National Test Institute for Cybersecurity

Cybersecurity of Hospital Information Systems

Summary Report with Recommendations for the Swiss Health System

Version	1.0
Date	23 January 2025
Classification	Public
Authors	Tobias Castagna, Andreas Leisibach, Dilip Many, Fabio Zuber, Patrik Fabian, Raphael M. Reischuk
Responsible	Tobias Castagna

Table of contents

Acknowledgements

We would like to thank all the organizations and experts who provided us with important insights into the Swiss healthcare system. The outstanding commitment to cybersecurity of the organizations listed below has contributed significantly to the success of this security analysis.

- National Cyber Security Centre NCSC
- Insel Gruppe
- Zuger Kantonsspital
- Kantonsspital Winterthur
- Kantonsspital Aarau
- Kantonsspital Graubünden
- Luzerner Psychiatrie
- Clienia AG

1 Introduction

The National Test Institute for Cybersecurity NTC has conducted a comprehensive technical security analysis of three hospital information systems (HIS) that are essential to Swiss hospitals. In fact, HIS are the central element of every hospital. During the security analysis, serious vulnerabilities were identified in all systems, which vendors have now started to address. In total, more than 40 medium to severe vulnerabilities were identified. Three of these are of the highest criticality. The detailed results have been communicated directly to the affected hospitals and vendors to ensure they are remediated quickly.

The security assessments were carried out under realistic conditions in several Swiss hospitals[1]. In order to ensure independence and neutrality, the respective vendors were informed about the tests, but were not involved in its execution or funding. The testing was carried out on the initiative and with the resources of the National Test Institute for Cybersecurity NTC. The participating hospitals provided organizational support for the assessment and contributed to some of the costs.

The key findings of the analysis are presented in this summary report:

- The chapter **"Initial Situation and Approach"** discusses the importance of cybersecurity assessments in the healthcare industry, presents reasons why they are rarely conducted to date, and explains how the NTC approached this technical analysis.
- The chapter **"Assessment Summary"** provides an overview of the main findings without disclosing specific vulnerabilities.
- The final and most important chapter, **"Recommendations"**, contains eight key recommendations for action, which are intended to guide people in charge at Swiss hospitals on how they can improve cybersecurity effectively with reasonable effort.

[1] *Hospitals* is used in this report to summarize Swiss hospitals, psychiatric clinics and rehabilitation clinics.

2 Initial Situation and Approach

Hospital Information Systems (HIS) are central platforms that control the flow of information and organizational processes in a hospital. They handle sensitive patient data such as diagnoses, treatment plans and laboratory results, and are essential for communication and collaboration between departments. A failure of the HIS would have a massive impact on both medical care and organizational processes. The HIS is therefore at the heart of every hospital.

In Switzerland, there are essentially three to five HIS solutions in use. These are specifically tailored to the needs and characteristics of the Swiss healthcare system and are used by almost all major Swiss hospitals.

Discussions with various hospitals have shown that despite the criticality of these systems, cybersecurity assessments are rarely carried out. There are many reasons for this, ranging from the intense pressure to cut costs in the healthcare sector to a lack of awareness of IT security and unclear responsibilities.

The National Test Institute for Cybersecurity NTC therefore conducted a comprehensive technical security assessment. It used its own resources and collaborated with numerous organizations in the healthcare sector, especially those that are particularly engaged in the field of cybersecurity. Over a period of approximately one year, the NTC tested the following three hospital information systems that are widely used in Switzerland:

- KISIM by Cistec: An application originally developed at the University Hospital of Zurich that is now used in around 30 medium and large hospitals, mainly in the German-speaking part of Switzerland. Based in Zurich, the vendor Cistec employs over 200 individuals and its customers are exclusively Swiss hospitals. The company's focus is therefore clearly on the specific requirements of Switzerland.
- inesKIS from ines: inesKIS is mainly used in medium-sized and smaller institutions. Although the vendor is based in Germany, the focus is clearly on the Swiss healthcare sector. ines has around 30 customers, all in the Swiss healthcare sector.
- Epic: The comprehensive application is used in more than 2,000 hospitals worldwide, including more than 100 in Europe. In Switzerland, only the Luzerner Kantonsspital and, more recently, the Insel Gruppe in Berne use the American vendor's hospital information system. However, other hospitals, especially larger ones, seem to show interest. It is to be expected that more Swiss hospitals will switch to Epic in the next few years.

The security assessments were conducted under realistic conditions in several Swiss hospitals. To ensure independence and neutrality, the vendors were informed about the tests but were not involved in their execution or funding. The tests were carried out on the initiative and with the resources of the National Test Institute for Cybersecurity NTC. The participating hospitals provided organizational support for the tests and, as in the example of Insel Gruppe in Berne, contributed to the costs.

3 Assessment Summary

The results show that cybersecurity assessments are urgently needed. Severe vulnerabilities were found in each of the systems analyzed, with some systems being significantly more affected than others. In total, more than 40 medium to severe vulnerabilities were identified. Three of these are of the highest criticality. Especially vulnerable are solutions that are still based on outdated two-tier architectures: In other words, a solutions with a "fat client", which implements much of the application logic. Many of the vulnerabilities found are so obvious and easy to exploit that complete control of the HIS and the patient data it contains was possible within hours of starting the tests. Four main areas of concern were identified:

- Basic architectural problems
- Missing or improperly implemented encryption of communication between the systems involved
- Vulnerable surrounding systems
- Insufficient separation of test and production environments

The security assessments confirmed the suspicion that there is not enough technical analysis being carried out in the healthcare sector. Many of the vulnerabilities identified fall into the category of those that are immediately apparent in standard security assessments. Although security analyses have occasionally been carried out by external specialists in the past, there are significant differences between organizations that have conducted such reviews and implemented appropriate measures and those that have not. Where security assessments have been carried out, it has often been under strict confidentiality agreements with vendors. As a result, vulnerabilities were sometimes kept under secrecy, could not be shared with other affected parties, and were not, or only slowly, addressed by some vendors.

During this project, some vendors also asked the NTC and participating hospitals to sign such non-disclosure agreements. Such agreements would have prevented the warning of patients, an open discussion, and the publication of reports such as this one. The NTC consistently rejects such agreements if they do not serve the protection of patient data, but only the interests of the vendors. The participating hospitals are deserving of recognition for their dedication to this open approach.

While most relevant vulnerabilities have now been addressed through patches or mitigations, certain fundamental issues require a more comprehensive approach, namely a complete change to the software architecture. This is a process that, according to the vendors, is likely to take several years. This step is time-consuming and expensive, and consequently not very appealing to vendors. Therefore, it is even more important that hospitals – in their role as customers – are informed and advocate for rapid implementation. It is acknowledged by all vendors that an architecture which incorporates security considerations from the start is imperative. Some vendors have been proactive in transitioning and are now quite far along, while others are still in the initial stages.

It is also worth noting that the assessment identified critical vulnerabilities in the various surrounding systems. Although these systems were not part of the assessment scope, the vulnerabilities were detected by coincidence, as they could hardly be overlooked. These findings highlight the need for holistic cybersecurity assessments – including surrounding systems - in the future.

It is striking that some vendors are reluctant to provide transparent and timely

information to their customers about identified vulnerabilities. In one case, almost a year passed between the initial notification to the vendor and the official notification to customers, which was only made after repeated urging by the NTC and the hospitals.

In addition to the information provided by the vendors, general information was made available via the public NTC Vulnerability Hub[2] and a notification by the National Cyber Security Centre (NCSC) via the Cyber Security Hub (CSH). This official, established and confidential channel provides further technical details that enables the hospitals to better assess the criticality and select appropriate protective measures.

As aforementioned, this public report deliberately avoids providing details about the identified vulnerabilities. These have been made available to the affected vendors and hospitals and have been used to implement appropriate protective measures.

The results and experiences of this analysis are in line with those of similar initiatives. The NTC is in contact with the Fraunhofer Institute for Secure Information Technology SIT, which is conducting a similar analysis in Germany in collaboration with the German Federal Office for Information Security (BSI). The SiKIS project[3] is also assessing several common hospital information systems in Germany. The results, which have not yet been published, demonstrate a similar pattern. From the NTC's perspective, these results suggest the presence of industry-wide problems. It is an indication for both a lack of cybersecurity awareness on the part of vendors and inadequate controls by hospitals.

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

4 Recommendations

The following technical and organizational recommendations can be drawn from the results of the review for those responsible for cybersecurity in hospitals.

- **Demanding and assessing cybersecurity at the procurement stage**

  When procuring new applications and IT infrastructures, binding and clearly formulated cybersecurity requirements should be defined and monitored. The guide 'IT-Grundschutzanforderungen für Systeme' from H+[4] (available in German and French) or the checklist 'Minimal Viable Secure Product'[5] (available in English) can be used as a basis. For complex procurements, such as hospital information systems, the involvement of cybersecurity specialists is also recommended.

- **Regular vulnerability assessments**

  Vulnerability assessments should be performed regularly, both when a system is first implemented and periodically thereafter, as well as when major changes are made. This applies particularly to publicly accessible systems, but also to less exposed internal systems such as this is typically the case with HIS. Depending on the criticality of the application and the resources available, the assessments may be carried out in the form of penetration tests, bug bounty programmes, automated scans or, ideally, a combination of these.

  In addition, we recommend publishing a vulnerability disclosure policy and a «security.txt» information file[6] on the website. This will make it easier to receive valuable vulnerability reports from ethical hackers.

- **Regular updates**

  The updates provided by vendors should be installed regularly and promptly. This applies to the assessed HIS, but also to all security-related updates in general. This is a particularly demanding task in hospitals, which are usually operating around the clock and must meet high availability requirements. However, it is crucial as most known vulnerabilities can be eliminated by installing updates promptly. This applies not only to critical applications such as HIS or Windows clients, but also to the growing number of connected devices, also known as the Internet of Medical Things (IoMT) in the hospital environment.

  Ideally, updates should only be fully released after compatibility and vulnerability testing. This way, any vendor errors or specific incompatibilities can be identified, further reducing the risk of failure. Cross-organizational collaboration with the inclusion of independent testing institutes can create synergies that reduce costs and promote tangible added value.

[4] The guidance document 'IT-Grundschutzanforderungen für Systeme' has not yet been published at the time of publication of this report, but is already being used in many hospitals. Its predecessor is the guide 'ICT security requirements for third-party systems', which can be downloaded here:
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/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/security-txt.html*

- **Separation of the productive environment from test environments and patient networks**

  The production environment in which patient data is processed should be strictly isolated. It should be clearly separated from other environments, such as test environments, acceptance systems and, most importantly, networks for guests and patients, both at system and network level. It is essential that guests and patients do not have access to the production IT environment. While this separation does not prevent vulnerabilities per se, it does reduce the attack surface and therefore the risk of vulnerabilities being exploited. This is particularly important in the healthcare sector, and especially in hospitals, where the assessment found numerous vulnerabilities.

- **Collaboration and exchange with industry**

  Swiss hospitals often face similar challenges, especially in cybersecurity. It is therefore advisable to exchange information on a regular basis. There are already established experience exchange groups (ERFA) and working groups that people in charge can join by invitation. Ideally, contact is made through existing members (usually the CISO or IT manager of larger hospitals).

  Such groups not only provide a platform for the exchange of knowledge and experience but also allow to join forces and carry out tasks jointly. For example, a united group of hospitals can exert greater influence on vendors to give higher priority to the implementation of security-related features. This is exactly what several hospitals have successfully achieved in this project. In addition, costs and resources can be shared through joint projects. For instance, a security analysis of a standard application, utilised by numerous hospitals, may be commissioned by the group. The results of this analysis will be of benefit to all participating organisations.

- **Cybersecurity specialists in hospitals**

  Responsibilities for protecting the confidentiality of patient data and ensuring IT availability should be clearly defined. Adequate human and financial resources must be allocated. Discussions with hospitals revealed that in many hospitals, especially smaller ones, responsibilities for cybersecurity are not clearly defined and resources are often lacking. This is a serious problem given the increasing digitisation of healthcare.

- **Obtaining important information via the NCSC Cyber Security Hub**

  Those responsible for cybersecurity in hospitals should have access to the Cyber Security Hub (CSH). The CSH is a central information system of the National Cyber Security Centre (NCSC). It serves as a tool for sharing and managing information about cyber threats, cyber incidents and cybersecurity practices. Also in this assessment, relevant information on the identified vulnerabilities was distributed to the hospitals via the CSH. This enables a correct assessment of criticality and the selection of appropriate measures.

  Access to the CSH is free of charge and can be requested via the following link: *https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/informationen-csh.html*

- **Rejection of one-sided confidentiality agreements in favour of vendors**

  Confidentiality agreements should not be signed if they do not serve to protect patient data, but rather unilaterally protect the interests of vendors. There are known cases where hospitals have entered into such agreements and were subsequently not allowed to inform other hospitals, even within the same canton and organization, or the relevant public authorities about vulnerabilities discovered. Such restrictions prevent an open and constructive discussion on how to improve cybersecurity.