Institut national de test pour la cybersécurité

Cybersécurité des systèmes d'information hospitaliers

Rapport sommaire avec recommandations pour le système de santé suisse

Version	1.0
Date	Jeudi 23 janvier 2025
Classification	Public
Auteurs	Tobias Castagna, Andreas Leisibach, Dilip Many, Fabio Zuber, Patrik Fabian, Raphael M. Reischuk
Responsable	Tobias Castagna

Sommaire

1 Introduction 3

2 Situation de départ et approche 4

3 Évaluation récapitulative 5

4 Recommandations 7

Remerciements

Nous tenons à remercier particulièrement toutes les organisations et tous les experts qui nous ont permis d'obtenir de précieuses informations sur le système de santé suisse. L'engagement exemplaire des établissements cités ci-après dans le domaine de la cybersécurité a contribué grandement à la réussite de cette analyse de sécurité.

- Office fédéral de la cybersécurité OFCS
- Insel Gruppe
- Zuger Kantonsspital
- Kantonsspital Winterthur
- Kantonsspital Aarau
- Kantonsspital Graubünden
- Luzerner Psychiatrie
- Clienia AG

1 Introduction

L'Institut national de test pour la cybersécurité NTC a procédé à une analyse de sécurité technique approfondie sur trois systèmes d'information hospitaliers (SIH), essentiels pour les hôpitaux suisses, le SIH étant l'élément pivot de tout hôpital. D'importantes failles de sécurité ont été constatées dans tous les systèmes, les fabricants ayant entre-temps commencé à les corriger. Au total, plus de 40 vulnérabilités avec des niveaux de gravité moyens à élevés ont été identifiées, dont trois présentent la criticité la plus importante. Les résultats détaillés ont été communiqués directement aux hôpitaux et aux fabricants concernés afin de garantir une correction rapide.

Les tests de sécurité ont été effectués au sein de plusieurs hôpitaux suisses dans des conditions[1] réelles. Afin de garantir l'indépendance et la neutralité, les fabricants concernés ont été informés des tests, mais n'ont pas participé à leur réalisation ni à leur financement. Le contrôle a été effectué à l'initiative et avec les ressources de l'Institut national de test pour la cybersécurité NTC. Les hôpitaux concernés ont apporté leur soutien organisationnel au contrôle et ont participé ponctuellement aux coûts.

Les principales conclusions de l'analyse sont présentées dans ce rapport de synthèse:

- Le chapitre **«Situation de départ et approche»** aborde l'importance des tests de cybersécurité dans le secteur de la santé, évoque les raisons pour lesquelles des contrôles n'ont été que rarement réalisés à ce jour et explique comment le NTC a procédé à cette vérification.
- Le chapitre **«Évaluation récapitulative»** donne un aperçu des principales conclusions sans toutefois divulguer les failles particulières.
- Le chapitre final et le plus important **«Recommandations»** comprend huit recommandations essentielles sur les mesures à prendre, destinées à montrer aux responsables des hôpitaux suisses comment améliorer durablement la cybersécurité moyennant des efforts raisonnables.

[1] Dans le présent rapport, le terme *Hôpitaux* est utilisé pour désigner les hôpitaux suisses, les cliniques psychiatriques et les cliniques de réhabilitation.

2 Situation de départ et approche

Les systèmes d'information hospitaliers (SIH) sont des plateformes centrales qui gèrent le flux d'informations et les processus organisationnels dans un hôpital. Ils traitent les données sensibles des patients, telles que les diagnostics, les plans de traitement et les résultats de laboratoire, et sont indispensables à la communication et à la collaboration entre les services. Une panne du SIH aurait des répercussions considérables tant sur les soins médicaux que sur les processus organisationnels. Le SIH constitue donc l'élément pivot de tout hôpital.

En Suisse, trois à cinq solutions SIH sont essentiellement mises en œuvre. Elles sont spécialement conçues pour répondre aux exigences et aux spécificités du système de santé suisse et sont utilisées par presque tous les grands hôpitaux suisses.

Des entretiens menés avec différents hôpitaux ont révélé que, malgré la criticité de ces systèmes, des tests de sécurité sont rarement effectués. Les raisons sont multiples: les sévères mesures d'économies imposées dans le secteur de la santé, un manque de sensibilisation à la sécurité informatique et des responsabilités mal définies.

Par conséquent, l'Institut national de test pour la cybersécurité NTC a procédé à un examen technique approfondi de la sécurité. Pour ce faire, il a utilisé ses propres ressources et a collaboré avec de nombreuses organisations du secteur de la santé, notamment celles qui sont particulièrement engagées dans le domaine de la cybersécurité. Sur une durée d'environ un an, le NTC a examiné les trois systèmes d'information hospitaliers suivants, très utilisés en Suisse:

- KISIM de Cistec: une application initialement développée à l'Hôpital universitaire de Zurich et employée aujourd'hui dans une trentaine de moyens et grands hôpitaux, principalement en Suisse alémanique. Le fabricant Cistec, domicilié à Zurich, emploie plus de 200 collaborateurs et collaboratrices et compte exclusivement des hôpitaux suisses parmi sa clientèle. L'entreprise se concentre ainsi clairement sur les exigences spécifiques de la Suisse.
- inesKIS d'ines: inesKIS est surtout utilisé dans les établissements de petite et moyenne taille. Bien que le fabricant ait son siège en Allemagne, l'accent est clairement mis sur le système de santé suisse. ines est au service d'une trentaine de clients, tous issus du secteur de la santé en Suisse.
- Epic: cette application complète est employée dans plus de 2000 hôpitaux à l'échelle mondiale, dont plus de 100 en Europe. En Suisse, seuls l'hôpital cantonal de Lucerne et, depuis peu, l'Insel Gruppe à Berne utilisent à ce jour le système d'information hospitalier du fabricant américain. L'intérêt d'autres hôpitaux, surtout de grande taille, est toutefois important. D'autres hôpitaux suisses devraient adopter Epic au cours des prochaines années.

Les tests de sécurité ont été effectués au sein de plusieurs hôpitaux suisses dans des conditions réelles. Afin de garantir l'indépendance et la neutralité, les fabricants concernés ont été informés des tests, mais n'ont pas participé à leur réalisation ni à leur financement. Le test a été effectué à l'initiative et avec les ressources de l'Institut national de test pour la cybersécurité NTC. Les hôpitaux concernés ont apporté leur soutien organisationnel au contrôle et ont participé aux coûts, comme c'est le cas pour l'Insel Gruppe à Berne.

3 Évaluation récapitulative

Les résultats révèlent que des contrôles de la cybersécurité s'imposent d'urgence. D'importantes failles ont été identifiées dans chacun des systèmes examinés, certains étant nettement plus touchés que d'autres. Au total, plus de 40 vulnérabilités avec des niveaux de gravité moyens à élevés ont été identifiées, dont trois présentent la criticité la plus importante. Les solutions qui reposent encore sur d'anciennes architectures à deux niveaux, à savoir celles qui disposent d'un «fat client» dans lequel est représentée une grande partie de la logique de l'application, sont particulièrement vulnérables. De nombreuses failles découvertes sont si flagrantes et faciles à exploiter qu'elles ont permis de prendre le contrôle total du SIH et des données de patients contenues en l'espace de quelques heures après le début des tests. Quatre points majeurs ont été identifiés:

- problèmes fondamentaux liés à l'architecture
- absence ou mise en œuvre incorrecte du cryptage des communications entre les systèmes concernés
- systèmes connexes vulnérables
- séparation insuffisante entre les environnements de test et de production

Lors de la réalisation des tests de sécurité, l'hypothèse suivante s'est confirmée: le nombre d'analyses techniques effectuées dans le secteur de la santé est insuffisant. Bon nombre des failles identifiées entrent dans la catégorie de celles qui sont immédiatement détectées lors des contrôles de sécurité habituels. Des analyses de sécurité ont néanmoins été effectuées dans des cas isolés par des spécialistes externes par le passé et des différences importantes sont constatées entre les organisations ayant procédé à de tels contrôles et mis en œuvre les mesures nécessaires et celles qui ne l'ont pas encore fait. Lorsque des analyses de sécurité ont été effectuées, elles ont souvent été menées dans le cadre d'accords de confidentialité stricts avec les fabricants. De ce fait, les failles sont parfois restées sous le boisseau, n'ont pas pu être partagées avec d'autres parties concernées et ont été corrigées par certains fabricants tardivement, voire pas du tout.

Dans le cadre du présent projet, certains fabricants ont également demandé au NTC et aux hôpitaux concernés de signer de tels accords de confidentialité. Ceux-ci auraient empêché une mise en garde des parties concernées, une discussion ouverte ou la publication de rapports comme celui-ci. Le NTC rejette systématiquement de tels accords s'ils ne visent pas à protéger les données des patients, mais servent uniquement les intérêts des fabricants. Nous remercions tout particulièrement les hôpitaux concernés qui ont soutenu cette position avec engagement.

La plupart des failles importantes ont été éliminées entre-temps ou désamorcées par des mesures d'atténuation. Cependant, la résolution de certains problèmes majeurs exige une modification complète de l'architecture logicielle, ce qui, d'après les fabricants, devrait prendre plusieurs années. Cette mesure est fastidieuse, onéreuse et, par conséquent, peu attrayante pour les fabricants. Il est donc d'autant plus important que les hôpitaux, en tant que clients, en soient informés et s'emploient à une mise en œuvre rapide. Tous les fabricants ont reconnu qu'une architecture qui prend en compte la sécurité dès le début est indispensable. Alors que certains fabricants ont entamé ce changement à un stade précoce et ont déjà bien avancé, d'autres n'en sont qu'au début.

En outre, il convient de mentionner que, dans le cadre du contrôle, des failles importantes ont également été identifiées dans les différents systèmes connexes. Bien

que ces systèmes n'entrent pas dans l'étendue du contrôle, les failles ont pu être facilement découvertes de façon fortuite car elles étaient flagrantes. Ces constatations montrent clairement que les tests de cybersécurité s'imposent d'urgence à l'avenir et même en dehors des systèmes d'information hospitaliers.

Force est de constater que certains fabricants ont du mal à informer leurs clients en toute transparence et en temps utile des failles détectées. Dans un cas, près d'un an s'est écoulé entre la première communication au fabricant et l'information officielle des clients, qui n'est intervenue qu'à la suite de demandes répétées du NTC et des hôpitaux.

En plus des informations fournies par les fabricants, une information générale a été diffusée via le NTC Vulnerability Hub public[2] et une notification a été envoyée par l'Office fédéral de la cybersécurité (OFCS) aux hôpitaux via le Cyber Security Hub (CSH). Des détails techniques supplémentaires ont été transmis via ce dernier canal officiel, reconnu et confidentiel, permettant aux hôpitaux d'évaluer plus précisément la criticité et de sélectionner des mesures de protection adéquates.

Tel qu'il est indiqué plus haut, le présent rapport public renonce délibérément à fournir des détails sur les failles constatées. Ceux-ci ont été transmis aux fabricants et aux hôpitaux concernés et utilisés pour la mise en œuvre des mesures de protection correspondantes.

Les résultats et les expériences de cette analyse se recoupent avec ceux d'initiatives similaires. Le NTC est en contact avec le Fraunhofer-Institut für Sichere Informationstechnologie, lequel réalise une analyse équivalente en Allemagne en collaboration avec le Bundesamt für Sicherheit in der Informationstechnik (BSI). Le projet SiKIS[3] se penche également sur plusieurs systèmes d'information hospitaliers répandus en Allemagne et les résultats, non publiés pour l'instant, s'avèrent similaires. D'après le NTC, il semble s'agir de problèmes courants dans le secteur, indiquant à la fois un manque de sensibilisation à la cybersécurité chez les fabricants et des contrôles insuffisants de la part des hôpitaux.

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

4 Recommandations

Les recommandations techniques et organisationnelles suivantes à l'intention des responsables de la cybersécurité au sein des hôpitaux sont établies à partir des résultats du test:

- **Exigence et contrôle de la cybersécurité dès l'acquisition**

  Des exigences obligatoires et clairement formulées en matière de cybersécurité devraient être imposées et contrôlées dès l'acquisition de nouvelles applications et infrastructures informatiques. Le guide «Exigences de base en matière de protection informatique des systèmes» de H+[4] ou la check-list «Minimal Viable Secure Product»[5] peuvent notamment servir de base. Pour les acquisitions complexes, notamment de systèmes d'information hospitaliers, il est également recommandé de faire appel à des spécialistes de la cybersécurité.

- **Vérification régulière des vulnérabilités**

  Des analyses des vulnérabilités devraient être effectuées régulièrement. Aussi bien lors de la première mise en service que sur une base régulière ou lors d'adaptations plus importantes. Cela vaut en particulier pour les systèmes accessibles au public, mais aussi pour les systèmes internes moins exposés, comme c'est généralement le cas des SIH. Selon la criticité de l'application et des ressources disponibles, les vérifications peuvent être réalisées sous forme de tests de pénétration, de programmes Bug Bounty, de scans automatisés ou, idéalement, d'une combinaison de ceux-ci.

  En outre, nous recommandons de publier une politique de divulgation des vulnérabilités et un fichier d'information «security.txt»[6] sur le site web. Cela facilite la réception des précieux rapports de vulnérabilités de la part de hackers éthiques.

- **Mises à jour régulières**

  Les mises à jour fournies par les fabricants doivent être installées régulièrement et en temps utile. Cela vaut en particulier pour les SIH soumis à des contrôles, mais aussi, de manière générale, pour toutes les mises à jour ayant une incidence sur la sécurité. Il s'agit d'une tâche particulièrement exigeante pour les hôpitaux qui fonctionnent généralement 24 heures sur 24 et qui doivent répondre à des exigences élevées en matière de disponibilité. Elle est toutefois primordiale, car bon nombre des failles connues peuvent être corrigées si les mises à jour sont déployées en temps utile. Cela ne concerne pas seulement les applications importantes telles que les SIH ou les clients Windows, mais aussi le nombre croissant d'appareils en réseau, également connus sous la dénomination Internet of Medical Things (IoMT) dans le milieu hospitalier.

[4] Le guide «Exigences de base en matière de protection informatique des systèmes» n'est pas encore rendu public au moment de la publication du présent rapport, mais est déjà utilisé dans de nombreux hôpitaux. Le document précédent est le guide intitulé «Exigences relatives à la sécurité ICT des systèmes tiers», qui peut être téléchargé ici: 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

Idéalement, les mises à jour ne devraient être déployées à grande échelle qu'après vérification de leur compatibilité et de l'absence de vulnérabilités. De cette manière, les éventuels défauts des fabricants ainsi que les incompatibilités spécifiques peuvent être détectés, réduisant encore le risque de défaillance. Une collaboration interorganisations impliquant des organismes de contrôle indépendants peut créer des synergies, réduire les coûts et promouvoir une valeur ajoutée tangible.

- **Séparation de l'environnement de production des environnements de test et du réseau de patients**

  L'environnement informatique de production dans lequel les données des patients sont traitées doit être entièrement isolé. Il doit être clairement séparé, tant au niveau du système que du réseau, des autres environnements tels que les environnements de test, des systèmes d'acceptation et en particulier des réseaux de visiteurs et de patients. Il est essentiel que les visiteurs et les patients n'aient pas accès à l'environnement informatique de production. Si elle n'empêche pas les vulnérabilités en soi, cette séparation réduit la surface d'attaque et donc le risque d'exploitation des vulnérabilités. Ceci est particulièrement important dans le secteur de la santé et notamment dans les hôpitaux, où le contrôle a révélé la présence de nombreuses vulnérabilités.

- **Regroupement des forces et échange avec le secteur**

  Les hôpitaux suisses sont souvent confrontés à des défis similaires, notamment dans le domaine de la cybersécurité. Un échange régulier est donc recommandé. Il existe déjà des groupes d'échange d'expériences (ERFA) et des groupes de travail que les responsables peuvent rejoindre sur invitation. La prise de contact se fait idéalement par l'intermédiaire des membres existants (en général le RSSI ou le responsable informatique des grands hôpitaux).

  De tels groupes offrent non seulement une plateforme d'échange de connaissances et d'expériences, mais permettent également d'accomplir des tâches de manière conjointe. Par exemple, le groupement d'hôpitaux permet d'exercer davantage d'influence sur les fabricants afin d'accorder une plus grande priorité à l'implémentation de fonctionnalités importantes pour la sécurité. C'est précisément ce que plusieurs hôpitaux sont parvenus à faire dans le cadre de ce projet. En outre, la conduite de projets communs permet de partager les coûts et les ressources. Par exemple, une analyse de sécurité d'une application standard utilisée par de nombreux hôpitaux peut faire l'objet d'une commande commune, toutes les organisations participantes bénéficiant des résultats.

- **Spécialistes de la cybersécurité dans les hôpitaux**

  Les responsabilités en matière de protection de la confidentialité des données des patients et de garantie de la disponibilité informatique doivent être clairement définies. À cet effet, des ressources humaines et financières suffisantes doivent être mises à disposition. Lors des échanges avec les hôpitaux, il est apparu clairement que dans de nombreux hôpitaux, surtout les plus petits, les responsabilités en matière de cybersécurité ne sont pas clairement définies et que les ressources nécessaires font souvent défaut. Il s'agit là d'un problème à prendre au sérieux compte tenu de l'avancée de la

dématérialisation dans le secteur de la santé.

- **Obtention d'informations importantes via le Cyber Security Hub de l'OFCS**

  Les personnes responsables de la cybersécurité dans les hôpitaux devraient avoir accès au Cyber Security Hub (CSH). Le CSH est un système d'information centralisé de l'Office fédéral de la cybersécurité (OFCS). Il fait office d'outil pour l'échange et la gestion d'informations concernant les cybermenaces, les cyberincidents et les pratiques de cybersécurité. Ainsi, dans ce cas également, des informations pertinentes sur les failles identifiées ont été diffusées aux hôpitaux via le CSH. Cela permet d'en évaluer correctement la criticité et de sélectionner les mesures adéquates.

  L'accès au CSH est gratuit et peut être demandé en cliquant sur le lien suivant: https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-it-spezialisten/informationen-csh.html

- **Refus des déclarations de confidentialité unilatérales en faveur des fabricants**

  Les accords de confidentialité ne devraient pas être signés s'ils ne servent pas à protéger les données des patients, mais préservent unilatéralement les intérêts des fabricants. Il existe des cas où des hôpitaux ont conclu de tels accords sans informer par la suite des failles découvertes, ni les autres hôpitaux, y compris au sein du même canton et de la même instance responsable, ni les autorités compétentes. De telles restrictions vont à l'encontre d'un débat ouvert et constructif pour l'amélioration de la cybersécurité.