Wie bewältigt man einen Cyberangriff?

Städtisches Klinikum Wolfenbüttel

100-prozentige Sicherheit vor einem Cyberangriff gibt es selbst mit der besten IT-Security nicht. Im Ernstfall ist es wichtig, schnell zu reagieren und Schaden zu minimieren. Das Städtische Klinikum Wolfenbüttel meisterte diese Herausforderung mit Bravour: Nach einer Ransomware-Attacke war es mit Hilfe von ACP IT Solutions und Sophos in kurzer Zeit wieder online.

IT for innovators.

Im Ernstfall zählt die Teamleistung

Der Schock war groß, als das Städtische Klinikum Wolfenbüttel feststellte: Wir wurden verschlüsselt. Doch IT-Leiter Sebastian Skalski behielt einen kühlen Kopf und reagierte blitzschnell. Er nahm alle Systeme vom Netz und berief einen Krisenstab ein. ACP IT Solutions und das Sophos Rapid Response-Team waren sofort zur Stelle. Weil alle internen und externen Partner nahtlos Hand in Hand arbeiteten, hatten sie die Lage schnell unter Kontrolle und die IT konnte wieder hochgefahren werden. Die Patientenversorgung war zu keinem Zeitpunkt eingeschränkt.

Es war mitten in der Nacht, als der Anruf kam. Sebastian Skalski erinnert sich: „Der ärztliche Dienst wollte auf das Krankenhausinformationssystem zugreifen. Als das nicht funktionierte, verständigte er den IT-Rufdienst. Der IT-Mitarbeiter hat dann alle Systeme gecheckt und festgestellt, dass eine Verschlüsselung vorliegt." Cyberkriminelle hatten eine Malware eingeschleust und forderten Lösegeld. Solche Ransomware-Attacken zählen nach wie vor zu den größten Cyberrisiken. Das Perfide daran: Man kann sich nie zu 100 Prozent davor schützen. Denn auch mit der besten IT-Security besteht immer noch ein Restrisiko, dass ein Angriff durchkommen kann. „Wir haben in der Nacht noch versucht, das System wiederherzustellen", erklärt Sebastian Skalski. „Als wir dann nicht mehr auf unseren Datenspeicher zugreifen konnten, war klar, dass die Verschlüsselung noch in Gang ist. Deshalb haben wir vorsichtshalber die gesamte IT heruntergefahren. Hätten wir die Systeme weiterlaufen lassen, wäre wahrscheinlich alles verschlüsselt worden. So war zum Glück nur ein Backup-Server betroffen."

Was bedeutet es, wenn ein Krankenhaus plötzlich offline ist?

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 Essensbestellung läuft alles digital ab. Wenn ein neuer Patient oder eine neue Patientin ins Klinikum kommt, erfolgt sofort die elektronische Meldung an die Krankenkasse. Alle Laborwerte liegen digital vor. Pflegekräfte sind mit Tablets ausgestattet, über die sie am Krankenbett wichtige Daten abrufen oder die Essenswahl der Patient*innen in die Küche übermitteln können. „Auch auf der Intensivstation ist alles komplett digitalisiert", erklärt Sebastian Skalski. „Da läuft ein Patientenmanagementsystem, das sämtliche Beatmungswerte, Blutdruckwerte, Pulswerte, Temperaturwerte etc. im Minutentakt aufzeichnet und zur Abrechnung übermittelt."

Weil in Folge des Cyberangriffs alle Systeme offline waren, mussten die Mitarbeitenden auf analoge Prozesse umstellen und sprichwörtlich wieder mit Papier und Bleistift arbeiten. Sämtliche Netzwerkverbindungen zu anderen Kliniken und Praxen wurden gekappt. Ärzte- und Pflegeteams konnten nicht mehr auf wichtige Anamnese-Daten zugreifen und mussten sie neu erheben. „Das hat zum Glück hervorragend funktioniert", lobt Skalski. „Jeder wusste sofort, was zu tun war, und hat sich schnell auf die neue Situation eingestellt, sodass die Patientenversorgung gesichert war. Hier hat uns geholfen, dass wir in den letzten Jahren eine KTQ-Zertifizierung durchlaufen hatten." Dieses Verfahren (Kooperation für Transparenz und Qualität im Gesundheitswesen) dient der Optimierung von Prozessabläufen und beinhaltet auch ein Notfallmanagement. Um den einstudierten Notfallplan zu aktivieren, hatte Sebastian Skalski noch in der Nacht des Cyberangriffs einen internen Krisenstab

Städtisches Klinikum Wolfenbüttel gGmbH
www.klinikum-wolfenbuettel.de

Städtisches Klinikum Wolfenbüttel

Facts

Kunde: Städtisches Klinikum Wolfenbüttel gGmbH

Sitz: Wolfenbüttel

Mitarbeiter*innen: ca. 900

Branche: Gesundheitswesen

Partner

Sophos

SOPHOS

Unsere Lösung

- Sofortiges Krisenmanagement
- Beschaffung und Implementierung der neuen Security-Systeme trotz Lieferengpass
- Sofortige Mobilisierung des Sophos Rapid Response-Teams
- Wiederherstellung des IT-Betriebs in kürzester Zeit
- Security-Lösung: Sophos XGS, Sophos Central Server Protection XDR, Synchronized Security

zusammengetrommelt, in dem bis zum Morgen alle Chefärzte und Vertretenden des Management-Teams versammelt waren. Anschließend ging es darum, die IT mithilfe von externen Spezialisten schnell wieder betriebsfähig zu machen. Denn jede Stunde Ausfall verursachte nicht nur zusätzliche Arbeit für das Klinikpersonal, sondern auch erheblichen wirtschaftlichen Schaden.

Ein beherztes Vorgehen mit kühlem Kopf

Skalski verständigte die Braunschweiger Cybercrime-Unit der Polizei, machte Meldung beim Bundesamt für Sicherheit in der Informationstechnik (BSI) und bei der Datenschutzbehörde. Außerdem holte er sich Unterstützung beim langjährigen IT-Partner ACP IT Solutions. Sofort setzte die zuständige Account Managerin bei ACP alle Hebel in Bewegung: „Ich habe sämtliche Termine verschoben. Wenn es bei einem Kunden brennt, sind wir da. Das ist uns ganz wichtig." ACP übernahm das Projektmanagement, mobilisierte das Rapid Response-Team des Security-Partners Sophos und war innerhalb von zwei Stunden beim Klinikum Wolfenbüttel vor Ort. Während die Security-Spezialist*innen den Tathergang analysierten, die Malware aufspürten und die Systeme bereinigten, kümmerte sich ACP darum, die IT schnellstmöglich wieder zum Laufen zu bringen. „Für uns war es sehr beruhigend, einen Partner wie ACP zu haben", sagt Sebastian Skalski. „Es hätte ja auch sein können, dass wir neue Hardware, Speicher oder Software brauchen. Mit ACP war ich mir sicher: Egal was passiert – auch wenn wir alles neu aufsetzen müssen – wir schaffen das." wDas Klinikum und ACP waren in ständigem Kommunikationsfluss. Und mit der lösungsorientierten Handlungsweise auf beiden Seiten sowie der direkten Zusammenarbeit mit der Geschäftsführung, konnten unbürokratisch Freigaben eingeholt werden und Bestellungen abgewickelt werden. Das hat die Situation natürlich maßgeblich vereinfacht.

Schnell wieder online

Dank der hervorragenden Herstellerbeziehungen gelang es ACP, trotz damaliger Lieferengpässe innerhalb von wenigen Stunden eine neue Firewall für das Klinikum zu organisieren. Die Techniker tauschten den bestehenden Sophos SG Cluster gegen den modernsten Sophos XGS Cluster, konfigurierten die Firewall, installierten Sophos Central Server Protection XDR und etablierten Synchronized Security. Nachdem das Rapid Response-Team die Schadsoftware gefunden und unschädlich gemacht hatte, stellte ACP 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. „Unsere Partner wollten natürlich eine Bescheinigung haben, dass wir tatsächlich virenfrei sind, bevor sie sich wieder mit uns vernetzen", erklärt Sebastian Skalski. „Sophos hat uns offiziell bestätigt, dass wir aktuell keine Auffälligkeiten mehr haben und noch 30 Tage lang überwacht werden. So konnten wir schnell wieder Verbindung zu anderen Kliniken und Praxen aufnehmen."

Künftig noch besser geschützt

Mit dem neuen Sophos XGS Cluster und Sophos Central Server Protection XDR verfügt das Klinikum 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. Wenn künftig ein Client einen schadhaften Befall meldet, erhalten alle anderen diese Information und stellen den Datenverkehr mit dem infizierten System ein. Auch die Firewall sperrt diesen Client für jedwede Kommunikation. „Wir haben jetzt genau die Security-Lösung, die wir schon vor dem Cybervorfall gemeinsam mit ACP einführen wollten", freut sich Sebastian Skalski. „Damals hatten wir nur noch auf die beantragten Fördermittel im Rahmen des Krankenhauszukunftsgesetzes gewartet." Doch eins ist klar: 100-prozentige Sicherheit kann auch die beste Technik nicht bieten. Im Ernstfall kommt es immer auf die Menschen an: „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 hätten wir nie so schnell alles wieder zum Laufen bekommen."

„Dass wir den Vorfall 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

Einfach für Sie da

ACP IT Solutions AG

+49 40 809077677
acp.nord@acp.de
www.acp.de