Cyber-Kriminalität

Hacker-Angriffe auf Krankenhäuser haben zugenommen

08.03.2016 | 06:00 Uhr

Hochtechnologie ist in Kliniken nicht mehr wegzudenken. Die Systeme sind vielfach vernetzt.
Foto: Svenja Hanusch

Bochum. Kliniken wehren sich mit ausgeklügelten Programmen gegen Schad-Software. Sicherheitssysteme fangen schädliche Mails ab.

Erfolgreiche Hacker-Angriffe auf mehrere Kliniken in NRW haben jüngst für Aufsehen gesorgt. Kriminelle entwendeten unter anderem digitale Patientendaten und beeinträchtigten mit virenverseuchten E-Mails den Krankenhausbetrieb erheblich. In einer Bochumer Klinik hat es in den vergangenen Jahren keine erfolgreiche Cyber-Attacke gegeben.

Dennoch gehört die Abwehr von Schadsoftware dort längst zum Alltag. So erhält beispielsweise das Knappschaftskrankenhaus „täglich verdächtige Mails, die durch unsere Sicherheitssysteme abgefangen werden. Teils sind es nur wenige, manchmal hunderte Mails am Tag", teilt das Krankenhaus mit. Diese Mails werden jedoch häufig zufällig an unzählige Adresse versandt. Einen gezielten Angriff habe man aber noch nicht festgestellt. Von ähnlichen Erfahrungen berichten auch die übrigen Bochumer Kliniken.

Angriff im Dezember schlug fehl

Im Bergmannsheil gab es lediglich im Dezember einen Versuch, mit Schadsoftware per E-Mail Daten im Krankenhaus-Netz zu sperren, um im Nachhinein für deren Freigabe Lösegeld zu verlangen, berichtet Sprecher Robin Jopp. „Unsere IT konnte die Schädlingsdatei jedoch rechtzeitig identifizieren, lokal begrenzen und unschädlich machen." Der Krankenhausbetrieb sei zu jeder Zeit normal weiter gelaufen.

Wären Hacker tatsächlich mit einem Angriff erfolgreich, „könnte das zu einer elementaren Störung der Abläufe führen, je nachdem, welche Systeme betroffen sind", sagt Oliver Leifels, IT-Leiter der Augusta-Kranken-Anstalt. Doch auch in dieser Ausnahmesituation würden Notfallkonzepte den Krankenhausbetrieb aufrecht erhalten. So habe ein Hacker-Angriff auf die Augusta-Klinik vor circa zehn Jahren, verursacht durch Schadsoftware auf einem USB-Stick, keine nachhaltigen Schäden angerichtet.

Auch die anderen Bochumer Krankenhäuser nutzen Sicherheitssysteme, die im Falle eines erfolgreichen Angriffs greifen sollen. „Dort ist vorgesehen, dass wir den Betrieb wichtiger Medizintechnik notfalls auch ‚offline' ohne Netzanbindung gewährleisten zu können", sagt Bergmannsheil-Sprecher Robin Jopp. Um so ein Szenario von vorneherein zu verhindern, habe man angesichts der aktuellen Vorkommnisse nochmals in die Sicherheit investiert. „Jede E-Mail, die uns erreicht, wird von acht Virenscannern geprüft." Bei der Helios-Gruppe, die das St. Josefs-Hospital in Linden betreibt, heißt es dazu: „Wir schützen unsere Kliniken durch hausindividuelle Sicherheitskonzepte mit mehrstufigen Sicherheitskontrollen."

Kliniken setzen auf Aufklärung

Viele Krankenhäuser greifen dabei auf Hilfe von außen zurück. So auch das Katholische Klinikum, wie Sprecher Jürgen Frech betont: „Der Schutz vor Schadsoftware ist eine permanente Aufgabe, deren Prozesse wir kontinuierlich verbessern. Schon vor längerer Zeit wurde dazu ein externer Sicherheitsberater hinzugezogen." Die Sicherung sensibler Daten auf externen Medien gehört nach Angaben der Bochumer Kliniken ebenso zum Standard, wie ein Passwortschutz für viele medizinische Geräte.

Um der Schadsoftware, die per E-Mail kommt, erst gar kein Einfallstor zu bieten, setzen die Krankenhäuser bei ihren Mitarbeitern angesichts der aktuellen Bedrohung verstärkt auf Aufklärung. „In Absprache mit der Geschäftsführung ist unter anderem eine Information mit Richtlinien zum Umgang mit Internet, E-Mails und mit deren möglichen Anhängen an alle Mitarbeiter erfolgt", heißt es exemplarisch in der Mitteilung der Augusta-Klinik .

Christoph Husemeyer