

Pressemitteilung

Wie geht guter IT-Schutz für Krankenhäuser?

Maßnahmenkatalog gibt konkrete Empfehlungen

Neubiberg, 03. August 2021

Immer wieder werden Krankenhäuser und andere kritische Infrastrukturen zum Ziel von Hackerangriffen und Erpressungsversuchen. Wie sich diese Einrichtungen besser schützen lassen, untersucht am Forschungsinstitut CODE der Universität der Bundeswehr München das Forschungsprojekt „Smart Hospitals – Sichere Digitalisierung bayerischer Krankenhäuser“ unter Förderung des Bayerischen Staatsministerium für Gesundheit und Pflege. Ende Juli hat das Projekt die zweite Ausgabe des „Maßnahmenkatalogs zur Verbesserung der IT-Sicherheit in bayerischen Krankenhäusern“ veröffentlicht, der Verantwortlichen konkrete und einfach umsetzbare Empfehlungen für mehr IT-Sicherheit im Gesundheitssystem an die Hand gibt.

Nicht erst seit den jüngsten Angriffen auf Lebensmittellieferanten und Energieversorgung in den USA und Europa ist klar, dass digitale Bedrohungen in unserer Welt reale Auswirkungen haben. Besonders kritisch wird es, wenn überlebenswichtige Infrastrukturen zum Ziel der Hacker werden: In Krankenhäusern können Systemausfälle schlimmstenfalls dafür sorgen, dass Patienten akut nicht mehr versorgt werden. Ein guter Schutz der IT-Infrastruktur von ist hier überlebenswichtig. Bayerns Gesundheitsminister Klaus Holetschek betont: „Krankenhäuser nehmen eine Schlüsselstellung ein, denn sie sind eine der ersten Anlaufstellen für die akute Versorgung der Menschen. Auch deshalb ist es ein wesentlicher Schwerpunkt bayerischer Gesundheitspolitik, eine leistungsfähige Krankenhausversorgung in allen Landesteilen Bayerns sicherzustellen.“

Konkrete Empfehlungen für bestmöglichen Schutz

Um dazu beizutragen und mögliche Bedrohungen aus dem Netz zu minimieren, hat das Projekt „Smart Hospitals“ bereits für die Jahre 2020/21 einen Maßnahmenkatalog erarbeitet, der als Leitfaden für guten und praktikablen IT-Schutz im Krankenhaus dienen kann. Der Katalog entstand durch gezielte Vor-Ort-Analyse der Situation in Krankenhäusern in ganz Bayern auf Basis von Interviews mit den dortigen Verantwortlichen für IT-Sicherheit – meist Geschäftsführung und IT-Abteilung. Er beschreibt rund 40 technische und organisatorische Maßnahmen, die sich am aktuellen Stand der Technik orientieren und gezielt auf Krankenhäuser ausgerichtet sind. Das Besondere: Die Publikation unterscheidet sich bewusst von

klassischen Standardwerken durch eine informelle und leserfreundliche Gestaltung – so ist beinahe jede Maßnahme auf maximal zwei Seiten beschrieben. Trotz viel Praxisnähe und Pragmatismus legen die Autorinnen und Autoren Wert auf einen hohen Detailgrad, indem sie z. B. in allen Themenbereichen auf weiterführende Literatur verweisen.

Von der Awareness bis zur Reaktion auf Angriffe

Ein Großteil des Katalogs konzentriert sich auf technische und organisatorische Präventionsmaßnahmen. Dazu gehört zum Beispiel die Absicherung der Datennetze und IT-Systeme in Krankenhäusern bis hin zu medizinischen Großgeräten. Im organisatorischen Bereich ist für die Prävention unter anderem das Schaffen von *Awareness* beim Personal oder auch die Dokumentation der IT-Landschaft des Krankenhauses wichtig. Der Katalog zeigt den Krankenhäusern hier viele konkrete Möglichkeiten der Umsetzung auf, beispielsweise den Einsatz von Flyern, Rundmails, Übungen, IT-Security-Awareness-Spielen (z.B. Online-Quizen) oder Möglichkeiten für einfache eigene technische Sicherheitstests.

Wenn bereits ein Schaden entstanden ist, hilft der Maßnahmenkatalog ebenfalls weiter. Prof. Wolfgang Hommel aus dem Projektteam „Smart Hospitals“ erklärt: „Eine sorgfältige Vorbereitung ist ausschlaggebend dafür, dass IT-Sicherheitsvorfälle schnell erkannt werden und professionell darauf reagiert wird. Unsere Maßnahmen helfen, Handlungsanweisungen vorzubereiten, die regelmäßige Aktualisierung von Notfall- und Wiederherstellungsplänen zu organisieren und Übungen des Ernstfalls gezielt durchzuführen.“

Größerer Umfang, erweiterte Inhalte

Auf Basis des Feedbacks der Krankenhäuser wurde die zweite Ausgabe des Maßnahmenkatalogs verbessert und um neue Inhalte erweitert. Dazu gehören beispielsweise die Themengebiete „Cloud Computing“ oder „Datenschutz und rechtliche Konformität“: Fragen rund um „Bring-Your-Own-Device“ oder Telearbeit im Krankenhaus kommen nun zur Sprache. Ein komplett neuer Bestandteil des Berichts sind Vorlagen für zentrale Dokumente, die gemeinsam mit mehreren Krankenhäusern und dem Landesamt für Sicherheit in der Informationstechnik (LSI) erstellt wurden. Sie sind der neuen Ausgabe im Anhang beigelegt und können von den jeweiligen Verantwortlichen im Krankenhaus an ihre Situation angepasst oder erweitert werden. Damit stellen sie einen einfachen Einstieg in den Aufbau eines Informationssicherheits-Managementsystems (ISMS) für das eigene Haus dar.

Weitere Informationen und den Maßnahmenkatalog zum Download finden Sie unter:

<https://www.unibw.de/code/smart-hospitals>

Michael Brauns
Pressesprecher
Universität der Bundeswehr München
Tel.: 089/6004-2004
E-Mail: michael.brauns@unibw.de