DIAGNOSE: LEBENSBEDROHLICHER VIRUS AUFGEDECKT, PATIENT AUSSER LEBENSGEFAHR

CYOSS Krankenhäuser werden immer wieder digital angegriffen. Anhand eines typischen Krankheitsverlaufs berichten wir, wie dies ablaufen kann und welche Lösungen es heute schon gibt. Das Krankenhaus war einige Tage in stationärer Behandlung von CYOSS, einem führenden Anbieter von Cyber-Sicherheitslösungen.

SYMPTOME

Das Krankenhaus stellte sich mit Symptomen wie Warnmeldungen des Virenscanners und Fehlermeldungen im Betriebssystem in der Notfallambulanz der CYOSS vor. Der Patient klagte darüber, dass Angestellte keinen Zugriff mehr auf ihre Computer hätten. Zahlreiche OP-Termine mussten verschoben werden. Die Office-IT wurde nach Bekanntwerden der Störung abgeschaltet, deshalb konnten zeitweise keine Telefonanrufe angenommen werden. Weitere Beschwerden waren verminderte Datengeschwindigkeit und der Ausfall mehrerer Rechner. Im vergangenen Jahr war bereits eine Episode ähnlicher Beschwerden vorangegangen, die lokal mit einem Anti-Virus-Programm behandelt wurden.

BEURTEILUNG & VERLAUF

Die klinische Symptomatik mit Änderungen an Konfigurationen und neu angelegten Administratorkonten in Kombination mit Hinweisen auf Anmeldungen aus ungewöhnlichen Ländern und zu ungewöhnlichen Uhrzeiten legten die Verdachtsdiagnose eines Befalls mittels eingeschleuster Schadsoftware nahe, um Dateien zu verschlüsseln und Aktionen zu blockieren.

Dr. Hanka von CYOSS teilte mit, dass die Schadsoftware bereits seit mehreren Wochen den Organismus befallen und sich seitdem „aggressiv" verbreitet hätte. Zur Diagnosesicherung wurde eine Sicherheitsanalyse durchgeführt, welche die größten Sicherheitslücken und Risiken aufzeigt. Dabei zeigte sich passend zum Erstbefund ein unzureichendes Administratoren- und Rollenkonzept für die Office-IT und eine fehlende Sensibilisierung der Mitarbeiter. Aufgrund des deutlich reduzierten Allgemeinzustandes des Patienten und der bereits ausgeprägten Symptomatik wurde der Patient stationär aufgenommen. Der Virus hatte bereits in mehrere Abteilungen gestreut und einen Großteil der Daten verschlüsselt – mit einem erheblichen finanziellen Schaden.

BEHANDLUNG

In einer mehrstündigen Operation wurde der Virus durch die CYOSS entfernt und die Betriebssysteme wiederhergestellt. Dazu wurde dem Patienten am offenen Herzen ein Security-Cockpit inklusive SOC-Service-Leistungen installiert. Mittels implantierter Sensoren wird künftig tagesaktuell der Cyber-Sicherheitsstand aufgezeigt und rechtzeitig auf Auffälligkeiten und Sicherheitslücken hingewiesen. Unterstützend bekam der Patient eine Awareness-Schulung für seine Mitarbeiter verabreicht.

Unter der Therapie besserte sich der Zustand des Patienten rasch. Am zweiten Tag des stationären Aufenthaltes kam es zur Normalisierung des OP-Alltags, sodass die weitere Therapie beim Patienten vor Ort erfolgen konnte. Dieser wird seitdem durch erfahrene Sicherheitsspezialisten der CYOSS betreut und durch Detection & Response Schulungen ausreichend gesichert, um künftig Angriffe schneller zu entdecken.

CYOSS GMBH
Ganghoferstraße 66, 80339 München
Ansprechpartner: Alexandra Spann
Tel.: +49-(0)89-92161-2914
office@cyoss.com
cyoss.com/health