

HERSTELLERINFORMATION // In Zeiten, in denen Daten nur noch digital gespeichert und verarbeitet werden, ist es insbesondere im Gesundheitswesen wichtig, das Praxisnetzwerk abzusichern und hochsensible Patientendaten vor Angriffen zu schützen. Daran kommt keiner vorbei: CGM PROTECT – der Rundum-sorglos-Schutz vor Angriffen auf das Praxisnetzwerk und die Daten von Patienten.

„ALLES AUS EINER HAND“

Bereits seit Anfang 2021 gilt daher die IT-Sicherheitsrichtlinie gemäß § 75b SGB V. Diese verpflichtet Arzt-, Zahnarzt- und Psychotherapiepraxen jeglicher Größenordnung dazu, Maßnahmen zur IT-Sicherheit, also zum Schutz von Hard- und Software, zu ergreifen, um Datenmissbrauch zu verhindern.

Darunter fällt unter anderem der Einsatz einer Firewall sowie eines Virenschutzprogramms. Diese müssen für einen vollumfänglichen Schutz und einen reibungslosen Praxisbetrieb perfekt auf die Rahmenbedingungen in der Institution sowie dem Praxisnetzwerk abgestimmt sein.

Als führendes E-Health-Unternehmen ist die CompuGroup Medical (CGM) seit über 30 Jahren der starke Partner für Gesundheitsprofis im Bereich Telematikinfrastruktur (TI) und Arztsoftware. Mit CGM PROTECT bietet sie nun auch IT-Security Produkte, die perfekt auf die Bedürfnisse von Praxen und Institutionen aller Fachbereiche abgestimmt sind.

Mit einer starken Kombination aus CGM Firewall und CGM Endpoint 360° bietet die CGM einen maßgeschneiderten Rundumschutz für das Praxisnetzwerk. TI und IT-Security: Alles aus einer Hand!

CGM Firewall – Der Türsteher für das Praxisnetzwerk

Die Wege, über welche sich Schadsoftware im Praxisnetzwerk einnisten kann, sind ebenso vielfältig wie die Arten der Schadsoftware selbst (Viren, Trojaner & Phishing). Umso wichtiger ist es, potenzielle Bedrohungen bereits „an der Schwelle“ aufzuhalten. Genau dazu dient die CGM Firewall: Durch ihre Grundkonfiguration werden die Anforderungen der IT-Sicherheitsrichtlinie für jede Praxis optimal umgesetzt. Anhand individuell festgelegter Regeln, die auf die Bedürfnisse der jeweiligen Praxis abgestimmt sind, wehrt sie gezielt Angriffe von außen auf das Praxisnetzwerk ab. Dabei erlaubt sie nur Verbindungen, die im Vorfeld explizit freigeschaltet wurden. Der Eingangskanal zur Praxis wird dadurch bes-

