IT-Sicherheitsrisiko Krankenhaus

Zahlreiche Cybersecurity-Schwachstellen bei deutschen Krankenhäusern entdeckt

Auch kritische Infrastruktur stark betroffen

Hagenberg (Österreich)/München/Berlin, 22. Januar 2021 – Bei einem Drittel aller deutschen Krankenhäuser gibt es Cybersecurity-Schwachstellen. Werden diese systematisch von Cyberkriminellen missbraucht, kann das zu einem nationalen Sicherheitsrisiko werden. Zu diesem Ergebnis kommt eine Studie von drei IT-Sicherheitsexperten aus Deutschland und Österreich für die CyCon-Konferenz der NATO, die aus Pandemiegründen virtuell stattfinden wird. Johannes Klick von Alpha Strike Labs, Robert Koch von der Universität der Bundeswehr und Thomas Brandstetter von Limes Security haben die Ergebnisse jetzt unter dem Titel „Epidemic? The Attack Surface of German Hospitals during the COVID-19 Pandemic" vorab veröffentlicht. Die Studie befindet sich im Review Prozess und hat die Sicherheitslage von im Internet öffentlich zugänglichen Systemen und Informationen von mehr als 1500 deutschen Krankenhäusern untersucht. 32 Prozent der analysierten Dienste wurden in unterschiedlichem Ausmaß als verwundbar eingestuft. 36 Prozent aller untersuchten Krankenhäuser weisen Angriffspunkte auf. Insgesamt wurden mehr als 900 kritische Schwachstellen identifiziert.

Besonders viele Schwachstellen bei großen Kliniken

Auffallend ist, dass Krankenhäuser, die nach der Einstufung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur kritischen Infrastruktur (KRITIS) gehören, eine erkennbar höhere Anzahl an Schwachstellen aufweisen als kleinere Krankenhäuser. Entgegen der Erwartung wird die IT-Sicherheit bei den zu KRITIS gehörenden Kliniken mit mehr als 30.000 vollstationären Behandlungen/Jahr offensichtlich nicht professioneller gehandhabt.

Insgesamt wurden mit Hilfe des Distributed Cyber Recon System (DCS) von Alpha Strike Labs, welches bereits auf dem CCCamp 2019 vorgestellt wurde, 1.483 GB Daten aus 89 verschiedenen globalen Internet-Scans ausgewertet. Damit konnten 1.555 deutsche Krankenhäuser erfasst werden. Bei der Angriffsoberflächenanalyse wurden mehr als

13.000 Service-Banner der Krankenhäuser zur Versionsidentifikation und anschließender CVE-basierter Schwachstellenidentifikation untersucht. 32 Prozent aller erreichbaren Netzwerkdienste waren schwachstellenbehaftet. So sind unter anderem immer noch sehr alte Windows 2003 Server im Einsatz, die schon seit 2015 keine Sicherheitsupdates mehr von Microsoft erhalten.

„Die deutschen Krankenhäuser stehen vor zentralen Herausforderungen im Bereich der kritischen IT-Infrastruktur. Es gibt immer noch eine hohe Zahl veralteter, manchmal proprietärer Systeme, welche nur schwierig patchbar sind, sei es aufgrund von erforderlichen Re-Zertifizierungen oder dem Support-Ende von Software. Dem stehen sehr begrenzte Mittel für die IT-Sicherheit gegenüber," so Mitautor Robert Koch. „Der deutsche Gesundheitssektor bietet im Jahr 2020 trotz erhöhter Kritikalität und verstärkten Regulierungsbestrebungen zahlreiche sichtbare Angriffsflächen. Aus Sicht des nationalen Risikomanagements muss die Aufklärungsarbeit im Bereich IT-Security für KRITIS-Organisationen deutlich verstärkt werden." Johannes Klick ergänzt: „Durch Penetrationstests bei unseren Kunden wissen wir, dass Krankenhäuser häufig nicht ausreichend vor Cyberangriffen geschützt sind, oft fehlt es schlicht an Budget, Personal und vor allem Risikobewusstsein. Deshalb stellt sich die Frage, ob der Staat nicht selbst die Schwachstellensuche in die Hand nehmen sollte." Thomas Brandstetter ergänzt: „In anderen Regionen der Welt ist der Schutz kritischer Infrastrukturen schon deutlich länger und intensiver Staatsthema, mit entsprechenden Regulatorien und Budgets. Es besteht deutlicher Nachholbedarf. Sowohl der Gesundheitssektor als auch der Staat müssen sich effektiver aufstellen, um den Schutz wichtiger kritischer Infrastrukturen wie Krankenhäuser auch von digitaler Seite sicherzustellen."

Die Studienautoren

Johannes Klick, M.Sc. (Informatik) ist Geschäftsführer der Alpha Strike Labs GmbH und promoviert zum Thema „Large-Scale Internet-Scanning und globaler Schwachstellenerkennung" an der Freien Universität Berlin.

Dr. Dr. habil Robert Koch ist Admiralstabsoffizier der Bundeswehr und Privatdozent an der Universität der Bundeswehr München.

FH-Prof. Prof. (h.c.) Dipl.-Ing. (FH) Thomas Brandstetter, MBA ist Geschäftsführer der Limes Security GmbH und Professor an der FH St. Pölten.

Das Unternehmen

Alpha Strike Labs ist ein innovatives Sicherheitsforschungsunternehmen mit Sitz in Berlin, Wien und Hagenberg. In den Alpha Strike Labs wird Schwachstellenforschung betrieben, an neuen Angriffsmethoden geforscht und Lösungen zur besseren Angriffserkennung auf OT Systeme entwickelt. Speziell die Erkennung von potentiellen externen Angriffsflächen mittels Open Source Intelligence und globaler umfassender Internet-Scans stehen im Fokus der Forschung. Das exzellente Technologiewissen aus dem universitären Forschungsbereich kombiniert mit praktischer Erfahrung aus einer Vielzahl an Beratungsprojekten fördert die laufende Entwicklung neuer Methoden, die mit großem Kundenmehrwert in Projekten zum Einsatz kommen. Die innovativen Ansätze der Alpha Strike Labs wurden beim UP18@it-sa Security-Start-Up Wettbewerb mit einer Nominierung unter den besten 18 Security-Start-ups 2018 in der DACH Region ausgezeichnet. Seit Anfang 2020 sind Alpha Strike Labs Teil der Limes Security GmbH und bilden eine eigene F&E Einheit für Sicherheitsforschung. Außerdem fungiert Alpha Strike Labs als Inkubator für Produkt- und Service-Ideen.

Link zum Paper: Epidemic? The Attack Surface of German Hospitals during the COVID-19 Pandemic

Kontakt

Johannes Klick
Geschäftsführer Alpha Strike Labs GmbH
j.klick@alphastrike.io
+49 (0)176 444 30475

Bildmaterial