Nationales Testinstitut
für Cybersicherheit

MEDIENMITTEILUNG

NTC identifiziert gravierende Sicherheitslücken in Klinikinformationssystemen und veröffentlicht Empfehlungen

Zug, 23. Januar 2025 – Das Nationale Testinstitut für Cybersicherheit NTC hat in mehreren Schweizer Spitälern drei der meistgenutzten Klinikinformationssysteme (KIS) einer umfassenden technischen Sicherheitsanalyse unterzogen. Die Hersteller wurden informiert und Massnahmen zu Risikominimierung eingeleitet. Der veröffentlichte Bericht weist auf schwerwiegende Schwachstellen hin und enthält konkrete Handlungsempfehlungen zur Verbesserung der Cybersicherheit im Gesundheitswesen.

Klinikinformationssysteme bilden das Herzstück moderner Spitäler. Sie steuern den Informationsfluss, verarbeiten sensible Patientendaten und sorgen für reibungslose Abläufe im Spitalumfeld. Die Untersuchung des NTC hat nun ergeben, dass die Cybersicherheit dieser essenziellen Systeme in vielen Fällen unzureichend ist.

Ergebnisse der Analyse
In allen untersuchten Systemen wurden schwerwiegende Schwachstellen festgestellt. Insgesamt wurden mehr als 40 mittlere bis schwere Schwachstellen identifiziert. Drei davon weisen die höchste Kritikalität auf. Besonders anfällig sind Lösungen, die auf veralteten Architekturen basieren. Die Hauptprobleme umfassen grundlegende Architekturprobleme, fehlende oder nicht ordnungsgemäss umgesetzte Verschlüsselung, verwundbare Umsysteme sowie eine unzureichende Trennung zwischen Test- und Produktionsumgebungen.

Einige der identifizierten Schwachstellen ermöglichten innerhalb weniger Stunden den vollständigen Zugriff auf Patientendaten und Systeme. Während die meisten relevanten Schwachstellen inzwischen behoben oder durch mitigierende Massnahmen entschärft wurden, erfordern einige grundlegende Probleme eine umfassende Neugestaltung der Softwarearchitektur, was laut den Herstellern mehrere Jahre in Anspruch nehmen wird. Zudem wurden im Rahmen der Analyse mehrere kritische Schwachstellen in Umsystemen entdeckt, die nicht Teil des definierten Prüfungsumfangs waren, jedoch aufgrund ihrer Auffälligkeit als Zufallsfunde erkannt wurden.

Im Bericht wird bewusst auf die Nennung von Details zu den Schwachstellen verzichtet. Stattdessen erfolgte eine allgemeine Information über den NTC Vulnerability Hub sowie eine gezielte Benachrichtigung der betroffenen Spitäler über den Cyber Security Hub (CSH) des Bundesamtes für Cybersicherheit (BACS).

Empfehlungen für Spitäler
Der Bericht enthält acht zentrale Empfehlungen zur nachhaltigen Verbesserung der Cybersicherheit in Schweizer Spitälern. Dazu zählt die Berücksichtigung von Cybersicherheitsanforderungen bereits bei der IT-Beschaffung sowie die Durchführung regelmässiger Schwachstellenanalysen zur fortlaufenden Kontrolle. Insbesondere in kleineren Spitälern müssen die Verantwortlichkeiten in Bezug auf die Cybersicherheit klar geregelt und die nötigen Ressourcen bereitgestellt werden. Zudem wird eine verstärkte Vernetzung unter den Spitälern sowie der Zugang zum Cyber Security Hub (CSH) des Bundesamtes für Cybersicherheit (BACS) empfohlen.

Die Ergebnisse verdeutlichen die Notwendigkeit regelmässiger Sicherheitsüberprüfungen und klarer Verantwortlichkeiten. Ein besonderer Dank gilt den Spitälern und Organisationen, deren Engagement im Bereich Cybersicherheit entscheidend zum Erfolg dieser Sicherheitsanalyse beigetragen hat.

Zum Bericht

Medienkontakt:
Andreas W. Kaelin, Geschäftsführer
+41 41 317 00 11, andreas.kaelin@ntc.swiss

Über das Nationale Testinstitut für Cybersicherheit NTC
Das Nationale Testinstitut für Cybersicherheit NTC trägt zur Sicherheit und zur digitalen Souveränität der Schweiz bei, indem es kritische Schwachstellen vorausschauend erkennt und deren Behebung fördert. Als nicht gewinnorientierter Verein mit Sitz in Zug folgt das NTC den Prinzipien der Unabhängigkeit und Objektivität. Es führt Cybersicherheitsprüfungen von vernetzten Infrastrukturen, Geräten und Anwendungen durch, die für Gesellschaft und Wirtschaft von grosser Bedeutung sind. https://www.ntc.swiss