Nationales Testinstitut für Cybersicherheit

# Cybersicherheit von Klinikinformationssystemen

Summarischer Bericht mit Empfehlungen für das Schweizer Gesundheitswesen

| | |
|---|---|
| Version | 1.0 |
| Datum | 23. Januar 2025 |
| Klassifikation | Öffentlich |
| Autoren | Tobias Castagna, Andreas Leisibach, Dilip Many, Fabio Zuber, Patrik Fabian, Raphael M. Reischuk |
| Verantwortlich | Tobias Castagna |

# Inhaltsübersicht



**Danksagung**

Ein besonderer Dank gilt allen Organisationen und Experten, die uns entscheidende Einblicke in das Schweizer Gesundheitswesen ermöglicht haben. Das herausragende Engagement im Bereich der Cybersicherheit der nachfolgend Aufgeführten hat massgeblich zum Gelingen dieser Sicherheitsanalyse beigetragen.

- Bundesamt für Cybersicherheit BACS
- Insel Gruppe Bern
- Zuger Kantonsspital
- Kantonsspital Winterthur
- Kantonsspital Aarau
- Kantonsspital Graubünden
- Luzerner Psychiatrie
- Clienia AG

# 1 Einleitung

Das Nationale Testinstitut für Cybersicherheit NTC hat drei für Schweizer Spitäler essenzielle Klinikinformationssysteme (KIS) – das zentrale Element jedes Spitals – einer umfassenden technischen Sicherheitsanalyse unterzogen. Dabei wurden in allen Systemen schwerwiegende Sicherheitslücken festgestellt, deren Behebung mittlerweile von den Herstellern in Angriff genommen wurde. Insgesamt wurden mehr als 40 mittlere bis schwere Schwachstellen identifiziert. Drei davon weisen die höchste Kritikalität auf. Die detaillierten Ergebnisse wurden den betroffenen Spitälern und Herstellern direkt mitgeteilt, um eine rasche Behebung sicherzustellen.

Die Sicherheitsüberprüfungen wurden unter realen Bedingungen in mehreren Schweizer Spitälern[1] durchgeführt. Um die Unabhängigkeit und Neutralität zu gewährleisten, wurden die jeweiligen Hersteller über die Tests informiert, waren aber weder an der Durchführung noch an der Finanzierung beteiligt. Die Überprüfung erfolgte auf Initiative und mit Ressourcen des Nationalen Testinstituts für Cybersicherheit NTC. Die beteiligten Spitäler haben die Überprüfung organisatorisch unterstützt und sich punktuell an den Kosten beteiligt.

Die zentralen Erkenntnisse der Analyse sind in diesem zusammenfassenden Bericht dargestellt:

- Das Kapitel **«Ausgangslage und Vorgehen»** diskutiert die Wichtigkeit von Cybersicherheits-Überprüfungen in der Gesundheitsbranche, führt Gründe auf, warum Prüfungen bislang nur selten durchgeführt werden, und wie das NTC in dieser Überprüfung vorgegangen ist.
- Das Kapitel **«Zusammenfassende Einschätzung»** gibt einen Überblick über die wichtigsten Erkenntnisse, ohne jedoch konkrete Schwachstellen offenzulegen.
- Das abschliessende und bedeutendste Kapitel, **«Empfehlungen»**, enthält acht zentrale Handlungsempfehlungen, die Verantwortlichen in Schweizer Spitälern aufzeigen sollen, wie sie die Cybersicherheit mit angemessenem Aufwand nachhaltig verbessern können.

[1] *Spitäler* wird in diesem Bericht zusammenfassend für Schweizer Spitäler, Psychiatrien und Rehakliniken verwendet.

# 2 Ausgangslage und Vorgehen

Klinikinformationssysteme (KIS) sind zentrale Plattformen, die den Informationsfluss und die organisatorischen Abläufe in einem Spital steuern. Sie verarbeiten sensible Patientendaten wie Diagnosen, Behandlungspläne und Laborergebnisse und sind für die Kommunikation und die Zusammenarbeit zwischen den Abteilungen unerlässlich. Ein Ausfall des KIS würde sowohl die medizinische Versorgung als auch die organisatorischen Abläufe massiv beeinträchtigen. Das KIS ist somit das Herzstück eines jeden Spitals.

In der Schweiz kommen im Wesentlichen drei bis fünf KIS-Lösungen zum Einsatz. Diese sind speziell auf die Anforderungen und Besonderheiten des schweizerischen Gesundheitswesens zugeschnitten und werden von nahezu allen grösseren Schweizer Spitälern eingesetzt.

Gespräche mit verschiedenen Spitälern haben ergeben, dass trotz der Kritikalität dieser Systeme nur selten Sicherheitsüberprüfungen durchgeführt werden. Die Gründe dafür sind vielfältig und reichen vom hohen Spardruck im Gesundheitswesen über ein mangelndes Bewusstsein für IT-Sicherheit bis hin zu unklaren Verantwortlichkeiten.

Das Nationale Testinstitut für Cybersicherheit NTC hat deshalb eine umfassende technische Sicherheitsüberprüfung durchgeführt. Dazu hat es eigene Ressourcen eingesetzt und mit zahlreichen Organisationen der Gesundheitsbranche zusammengearbeitet, insbesondere mit besonders engagierten im Bereich der Cybersicherheit. Über den Zeitraum von rund einem Jahr hat das NTC die folgenden drei, in der Schweiz weit verbreiteten Klinikinformationssysteme überprüft:

- KISIM von Cistec: Eine ursprünglich am Universitätsspital Zürich entwickelte Anwendung, die heute in rund 30 mittleren und grossen Spitälern vorwiegend in der Deutschschweiz eingesetzt wird. Die in Zürich domizilierte Herstellerfirma Cistec beschäftigt über 200 Mitarbeitende und zählt ausschliesslich Schweizer Spitäler zu ihren Kunden. Damit liegt der Fokus der Firma klar auf den spezifischen Anforderungen der Schweiz.
- inesKIS von ines: inesKIS wird vor allem in mittleren und kleineren Einrichtungen eingesetzt. Obwohl der Hersteller seinen Sitz in Deutschland hat, liegt der Fokus klar auf dem Schweizer Gesundheitswesen. Ines bedient rund 30 Kunden, die alle aus dem Schweizer Gesundheitswesen stammen.
- Epic: Die umfassende Anwendung wird weltweit in über 2'000 Spitälern eingesetzt, davon über 100 in Europa. In der Schweiz setzen bisher nur das Luzerner Kantonsspital und seit kurzem die Insel Gruppe in Bern das Klinikinformationssystem des US-amerikanischen Herstellers ein. Das Interesse weiterer, vor allem grösserer Spitäler ist jedoch gross. Es ist zu erwarten, dass in den nächsten Jahren weitere Schweizer Spitäler auf Epic umstellen werden.

Die Sicherheitsüberprüfungen wurden unter realen Bedingungen in mehreren Schweizer Spitälern durchgeführt. Um die Unabhängigkeit und Neutralität zu gewährleisten, wurden die jeweiligen Hersteller über die Tests informiert, waren aber weder an der Durchführung noch an der Finanzierung beteiligt. Die Überprüfung erfolgte auf Initiative und mit Ressourcen des Nationalen Testinstituts für Cybersicherheit NTC. Die beteiligten Spitäler haben die Überprüfung organisatorisch unterstützt und sich, wie im Beispiel der Berner Insel Gruppe, an den Kosten beteiligt.

# 3 Zusammenfassende Einschätzung

Die Ergebnisse zeigen, dass Überprüfungen der Cybersicherheit dringend notwendig sind. In jedem der untersuchten Systeme wurden schwerwiegende Schwachstellen identifiziert, wobei einige deutlich stärker betroffen sind als andere. Insgesamt wurden mehr als 40 mittlere bis schwere Schwachstellen identifiziert. Drei davon weisen die höchste Kritikalität auf. Besonders anfällig sind Lösungen, die noch auf veralteten Zwei-Schichten-Architekturen basieren, also solche mit einem sogenannten "Fat Client", in dem ein Grossteil der Anwendungslogik abgebildet ist. Viele der gefundenen Schwachstellen sind derart offensichtlich und leicht auszunutzen, dass sie innerhalb weniger Stunden nach Testbeginn die vollständige Kontrolle über das KIS und die darin enthaltenen Patientendaten ermöglichten. Es wurden im Wesentlichen vier zentrale Problembereiche identifiziert:

- grundlegende Architekturprobleme
- fehlende oder nicht ordnungsgemäss umgesetzte Verschlüsselung der Kommunikation zwischen beteiligten Systemen
- verwundbare Umsysteme
- unzureichende Trennung von Test- und Produktionsumgebungen

Während der Durchführung der Sicherheitsüberprüfungen erhärtete sich die Vermutung, dass insgesamt zu wenig technische Analysen im Gesundheitswesen durchgeführt werden. Viele der identifizierten Schwachstellen fallen in die Kategorie derer, die bei üblichen Sicherheitsprüfungen unmittelbar auffällig sind. Zwar wurden in der Vergangenheit vereinzelt Sicherheitsanalysen durch externe Spezialisten durchgeführt, und es lassen sich signifikante Unterschiede zwischen den Organisationen feststellen die solche Überprüfungen durchgeführt und entsprechende Massnahmen umgesetzt haben, und solche, die dies noch nicht getan haben. Wurden Sicherheitsanalysen durchgeführt, so fanden diese oft unter strengen Geheimhaltungsvereinbarungen mit den Herstellern statt. Dadurch blieben Schwachstellen teilweise unter Verschluss, konnten nicht mit anderen Betroffenen geteilt werden und wurden von einigen Herstellern nicht oder nur zögerlich behoben.

Auch im Verlauf des vorliegenden Projektes haben einzelne Hersteller das NTC und die beteiligten Spitäler aufgefordert, solche Geheimhaltungsvereinbarungen zu unterzeichnen. Diese hätten eine Warnung der Betroffenen, eine offene Diskussion oder die Veröffentlichung von Berichten wie dem vorliegenden verhindert. Das NTC lehnt solche Vereinbarungen konsequent ab, wenn sie nicht dem Schutz der Patientendaten, sondern ausschliesslich der Interessen der Hersteller dienen. Ein besonderer Dank gilt den beteiligten Spitälern, die diese Haltung engagiert mitgetragen haben.

Die meisten relevanten Schwachstellen wurden inzwischen behoben oder durch mitigierende Massnahmen entschärft. Einige grundlegende Probleme lassen sich jedoch nur durch eine komplette Änderung der Softwarearchitektur lösen, was den Herstellern zufolge mehrere Jahre dauern dürfte. Dieser Schritt ist für die Hersteller aufwändig, teuer und daher wenig attraktiv. Umso wichtiger ist es, dass die Spitäler als Kunden darüber informiert sind und auf eine rasche Umsetzung hinwirken. Alle Hersteller haben erkannt, dass eine Architektur, welche die Sicherheit von Anfang an berücksichtigt, unabdingbar ist. Während einige Hersteller diesen Wandel frühzeitig eingeleitet haben und bereits weit fortgeschritten sind, stehen andere noch am Anfang.

Erwähnenswert ist zudem, dass im Rahmen der Überprüfung kritische Schwachstellen auch in den verschiedenen Umsystemen identifiziert wurden. Obwohl diese Systeme nicht Teil des Prüfungsumfangs waren, konnten die Schwachstellen als Zufallsfund leicht

festgestellt werden, da sie kaum zu übersehen waren. Diese Feststellungen machen deutlich, dass Cybersicherheitsüberprüfungen auch in Zukunft und auch abseits von Klinikinformationssystemen dringend erforderlich sind.

Auffallend ist, dass einige Hersteller sich schwer damit tun, ihre Kunden transparent und zeitnah über festgestellte Schwachstellen zu informieren. In einem Fall verging fast ein Jahr zwischen der ersten Mitteilung an den Hersteller und der offiziellen Information der Kunden, die erst auf wiederholtes Drängen des NTC und der Spitäler erfolgte.

Zusätzlich zur Information durch die Hersteller erfolgte eine allgemeine Information über den öffentlichen NTC Vulnerability Hub[2] und eine Benachrichtigung durch das Bundesamt für Cybersicherheit (BACS) an die Spitäler via Cyber Security Hub (CSH).». Über letztgenannten offiziellen, etablierten und vertraulichen Kanal wurden weitere technische Details zur Verfügung gestellt, die den Spitälern eine genauere Einschätzung der Kritikalität sowie die Auswahl geeigneter Schutzmassnahmen ermöglichten.

Wie eingangs erwähnt, wird in diesem öffentlichen Bericht bewusst darauf verzichtet, Details zu den festgestellten Schwachstellen zu nennen. Diese wurden den betroffenen Herstellern und Spitälern zur Verfügung gestellt und für die Umsetzung entsprechender Schutzmassnahmen genutzt.

Die Ergebnisse und Erfahrungen dieser Analyse decken sich mit denen ähnlicher Initiativen. Das NTC steht im Austausch mit dem Fraunhofer-Institut für Sichere Informationstechnologie, welches in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine vergleichbare Analyse in Deutschland durchführt. Das SiKIS-Projekt[3] untersucht ebenfalls mehrere in Deutschland verbreitete Krankenhausinformationssysteme und die derzeit unveröffentlichten Ergebnisse sind ähnlich. Aus Sicht des NTC scheint es sich hierbei um branchenübliche Probleme zu handeln. Sie deuten sowohl auf ein mangelndes Bewusstsein für Cybersicherheit bei den Herstellern als auch auf unzureichende Kontrollen durch die Spitäler hin.

[2] https://hub.ntc.swiss/?term=Hospital+Information+System&area=3
[3] https://www.sit.fraunhofer.de/de/sikis/

# 4 Empfehlungen

Aus den Ergebnissen der Überprüfung lassen sich die folgenden technischen und organisatorischen Empfehlungen für die Cybersicherheitsverantwortlichen in den Spitälern ableiten:

- **Einforderung und Kontrolle der Cybersicherheit bereits bei der Beschaffung**

  Bereits bei der Beschaffung von neuen Anwendungen und IT-Infrastrukturen sollten verbindliche und klar formulierte Anforderungen an die Cybersicherheit gestellt und kontrolliert werden. Als Grundlage können beispielsweise der Leitfaden «IT-Grundschutzanforderungen für Systeme» von H+[4] oder die Checkliste «Minimal Viable Secure Product»[5] verwendet werden. Bei komplexen Beschaffungen, z.B. von Klinikinformationssystemen, empfiehlt sich zusätzlich der Beizug von Cybersicherheitsspezialisten.

- **Regelmässige Überprüfung auf Schwachstellen**

  Schwachstellenanalysen sollten regelmässig durchgeführt werden. Sowohl bei der Erstinbetriebnahme als auch periodisch oder bei grösseren Anpassungen. Dies gilt insbesondere für öffentlich zugängliche Systeme, aber auch für weniger exponierte interne Systeme, wie dies in der Regel bei KIS der Fall ist. Je nach Kritikalität der Anwendung und den zur Verfügung stehenden Ressourcen können die Überprüfungen in Form von Penetrationstests, Bug Bounty Programmen, automatisierten Scans oder idealerweise einer Kombination dieser durchgeführt werden.

  Zusätzlich empfehlen wir, eine Vulnerability Disclosure Policy und eine «security.txt» Informationsdatei[6] auf der Website zu veröffentlichen. Dies erleichtert die Entgegennahme von wertvollen Schwachstellenmeldungen von ethischen Hackern.

- **Regelmässige Updates**

  Die von den Herstellern zur Verfügung gestellten Updates sollten regelmässig und zeitnah installiert werden. Dies gilt insbesondere für die untersuchten KIS, aber auch generell bei allen sicherheitsrelevanten Updates. In Spitälern, die in der Regel rund um die Uhr in Betrieb sind und hohe Anforderungen an die Verfügbarkeit erfüllen müssen, ist dies eine besonders anspruchsvolle Aufgabe. Sie ist aber entscheidend, da ein Grossteil der bekannten Schwachstellen durch das zeitnahe Einspielen von Updates behoben werden kann. Dies betrifft nicht nur kritische Anwendungen wie KIS oder Windows-Clients, sondern auch die stetig wachsende Zahl vernetzter Geräte, im Spitalumfeld auch Internet of Medical Things (IoMT) genannt.

  Idealerweise sollten Updates erst nach der Prüfung ihrer Kompatibilität und

[4] Der Leitfaden "IT-Grundschutzanforderungen für Systeme" ist zum Zeitpunkt der Veröffentlichung dieses Berichts noch nicht publiziert, wird aber bereits in vielen Spitälern eingesetzt. Das Vorgängerdokument ist der Leitfaden «Anforderungen zur ICT-Sicherheit von Fremdsystemen», der hier heruntergeladen werden kann:
https://www.hplus.ch/fileadmin/hplus.ch/public/Politik/Cyber_Security/Leitfaden_Cyber_Security_D.pdf
[5] https://mvsp.dev/
[6] https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/security-txt.html

Schwachstellenfreiheit flächendeckend eingespielt werden. Allfällige Fehler der Hersteller sowie spezifische Unverträglichkeiten können auf diese Weise erkannt werden, was das Ausfallrisiko weiter reduziert. Eine organisationsübergreifende Zusammenarbeit unter Einbezug unabhängiger Prüfinstitute kann Synergien schaffen und somit Kosten senken und spürbaren Mehrwert fördern.

- **Trennung der produktiven Umgebung von Testumgebungen und Patienten-Netzwerk**

  Die produktive IT-Umgebung, in der Patientendaten verarbeitet werden, sollte strikt isoliert sein. Sie sollte sowohl auf System- als auch auf Netzwerkebene klar von anderen Umgebungen wie Testumgebungen, Abnahmesystemen und vor allem von Netzwerken für Gäste und Patienten getrennt sein. Es ist essenziell, dass Gäste und Patienten keinerlei Zugriffsmöglichkeiten auf die produktive IT-Umgebung erhalten. Diese Trennung verhindert zwar nicht Schwachstellen an sich, reduziert aber die Angriffsfläche und damit das Risiko, dass Schwachstellen ausgenutzt werden. Dies ist besonders wichtig im Gesundheitswesen und vor allem in Spitälern, wo die Überprüfung gezeigt hat, dass zahlreiche Schwachstellen existieren.

- **Bündelung der Kräfte und Austausch mit der Branche**

  Schweizer Spitäler stehen oft vor ähnlichen Herausforderungen, gerade im Bereich der Cybersicherheit. Ein regelmässiger Austausch ist deshalb empfehlenswert. Es gibt bereits etablierte Erfahrungsaustauschgruppen (ERFA) und Arbeitsgruppen, denen Verantwortliche auf Einladung beitreten können. Die Kontaktaufnahme geschieht idealerweise über bestehende Mitglieder (in der Regel der CISO oder der IT-Verantwortliche von grösseren Spitälern).

  Solche Gruppen bieten nicht nur eine Plattform für den Wissens- und Erfahrungsaustausch, sondern ermöglichen auch die gemeinsame Bewältigung von Aufgaben. Beispielsweise kann eine geeinte Gruppe von Spitälern einen stärkeren Einfluss auf die Hersteller ausüben, um der Implementierung sicherheitsrelevanter Funktionalitäten eine höhere Priorität einzuräumen. Genau dies wurde im Rahmen dieses Projektes von mehreren Spitälern erfolgreich erreicht. Darüber hinaus können Kosten und Ressourcen durch gemeinsame Projekte geteilt werden. So kann beispielsweise eine Sicherheitsanalyse einer Standardanwendung, die von vielen Spitälern genutzt wird, im Verbund in Auftrag gegeben werden, wobei die Ergebnisse allen beteiligten Organisationen zugutekommen.

- **Cybersicherheitsspezialisten in den Spitälern**

  Die Verantwortlichkeiten in Bezug auf den Schutz der Vertraulichkeit von Patientendaten und die Sicherstellung der IT-Verfügbarkeit sollten klar definiert sein. Dafür müssen ausreichende personelle und finanzielle Ressourcen bereitgestellt werden. Im Austausch mit den Spitälern wurde deutlich, dass in vielen, vor allem kleineren Spitälern die Verantwortlichkeiten für die Cybersicherheit nicht klar geregelt sind und oft die notwendigen Ressourcen fehlen. Dies ist angesichts der fortschreitenden Digitalisierung im Gesundheitswesen ein ernstzunehmendes Problem.

- **Bezug von wichtigen Informationen über den Cyber Security Hub vom BACS**

  Die für die Cybersicherheit verantwortlichen Personen in den Spitälern sollten Zugang zum Cyber Security Hub (CSH) haben. Der CSH ist ein zentrales Informationssystem des Bundesamtes für Cybersicherheit (BACS). Es dient als Instrument für den Austausch und das Management von Informationen über Cyberbedrohungen, Cybervorfälle und Cybersicherheitspraktiken. So wurden auch in diesem Fall relevante Informationen zu den identifizierten Schwachstellen über den CSH an die Spitäler verteilt. Dies ermöglicht eine korrekte Einschätzung der Kritikalität und die Auswahl geeigneter Massnahmen.

  Der Zugang zum CSH ist kostenlos und kann über den folgenden Link beantragt werden: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/informationen-csh.html

- **Ablehnung einseitiger Geheimhaltungserklärungen zugunsten der Hersteller**

  Geheimhaltungsvereinbarungen sollten nicht unterzeichnet werden, wenn sie nicht dem Schutz der Patientendaten dienen, sondern einseitig die Interessen der Hersteller wahren. Es sind Fälle bekannt, in denen Spitäler solche Vereinbarungen eingegangen sind und in der Folge weder andere Spitäler, selbst innerhalb desselben Kantons und derselben Trägerschaft, noch die zuständigen Behörden über entdeckte Schwachstellen informieren durften. Solche Einschränkungen behindern eine offene und konstruktive Diskussion zur Verbesserung der Cybersicherheit.