



# Zukunftsfähige IT-Sicherheit aus einer Hand

100-prozentige Sicherheit vor einem Cyberangriff gibt es selbst mit der besten IT-Security nicht: Das Städtische Klinikum Wolfenbüttel meisterte einen Ransomware-Angriff jedoch mit Bravour. Und so gaben die Verantwortlichen dank dem schnellen und unkomplizierten Einsatz des Rapid-Response-Teams von Sophos und den IT-Beratern von ACP IT Solutions auch die Umsetzung eines neuen IT-Security-Konzepts in die Hände der beiden Spezialisten. Das Ergebnis ist ein modernes Cybersecurity-Ökosystem aus einer Hand, das den Netzwerkschutz intelligent mit dem Schutz der Endpoints und Server kommunizieren lässt.

## AUF EINEN BLICK



**Städtisches Klinikum  
Wolfenbüttel gGmbH**

**Branche**  
Gesundheitswesen

**Anzahl der Nutzer**  
1.000

**Sophos-Partner**  
ACP IT Solutions AG

**Sophos-Produkte**  
Sophos Firewall  
Sophos Central Endpoint Protection with XDR  
Sophos Central Server Protection with XDR

*“Dass wir den IT-Sicherheitsvorfall so schnell bewältigen konnten, ist eine wunderbare Teamleistung gewesen. Ohne ACP hätten wir nie so schnell alles wieder zum Laufen bekommen.”*

Sebastian Skalski, Leitung Informationstechnologie, Städtisches Klinikum Wolfenbüttel gGmbH



Das Städtische Klinikum Wolfenbüttel ist mit seinen rund 900 Mitarbeitenden der einzige Anbieter für stationäre und ambulante Krankenhausleistungen im Landkreis. Das Tochterunternehmen der Stadt Wolfenbüttel versteht sich als Vordenker und Vorreiter einer zukunftsfähigen Gesundheitswirtschaft. Auch in seiner digitalen Transformation ist das Klinikum vorbildlich und bereits zu 85 Prozent fortgeschritten. Von der Patientenaufnahme über die Medikamentenversorgung bis zur Werteerfassung auf der Intensivstation und der Essensbestellung läuft alles digital ab.

## Die Herausforderung

Im Juli 2021 wurde das Klinikum Wolfenbüttel Opfer eines Cyberangriffs. Cyberkriminelle hatten eine Ransomware eingeschleust und einen Backup-Server verschlüsselt, sodass der ärztliche Dienst nicht mehr auf das Krankenhausinformationssystem zugreifen konnte. Solche Angriffe können jedes Unternehmen treffen – trotz bester Schutzvorkehrungen. IT-Leiter Sebastian Skalski bewahrte einen kühlen Kopf und reagierte blitzschnell: Er nahm die gesamte IT vom Netz, um eine weitere Ausbreitung der Malware zu verhindern. Dann berief er einen Krisenstab ein und holte sich Unterstützung von ACP IT Solutions und Sophos. Die Herausforderung war, die Malware aufzuspüren, die Systeme zu bereinigen und den IT-Betrieb schnell wiederherzustellen.

## Die Lösung

Der mit dem Projektmanagement beauftragte IT-Spezialist ACP mobilisierte das Rapid Response-Team des Security Partners Sophos und war sofort im Einsatz. Noch am selben Tag wurde eine neue Firewall beschafft und installiert. Während die Security-Spezialisten von Sophos den Tathergang analysierten, die Eintrittspforte ermittelten und die Malware unschädlich machten, installierten die ACP-Techniker den neuen Sophos XGS Cluster, konfigurierten die Firewall, installierten Sophos Central Server Protection XDR und etablierten Synchronized Security. Die Lösung stellte die verschlüsselte Datenbank mit einem Backup wieder her und baute einen sicheren VPN-Tunnel für die Kommunikation mit den Krankenkassen und anderen externen Partnern des Klinikums auf.

## Das Ergebnis

Innerhalb von kurzer Zeit war das Städtische Klinikum Wolfenbüttel wieder am Netz. „Dass wir den Vorfall so schnell bewältigen konnten, ist eine wunderbare Teamleistung gewesen – von der Geschäftsführung bis zu den Ärzte- und Pflegekräften und auch zu unseren Partnern. Ohne ACP und Sophos hätten wir nie so schnell alles wieder zum Laufen bekommen“, lobt IT-Leiter Sebastian Skalski. Mit dem neuen Sophos XGS Cluster und Sophos Central Server Protection XDR verfügt das Unternehmen jetzt über bestmöglichen Schutz vor Malware-Angriffen nach aktuellem Stand der Technik. Alle Clients und Server, die mit der Sophos Endpoint Protection gesichert sind, kommunizieren mit dem Cloudservice Sophos Central und der Firewall und können bei einem Angriff dank des Adaptiven Cybersecurity Ecosystems ACE schnell reagieren.



## Der Partner: ACP Gruppe

Die ACP entwickelt als IT- und Digitalisierungspartner den maximalen Spielraum für das Business von Unternehmen. Mit unserer Erfahrung und den Potentialen neuer Technologien ermöglichen wir unseren Kunden, innovativ zu sein. Mit mehr als 50 Geschäftsstellen in ganz Deutschland und Österreich ist ACP immer in Kundennähe und ein Ansprechpartner auf Augenhöhe.

Mehr Informationen  
unter [www.sophos.de](http://www.sophos.de)