Thema: Schwerer Cyberangriff auf Klinikum Lippe
Zeichenzahl: 5.200 (inkl. LZ)

---

indevis unterstützt Klinikum Lippe nach schwerem Cyberangriff

München, 07.02.2023 – Mitte November 2022 wurde das Klinikum Lippe Opfer eines Cyberangriffs einer internationalen Hacker-Gruppe. Die Angreifer verschlüsselten Daten und legten große Teile der IT-Infrastruktur lahm. Mithilfe des Managed Security Service Providers indevis konnte der Klinikumsbetreiber aber rasch die wichtigsten Systeme wieder online nehmen, der digitale Wiederaufbau und zusätzliche Härtung sind fast abgeschlossen.

Am 17.11.2022 entdeckten Administratoren des Klinikums Anzeichen für einen Cyberangriff: Sie konnten sich nicht mehr in die Systeme einloggen und die Berechtigungen einiger Nutzer waren verändert. Das Klinikum Lippe war zur gleichen Zeit bereits wegen eines potenziellen Projektes in erstem Kontakt mit dem Security-Dienstleister indevis. Als klar war, dass Hacker am Werk sind, wurde der Security-Dienstleister direkt hinzugezogen. Zusammen mit Grant Thornton, einem Spezialisten für Cyber-Forensik, nahm indevis bereits am 18.11.2022 die Arbeit auf. Da das Klinikum Lippe als kritische Infrastruktur (KRITIS) eingestuft ist, zog man außerdem u. a. das Landeskriminalamt NRW, Kriminalpolizei sowie informativ das Bundesamt für Sicherheit in der Informationstechnik (BSI) hinzu.

„Zum Zeitpunkt des Angriffs waren im Klinikum bereits eine ganze Reihe von Security-Maßnahmen im Aktivbetrieb. Das Netzwerk war segmentiert und die Firewalls scharf, das Sicherheitsniveau war hoch. Aber die Angriffe höchstprofessioneller internationaler Hacker-Gruppen zeigen immer mehr, dass jenseits des defensiven Schutzes auch weitere Maßnahmen zur schnellen Angriffserkennung und -abwehr notwendig werden. Nur so kann der Schaden bestmöglich minimiert werden“, sagt Constantin Schlachetzki, Abteilungsleiter Strategic Program Management bei indevis. „In letzter Zeit erleben wir solche Angriffe leider immer häufiger. Die Organisierte Kriminalität macht auch vor KRITIS nicht halt und gefährdet Menschenleben. Entsprechend wichtig ist es für unsere Kunden, sich rund um die Uhr auf unsere eingespielte Truppe von Cybersecurity-Analysts und System-Engineers verlassen zu können, die wir sofort in den Einsatz schicken.“

Um die Auswirkungen des Angriffs einzudämmen, nahmen die Experten von indevis die webbasierten Services des Klinikums erst einmal vom Netz. Dann isolierte der Dienstleister infizierte Netzwerkteile, um die Verbreitung der Schadsoftware zu vermeiden. Parallel starteten mit Unterstützung eines Unterhändlers des Landeskriminalamts Verhandlungen mit den Hackern. Glücklicherweise erhielt das Klinikum auf diesem Weg den digitalen Schlüssel für die gesperrten Daten.

Um zu verhindern, dass solch ein Angriff erneut passiert, startete indevis den Wieder- beziehungsweise Neuaufbau des Netzwerks. Der Dienstleister versuchte dabei, möglichst viele Bestandssysteme zu retten. Der Sicherheit geschuldet mussten jedoch einige Komponenten neu aufgesetzt werden. Außerdem implementierte indevis nun eine mehrschichtige Verteidigung zur Härtung der Gesamtarchitektur. Dadurch sinkt die Wahrscheinlichkeit erheblich, dass sich so ein Angriff auf das Klinikum wiederholt. „Unser Ziel war es, parallel zu den forensischen und kriminaltechnischen Maßnahmen mit dem Wiederaufbau zu beginnen, um zu jeder Zeit die Auswirkungen auf den IT-Betrieb so gering wie möglich zu halten. Unser Consulting-Team hat langjährige Erfahrung mit der schnellen Umsetzung von IT-Security-Lösungen in hochkritischen Situationen und konnte so kurzfristig alle notwendigen Maßnahmen implementieren“, erklärt Constantin Schlachetzki.

Zu den neu implementierten Security Services gehört u. a. Palo Alto Cortex XDR (Extended Detection and Response). Das XDR ist Teil des Services Managed Detection and Response (MDR) von indevis. Security-Profis überwachen hier den Netzwerk-Traffic und greifen bei verdächtigen Aktivitäten direkt ein. „Mit einer MDR-Lösung können Angriffe noch frühzeitiger gebremst werden. Security-Profis wissen, worauf sie achten müssen, denn sie kennen das Vorgehen der Angreifer. „Nur“ Firewalls sind schon einfacher zu überwinden“, erläutert Constantin Schlachetzki.

Durch die kompetente Hilfe von indevis konnten einige Systeme nach kurzer Zeit wieder online gehen. Grundfunktionen wie die Patientendatenverwaltung ließen sich wieder digital ausführen. „Wir waren erleichtert, dass die indevis-Experten uns unmittelbar helfen und wir in enger Zusammenarbeit Teilsysteme schnell wieder in Betrieb nehmen konnten. Ob am Wochenende oder bis spät in die Nacht, die Security-Profis arbeiteten durchgehend. Der Wert des Zusammenspiels einer gut aufgestellten IT und eines verlässlichen Sicherheitspartners wird hier deutlich“, sagt Dr. Johannes Hütte, Geschäftsführer und Sprecher der Klinikum Lippe GmbH.

Cyberangriffe durch professionelle, internationale Hacker-Gruppen nehmen zu. Unternehmen und KRITIS-Organisationen sollten ihre Cybersecurity überdenken und Maßnahmen zur frühzeitigen Angriffserkennung implementieren. Managed Detection and Response (MDR) ist eine sinnvolle Ergänzung für IT-Security-Architekturen, um den Cyberkriminellen Paroli zu bieten.

Über die indevis GmbH

Die nach der internationalen Norm ISO/IEC 27001 zertifizierte indevis GmbH ist einer von Deutschlands führenden Managed Security Service Providern (MSSP). Bereits seit über 20 Jahren setzt das Unternehmen Sicherheitsstandards in der Informationstechnologie und bietet Kunden jeder Größe und Branche passende IT-Sicherheitslösungen für Netzwerk, Rechenzentrum und Cloud.

Mit modernsten Rechenzentren und einer redundant angelegten Infrastruktur bietet indevis den bestmöglichen Schutz vor IT-Sicherheitsrisiken und sorgt für Sicherheit in einer vernetzten Welt.

Flankiert von professionellen Consulting-, Management- und Supportdiensten schützen die Produkte und Managed Security Services von indevis die digitalen Geschäftsprozesse der Kunden und erfüllen sowohl die Anforderungen der Wirtschaft als auch die öffentlicher Einrichtungen, wie Behörden und Hochschulen.

Weitere Informationen finden Sie unter www.indevis.de.

Pressekontakt
Akima Media
Daniela Fichtl / Caroline Arheidt
Garmischer Str. 8
80339 München
Tel.: +49 (0) 89-1795918-0
indevis@akima.de
www.akima.de

Bildmaterial:

BU:
Dr. Johannes Hütte, Geschäftsführer und Sprecher der Klinikum Lippe GmbH (Bild © Klinikum Lippe GmbH)

BU:
Constantin Schlachetzki, Abteilungsleiter Strategic Program Management der indevis GmbH