



Kapsch BusinessCom

## **Krankenhaus Spittal an der Drau.** *Success Story.*

Krankenhäuser sind hochsensible Orte. Es geht um vertrauliche Daten von Patient:innen, wirksam abgesicherte Prozesse und generell um die Zukunftssicherheit von IT und Netzwerken. Auch das Netz- und Informationssystemsicherheitsgesetz (NISG) stellt hier klare Anforderungen. Im Krankenhaus Spittal an der Drau wartet man nicht, bis man selbst „IT-Patient“ und anfällig für Netzwerkangriffe wird, sondern geht auf Nummer sicher. Mit Kapsch BusinessCom als Partner für Cyber Security. Eine mehr als gesunde Entscheidung.

# Diagnose: NISG. Therapie: Cyber Security von KBC.

In Spitälern können Störungen und Ausfälle in der Netzwerkkommunikation oder bei Datenbanken massive Probleme zur Folge haben und die medizinische Versorgung gefährden. Das Netz- und Informationssystemsicherheitsgesetz (NISG) spricht in diesem Zusammenhang eine klare Sprache: Umfangreiche Maßnahmen zum Schutz der wesentlichen Dienste müssen zu jeder Zeit gegeben sein.

## Das A. ö. Krankenhaus Spittal an der Drau: wohnortnahe Versorgung auf höchstem Niveau.

Das KH Spittal/Drau steht seit knapp 100 Jahren im Dienste der medizinischen Versorgung Oberkärntens. Form und Inhalt gehen hier Hand in Hand, so kann das Haus seine Funktion als regionales Kompetenzzentrum für Gesundheit optimal erfüllen.

Mit modernsten diagnostischen und therapeutischen Methoden und Einrichtungen, engagierten Mitarbeiter:innen und dem Blick für die Bedürfnisse der Patient:innen. Besonderes Anliegen: die wohnortnahe medizinische Versorgung – stationär und ambulant.



## Ausgangssituation.

Gemeinsam mit den IT-Verantwortlichen im KH Spittal/Drau hat Kapsch BusinessCom (KBC) eine genaue Problem- und Bedarfsanalyse durchgeführt. Man stellte rasch fest, dass ein krankenhausinterner Kompetenzaufbau rund um die IT-Sicherheit nur schwer möglich ist. Folgende Notwendigkeiten ergaben sich:

- Umstellung von reaktiver auf proaktive Sicherheitsstrategie
- Externe Unterstützung in besonderen IT-Stresssituationen
- Rasche professionelle Hilfestellung durch persönlichen Kontakt vor Ort

## Nutzen und Vorteile:

- Mehr Sicherheit dank einer maßgeschneiderten „Endpoint Detection & Response“-Lösung
- Kontinuierliche proaktive Überwachung
- Höhere Visibilität in der IT-Infrastruktur: Logdatenanalyse und Auswertung durch Expert:innen
- Schnelle und zuverlässige Erkennung sicherheitsrelevanter Vorfälle, sofortige persönliche Kontaktaufnahme mit IT-Verantwortlichen im KH Spittal/Drau
- Laufende Dokumentation und Abstimmung alarm-spezifischer Maßnahmen

## Ein Fall für KBC und sein CDC.

Mit dem Cyber Defense Center (CDC) verfügt Kapsch BusinessCom, Österreichs führendes Digitalisierungsunternehmen, über ein eigenes schlagkräftiges Kompetenzzentrum für Cyber-Sicherheit. Für das KH Spittal/Drau wurde ein Frühwarnsystem rund um die IT-Security etabliert:

ein flächendeckender Roll-out der Endpoint Protection auf 600 Clients durch die Krankenhaus-IT mit von KBC etablierter SCCM-Infrastruktur. Das Onboarding der Clients in die Cyber-Security-Plattform konnte rasch umgesetzt werden.

## Darum vertraut man im Krankenhaus Spittal a. d. Drau auf Kapsch BusinessCom.

„KBC hat sich als professioneller, kompetenter, zuverlässiger Partner erwiesen. Die Präsenz der KBC vor Ort in Kärnten war uns sehr wichtig für den persönlichen Kontakt. Das Cyber Defense Center hilft uns bei der Früherkennung relevanter Vorfälle und wir können sehr rasch reagieren.“

**Herbert Wutti, MBA, MSc.**

IT-Leiter im KH Spittal/Drau

## Der Mehrwert der Kapsch BusinessCom Lösung für das A. ö. Krankenhaus Spittal a. d. Drau.

- Langfristige Lösung mit hoher Performance und Investitionssicherheit
- Zusammenarbeit mit einem verlässlichen Partner
- Optimale IT-, Netzwerk- und Datensicherheit
- Verbesserung der Geschäftsprozesse