BUSINESS CONTINUITY FÜR DIE DIAGNOSTIK

Hohe Cyberbedrohungslage für Krankenhäuser

Die allgemeine Cyberbedrohungslage in Deutschland wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als hoch bewertet („Lage der IT-Sicherheit in Deutschland 2023“). Das Ziel der Angriffe sind dabei die Grundwerte der IT-Sicherheit: Vertraulichkeit, Integrität und Verfügbarkeit. Cyberattacken auf Krankenhäuser zielen meist darauf ab, Patientendaten zu verschlüsseln und die Betriebsfähigkeit der Einrichtung zu stören.

Hohe Kosten durch Ransomware-Angriffe
Die Wiederherstellung illegal verschlüsselter Daten dauert oft Monate und ist teuer. So beziffert z.B. das Lukaskrankenhaus Neuss in einem Interview mit der Computerwoche die Kosten in Folge einer Ransomware-Attacke auf eine Million Euro. Notfälle konnten 36 Stunden nicht aufgenommen werden; insgesamt dauerte der Blackout fünf Tage.

Der IT-bedingte Ausfall von Behandlungen führt zu fehlenden Einnahmen. Gleichzeitig laufen die fixen Kosten weiter und Zusatzkosten für die Aufarbeitung der Attacke fallen an. Damit entstehen schnell hohe finanzielle Schäden.

Bilddaten sind besonders gefährdet
Medizinische Bilddaten machen 80 bis 90 Prozent am Datenvolumen eines Krankenhauses aus. Je nach Anzahl an Untersuchungen kommen pro Woche schnell über 100 GB an Bilddaten zusammen.

Gleichzeitig sind Bilddaten essentiell für die Diagnostik, einem der fünf relevanten Prozesschritte der kritischen Dienstleistung (kDL) in der medizinischen Versorgung. In der Notaufnahme geht ohne bildgebende Verfahren quasi nichts.

Notfallkonzepte für Bilddaten unzureichend
Auch wenn gesetzlich vorgegebene, organisatorische und technische Maßnahmen die Business Continuity von Gesundheitseinrichtungen addressieren, exisiteren in der Praxis oft keine oder nur unzureichende Notfallkonzepte für die Bilddaten.

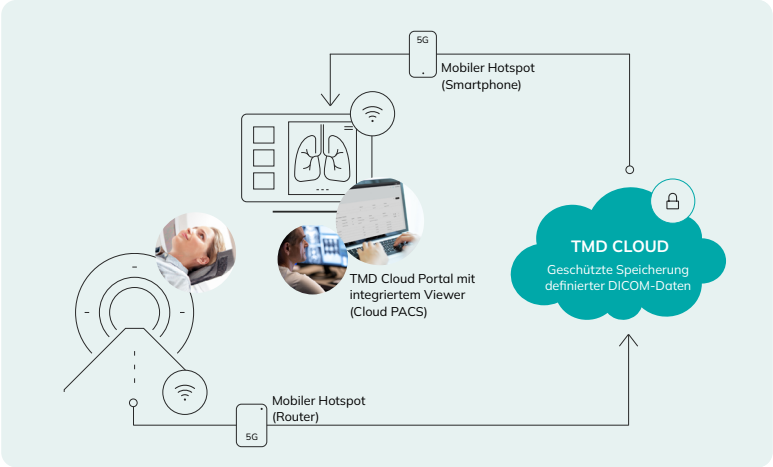
So können lokale Daten-Backups während eines Cyberangriffs meist nicht abgerufen werden, da die notwendigen Software-Tools (z.B. PACS, KIS) offline sind. Selbst die Wiederherstellung eines Notbetriebs dauert daher Tage. Cloud-Lösungen wie die TMD Cloud können hier Abhilfe schaffen.

Bilddaten im Notfall sofort abrufbar

Greifen Sie mit der TMD Cloud einfach auf DICOM-Daten zu - auch bei Cyberattacken.

Durch ein parallel zum Regelbetrieb stattfindendes Bilddaten-Backup in der TMD Cloud erhalten Sie im Falle eines Cyberangriffs in wenigen Minuten Zugriff auf die gespeicherten Daten - unabhängig von der übrigen IT-Infrastruktur, anderen Applikationen oder dem internen Netzwerk. Dadurch können Sie einen Notbetrieb schneller herstellen und die Business Continuity unterstützen.

Notfallzugriff auf DICOM-Daten in wenigen Minuten

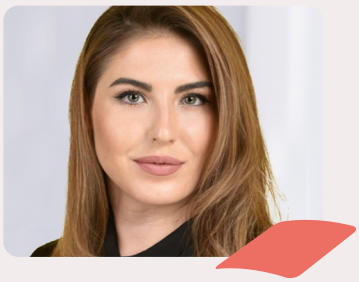


Dank der TMD Cloud können Sie im Falle einer Cyberattacke mit einem vom Netzwerk unabhängigen Endgerät und einem mobilen Internetzugang schnell auf gespeicherte Bilddaten zugreifen sowie neue Bilddaten in der TMD Cloud hinterlegen. Damit sind Sie in der Lage, einzelne Modalitäten kurzfristig live zu nehmen und Ihre Business Continuity zu verbessern.

Unser Angebot für Sie

- **Cloud-Backup:** Cloud-basierte Speicherung von DICOM-Daten in der TMD Cloud bis zu einem definierten Volumen.
- **Integriertes Nutzerportal:** Datenzugriff auf Ihre Bilddaten über das anwenderfreundliche TMD Cloud Portal.
- **Integrierter Web-Viewer:** Betrachtung und Befundung von DICOM-Bildern aus dem Browser über zertifizierten Viewer.
- **User- & Identity Management:** Individuelles Rechte- und Zugriffsmanagement über das TMD Cloud Portal.
- **Planungssicherheit:** Kalkulierbare Kosten in Abhängigkeit von der Datenmenge und benötigten Notfall-Nutzern.

Termin vereinbaren



Adina Zusek

azusek@telepaxx.de
+49 (0)173 26 40 231
Sprechen Sie mich an!