG

- Sichere Kommunikation zwischen dem Rechenzentrum und den an das Krankenhaus angeschlossenen Pflegeheimen
- Telekommunikationsbetreiber mit Einschränkungen im Zusammenhang mit dem MPLS-Netzwerk und der Glasfaser-Verbindung
- Technische Herausforderung: mehrere VRF, Multicast-Routing

LÖSUNG

- R&S®SITLine ETH
- Einsatz von 4 Ethernet-Verschlüsselern in Glasfaser- und MPLS-Netzwerken
- Garantierte Sicherheit für die Kommunikation zwischen EHPAD-Standorten

KUNDE

- Gesundheitsamt einer Landeshauptstadt

HERAUSFORDERUNG

- Internetrecherche ist Arbeitsbestandteil
- Getrennte Verarbeitung personenbezogener Daten und Gesundheitsdaten erforderlich
- Fachverfahren mit speziellen Sicherheitsanforderungen erfordern Datentrennung

LÖSUNG

- R&S®Browser in the Box
- Mehrstufige Kapselung erfüllt gesetzliche Sicherheitsanforderungen

FAZIT

Im Februar 2020 veröffentlichte die ENISA (European Union Agency for Cybersecurity) sogenannte „Beschaffungsrichtlinien für Cybersicherheit in Krankenhäusern“ (Original: PROCUREMENT GUIDELINES FOR CYBER-SECURITY IN HOSPITALS)[14], da der Einkauf von Dienstleistungen, Produkten sowie der gesamten Infrastruktur natürlich ein Schlüsselprozess innerhalb des IKT-Umfeldes von Gesundheitseinrichtungen und besonders Krankenhäusern ist. Hier beginnt holistische Cybersecurity.

Eine zuverlässige IT-Infrastruktur ist erforderlich, um Gesundheitseinrichtungen wie Krankenhäuser gegen Manipulierung oder Sabotage zu schützen, denn ein breit angelegter Angriff auf medizinische Infrastrukturen hätte ohne Zweifel desaströse Folgen für die Versorgung der Bevölkerung.

Die Einhaltung steigender regulatorischer Anforderungen an die IT-Sicherheit und den Datenschutz gilt es ebenso zu sichern, wie die grundsätzliche Verfügbarkeit von technischen Systemen und Daten der Gesundheitsversorgung.

Proaktive, zukunftsfähige Lösungen auf dem neuesten Stand der Technik sind die Grundvoraussetzung für funktionierende Gesundheitsdienstleistungen und um sicheres, vernetztes Arbeiten in einem Krankenhausbetrieb zu gewährleisten.

Rohde&Schwarz Cybersecurity unterstützt das Gesundheitswesen mit Sicherheitsstrategien, die auf die jeweilige medizinische Einrichtung angepasst sind.

INTEGRITÄT SCHAFFT KONFORMITÄT

- Stellen Sie sicher, dass Daten (Dateien) mit einer vertrauenswürdigen Lösung in der Cloud verschlüsselt werden
- Auf diese Weise kann das Krankenhaus EU-DSGVO-Richtlinien einhalten und Verstöße vermeiden
- Machen Sie die IT-Sicherheit für Anwender transparent – dies ist der Schlüssel zur Akzeptanz
- Sorgen Sie für leichten Umgang mit regulierten und unregulierten Daten

[14] https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services)

Service mit Mehrwert

- Weltweit
- Lokal und persönlich
- Flexibel und maßgeschneidert
- Kompromisslose Qualität
- Langfristige Sicherheit

Rohde&Schwarz Cybersecurity

Das IT-Sicherheitsunternehmen Rohde&Schwarz Cybersecurity schützt digitale Informationen und Geschäftsprozesse von Unternehmen und öffentlichen Institutionen weltweit vor Cyberangriffen. Der IT-Sicherheitsexperte bietet innovative Datensicherheitslösungen für Cloud-Umgebungen, erweiterte Sicherheit für Websites, Webanwendungen und Webservices sowie Netzwerkverschlüsselung, Desktop- und Mobile-Security. Die vertrauenswürdigen Sicherheitslösungen werden nach dem Security-by-Design-Ansatz entwickelt und verhindern Cyberangriffe proaktiv.

Rohde&Schwarz

Rohde&Schwarz ist ein führender Lösungsanbieter in den Geschäftsfeldern Messtechnik, Broadcast- und Medientechnik, Aerospace | Verteidigung | Sicherheit sowie Netzwerke und Cybersicherheit. Mit seinen innovativen Produkten der Kommunikations-, Informations- und Sicherheitstechnik unterstützt der Technologiekonzern professionelle Anwender aus Wirtschaft und hoheitlichem Sektor beim Aufbau einer sicheren und vernetzten Welt. Der Firmensitz ist München. Das internationale Geschäft wird in mehr als 70 Ländern über Tochterfirmen betrieben. In Asien und Amerika steuern regionale Hubs die Geschäfte.

Rohde&Schwarz Cybersecurity GmbH
Mühldorfstraße 15 | 81671 München
Info: +49 30 65884-222
Email: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

Rohde&Schwarz GmbH & Co. KG
www.rohde-schwarz.com

PD 3608.4997.61 | Version 01.01 | April 2020 (sch)
IT-Sicherheit im Gesundheitswesen

3608499761
3608.4997.61 01.01 PDP 1 de