Istituto nazionale di test per la cibersicurezza

La cibersicurezza dei sistemi di informazione clinica

Rapporto sommario con raccomandazioni per il sistema sanitario pubblico svizzero

Versione	1.0
Data	23 gennaio 2025
Classificazione	Pubblico
Autori	Tobias Castagna, Andreas Leisibach, Dilip Many, Fabio Zuber, Patrik Fabian, Raphael M. Reischuk
Responsabile	Tobias Castagna

Indice

Ringraziamenti

Un ringraziamento particolare va a tutte le organizzazioni e a tutti gli esperti che ci hanno fornito informazioni cruciali sul sistema sanitario pubblico svizzero. L'eccezionale impegno a favore della cibersicurezza da parte delle strutture di seguito elencate ha contribuito in modo significativo alla riuscita della presente analisi della sicurezza.

- Ufficio federale della cibersicurezza UFCS
- Insel Gruppe
- Zuger Kantonsspital
- Kantonsspital Winterthur
- Kantonsspital Aarau
- Kantonsspital Graubünden
- Luzerner Psychiatrie
- Clienia AG

1 Introduzione

L'Istituto nazionale di test per la cibersicurezza NTC ha sottoposto a un'ampia analisi della sicurezza tecnica tre sistemi di informazione clinica (SIC), ossia l'elemento centrale ed essenziale di ogni ospedale svizzero. L'analisi ha evidenziato lacune importanti nella sicurezza, che i produttori hanno nel frattempo iniziato a risolvere. Complessivamente sono state identificate più di 40 vulnerabilità da medie a gravi. Tre di queste presentano il livello di criticità più alto. I risultati dettagliati sono stati comunicati direttamente agli ospedali e ai produttori interessati, al fine di assicurare la loro rapida eliminazione.

I controlli di sicurezza sono stati eseguiti in condizioni reali in diversi ospedali svizzeri[1]. Per garantire l'indipendenza e la neutralità, i singoli produttori sono stati informati dei test, ma non sono stati coinvolti né nell'esecuzione né nel finanziamento. La verifica è stata condotta su iniziativa e con risorse dell'Istituto nazionale di test per la cibersicurezza NTC. Gli ospedali coinvolti hanno supportato la verifica a livello organizzativo e hanno preso parte ai costi su base selettiva.

I risultati principali dell'analisi sono presentati in questo rapporto sommario:

- Il capitolo **«Situazione iniziale e procedura»** tratta l'importanza delle verifiche sulla cibersicurezza in ambito sanitario, espone le ragioni per le quali finora i controlli sono stati eseguiti solo raramente e spiega come l'NTC ha proceduto nel controllo.
- Il capitolo **«Sintesi della valutazione»** fornisce una panoramica dei risultati più importanti, senza tuttavia evidenziare vulnerabilità concrete.
- Il capitolo conclusivo e più importante, **«Raccomandazioni»**, presenta otto raccomandazioni operative centrali che intendono mostrare ai responsabili degli ospedali svizzeri come sia possibile migliorare in modo sostenibile la cibersicurezza con uno sforzo ragionevole.

[1] Nel presente rapporto, il termine *ospedali* viene utilizzato per riassumere gli ospedali, le cliniche psichiatriche e le cliniche di riabilitazione svizzere.

2 Situazione iniziale e procedura

I sistemi di informazione clinica (SIC) sono piattaforme centrali che gestiscono il flusso di informazioni e i processi organizzativi in un ospedale. Elaborano dati sensibili dei pazienti, come diagnosi, piani terapeutici ed esiti di laboratorio, e sono indispensabili per la comunicazione e la collaborazione tra i reparti. Un'interruzione del SIC avrebbe un impatto enorme sia sull'assistenza sanitaria sia sui processi organizzativi. Pertanto, il SIC è da considerarsi il centro nevralgico di ogni ospedale.

In Svizzera trovano impiego essenzialmente da tre a cinque soluzioni di SIC, che sono adattate appositamente alle esigenze e alle peculiarità del sistema sanitario svizzero e vengono utilizzate da quasi tutti i principali ospedali del Paese.

Dai colloqui con diversi ospedali è emerso che, nonostante la criticità di questi sistemi, solo raramente vengono effettuati controlli della sicurezza. Le ragioni sono molteplici e spaziano dall'elevata pressione al risparmio nel settore sanitario alla scarsa consapevolezza in termini di sicurezza informatica fino alla mancanza di chiarezza delle responsabilità.

L'Istituto nazionale di test per la cibersicurezza NTC ha pertanto condotto un'ampia verifica della sicurezza tecnica. Per questo lavoro ha impiegato risorse proprie e ha collaborato con numerose organizzazioni del settore sanitario, soprattutto con quelle particolarmente impegnate nell'ambito della cibersicurezza. Nel corso di circa un anno l'NTC ha sottoposto a verifica i tre seguenti sistemi di informazione clinica ampiamente diffusi in Svizzera:

- KISIM di Cistec: applicazione sviluppata inizialmente nell'Ospedale universitario di Zurigo, oggi è utilizzata in circa 30 ospedali di medie e grandi dimensioni, prevalentemente nella Svizzera tedesca. Cistec, l'azienda produttrice con sede a Zurigo, impiega circa 200 collaboratrici e collaboratori e tra i suoi clienti figurano esclusivamente ospedali svizzeri. Per questo motivo l'azienda è focalizzata sulle esigenze specifiche della Svizzera.
- inesKIS di ines: inesKIS è utilizzato soprattutto in istituti medi e piccoli. Benché l'azienda produttrice abbia sede in Germania, si concentra sul sistema sanitario svizzero. ines serve circa 30 clienti, tutti appartenenti al sistema sanitario svizzero.
- Epic: questa applicazione completa è utilizzata in oltre 2000 ospedali in tutto il mondo, più di 100 dei quali in Europa. In Svizzera questo sistema di informazione clinica del produttore statunitense è utilizzato finora solo dal Luzerner Kantonsspital e recentemente dalla Insel Gruppe di Berna. Tuttavia, c'è molto interesse da parte di altri ospedali, soprattutto di grandi dimensioni. Ci si aspetta che nei prossimi anni altri ospedali svizzeri passeranno a Epic.

I controlli di sicurezza sono stati eseguiti in condizioni reali in diversi ospedali svizzeri. Per garantire l'indipendenza e la neutralità, i singoli produttori sono stati informati dei test, ma non sono stati coinvolti né nell'esecuzione né nel finanziamento. La verifica è stata condotta su iniziativa e con risorse dell'Istituto nazionale di test per la cibersicurezza NTC. Gli ospedali coinvolti hanno supportato la verifica a livello organizzativo e hanno preso parte ai costi, come ad esempio nel caso dell'Insel Gruppe di Berna.

3 Sintesi della valutazione

I risultati mostrano che i controlli della cibersicurezza sono urgentemente necessari. Sono state individuate importanti vulnerabilità in ciascuno dei sistemi analizzati, con alcuni ad esserne decisamente più interessati di altri. Complessivamente sono state identificate più di 40 vulnerabilità da medie a gravi. Tre di queste presentano il livello di criticità più alto. A essere particolarmente esposte sono le soluzioni basate ancora su architetture obsolete a due livelli, cioè quelle con un cosiddetto «fat client», in cui viene riprodotta gran parte della logica dell'applicazione. Molte delle vulnerabilità riscontrate sono talmente ovvie e facili da sfruttare che, entro poche ore dall'inizio del test, hanno consentito di assumere il pieno controllo del SIC e dei dati dei pazienti in esso contenuti. Sono stati identificati quattro ambiti problematici centrali:

- problemi di base dell'architettura
- crittografia della comunicazione tra i sistemi coinvolti assente o non implementata correttamente
- sistemi periferici vulnerabili
- separazione degli ambienti di test e di produzione insufficiente

Durante l'esecuzione dell'analisi di sicurezza è stata confermata l'ipotesi che in ambito sanitario si effettuino in generale troppo poche analisi tecniche. Molte delle vulnerabilità identificate rientrano nella categoria di quelle immediatamente individuabili durante i controlli di sicurezza standard. In singoli casi, in passato sono state effettuate analisi della sicurezza da parte di specialisti esterni, e le differenze tra le organizzazioni che le hanno eseguite e hanno adottato provvedimenti e quelle che non hanno ancora compiuto questo passo sono significative ed evidenti. Laddove si sono effettuate analisi della sicurezza, queste sono state spesso condotte nel rispetto di severi accordi di riservatezza con i produttori. Di conseguenza, alcune vulnerabilità sono rimaste celate, non sono state condivise con altre parti interessate e non sono state risolte da alcuni produttori, o lo sono state solo con esitazione.

Anche nel corso del presente progetto alcuni produttori hanno richiesto all'NTC e agli ospedali coinvolti di sottoscrivere tali accordi di riservatezza. Tali accordi avrebbero impedito di avvertire i soggetti interessati, di avviare una discussione aperta o di pubblicare rapporti come il presente. L'NTC respinge sistematicamente tali accordi se non sono finalizzati a proteggere i dati dei pazienti, ma solo gli interessi dei produttori. Un ringraziamento particolare va agli ospedali partecipanti, che hanno sostenuto con impegno questo approccio.

Nel frattempo, la maggior parte delle vulnerabilità è stata risolta o mitigata con opportuni interventi. Tuttavia, alcuni problemi di fondo possono essere risolti solo con un cambiamento completo dell'architettura software, che, a detta dei produttori, potrebbe richiedere diversi anni. Questa fase richiede tempo, è costosa e quindi non è molto allettante per i produttori. È quindi ancora più importante che gli ospedali, in quanto clienti, ne siano informati e si impegnino per una rapida attuazione. Tutti i produttori hanno riconosciuto che è indispensabile disporre di un'architettura che tenga conto della sicurezza fin dall'inizio. Mentre alcuni produttori hanno avviato questo cambiamento tempestivamente e sono già in una fase avanzata, altri sono ancora agli inizi.

Vale la pena ricordare che nell'ambito dell'analisi sono state individuate vulnerabilità importanti anche nei vari sistemi periferici. Benché questi sistemi non fossero oggetto dell'analisi, le vulnerabilità sono state facilmente identificate in circostanze fortuite, poiché era difficile non notarle. Sulla base di tali riscontri è chiaro che sarà urgente

effettuare i controlli di cibersicurezza anche in futuro e anche al di fuori dei sistemi di informazione clinica.

È inoltre saltato all'occhio che alcuni produttori hanno difficoltà a informare i propri clienti in modo trasparente e tempestivo sulle vulnerabilità individuate. In un caso è trascorso quasi un anno tra la prima comunicazione al produttore e l'inoltro ufficiale dell'informazione ai clienti, che ha avuto luogo solo dopo ripetute insistenze da parte dell'NTC e degli ospedali.

Oltre alle informazioni provenienti dai produttori, sono state fornite informazioni generali tramite l'NTC Vulnerability Hub pubblico[2] e una notifica agli ospedali tramite il Cyber Security Hub (CSH) da parte dell'Ufficio federale per la cibersicurezza (UFCS). Attraverso quest'ultimo canale ufficiale, consolidato e confidenziale sono stati messi a disposizione ulteriori dettagli tecnici che hanno permesso agli ospedali di effettuare una valutazione più precisa delle criticità e di scegliere gli interventi di protezione adeguati.

Come menzionato all'inizio, nel presente rapporto pubblico si rinuncia volutamente a fornire dettagli relativi alle vulnerabilità riscontrate. Essi sono stati resi disponibili ai produttori e agli ospedali interessati e utilizzati per l'implementazione dei relativi interventi di protezione.

I risultati e le esperienze di questa analisi sono in linea con quelli di iniziative simili. L'NTC è in contatto con il Fraunhofer-Institut für Sichere Informationstechnologie, che sta conducendo un'analisi simile in Germania in collaborazione con il Bundesamt für Sicherheit in der Informationstechnik (BSI). Anche il progetto SiKIS[3] prende in esame diversi sistemi di informazione clinica diffusi in Germania e i risultati, attualmente non pubblicati, sono simili. L'NTC ritiene che si tratti di problemi tipici del settore. Indicano sia una mancanza di consapevolezza in termini di cibersicurezza da parte dei produttori, sia l'inadeguatezza dei controlli da parte degli ospedali.

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

4 Raccomandazioni

Dai risultati dell'analisi si possono trarre le seguenti raccomandazioni tecniche e organizzative per le persone responsabili di cibersicurezza negli ospedali:

- **Esigere e controllare la cibersicurezza fin dalla fase di approvvigionamento**

  Già nella fase di approvvigionamento di nuove applicazioni e infrastrutture informatiche si dovrebbero stabilire e monitorare requisiti di cibersicurezza vincolanti e formulati chiaramente. Come base si possono prendere ad esempio le linee guida «IT-Grundschutzanforderungen für Systeme» (Requisiti di protezione di base per sistemi IT) di H+[4] o la lista di controllo «Minimal Viable Secure Product»[5]. In caso di approvvigionamento di sistemi complessi, ad es. di sistemi di informazione clinica, si raccomanda di coinvolgere anche specialisti di cibersicurezza.

- **Effettuare verifiche periodiche per rilevare eventuali vulnerabilità**

  Le analisi delle vulnerabilità dovrebbero essere effettuate con cadenza regolare, sia in occasione della prima messa in servizio sia periodicamente o dopo modifiche rilevanti. Questa regola vale in particolare per i sistemi accessibili pubblicamente, ma anche per quelli interni meno esposti, come è il caso solitamente per i SIC. A seconda della criticità dell'applicazione e delle risorse disponibili, le verifiche possono essere effettuate sotto forma di test di penetrazione, programmi di bug bounty, scansioni automatiche o, idealmente, una combinazione di questi.

  Inoltre, raccomandiamo di pubblicare sul sito web una Vulnerability Disclosure Policy e un file informativo «security.txt»[6]: in questo modo è più facile ricevere preziose segnalazioni di vulnerabilità da parte di hacker etici.

- **Eseguire aggiornamenti periodici**

  Gli aggiornamenti messi a disposizione dai produttori dovrebbero essere installati periodicamente e senza indugi. Questa raccomandazione vale soprattutto per i SIC esaminati, ma in generale anche per tutti gli aggiornamenti con rilevanza per la sicurezza. Negli ospedali, che generalmente sono operativi 24 ore su 24 e devono soddisfare severi requisiti di disponibilità, questo è un compito particolarmente impegnativo ma essenziale, dal momento che le vulnerabilità note possono in gran parte essere risolte con l'installazione tempestiva di aggiornamenti. La raccomandazione riguarda non soltanto applicazioni importanti come i SIC o i client Windows, ma anche il numero in continua crescita di dispositivi collegati in rete, noti anche con il termine di «Internet of Medical Things (IoMT)» nell'ambiente ospedaliero.

  Idealmente, gli aggiornamenti dovrebbero essere installati solo dopo averne

[4] Al momento della pubblicazione del presente rapporto le linee guida «IT-Grundschutzanforderungen für Systeme» non sono state ancora pubblicate, ma sono già in uso presso molti ospedali. Il documento precedente è rappresentato dalle linee guida «Esigenze sulla sicurezza ICT dei sistemi esterni», che può essere scaricato qui: https://www.hplus.ch/fileadmin/hplus.ch/public/Politik/Cyber_Security/Leitfaden_Cyber_Security_I.pdf

[5] https://mvsp.dev/

[6] https://www.ncsc.admin.ch/ncsc/it/home/infos-fuer/infos-unternehmen/aktuelle-themen/security-txt.html

verificato la compatibilità e l'assenza di vulnerabilità. In questo modo è possibile riconoscere eventuali errori dei produttori e incompatibilità specifiche, riducendo ulteriormente il rischio di interruzioni. La collaborazione tra organizzazioni con il coinvolgimento di istituti di verifica indipendenti può creare una sinergia in grado di ridurre i costi e promuovere un valore aggiunto tangibile.

- **Separare l'ambiente produttivo dagli ambienti di test e dalla rete dei pazienti**

  L'ambiente informatico produttivo, nel quale vengono elaborati i dati dei pazienti, dovrebbe essere assolutamente isolato e separato in maniera ben definita, sia a livello di sistema che di rete, da altri ambienti come quelli di test, i sistemi di accettazione e, soprattutto, le reti per ospiti e pazienti. È essenziale che gli ospiti e i pazienti non abbiano alcuna possibilità di accedere all'ambiente informatico produttivo. Questa separazione non impedisce di per sé le vulnerabilità, ma riduce la superficie di attacco e quindi il rischio che queste vengano sfruttate. Ciò è particolarmente importante in ambito sanitario e soprattutto negli ospedali, dove la verifica ha accertato l'esistenza di numerose vulnerabilità.

- **Unire le forze e scambiare esperienze con gli attori del settore**

  Gli ospedali svizzeri si trovano spesso a dover affrontare sfide simili proprio nell'ambito della cibersicurezza. Pertanto, si raccomanda uno scambio costante. Esistono già gruppi costituiti di scambio di esperienze (ERFA) e gruppi di lavoro ai quali i responsabili possono partecipare su invito, idealmente, dei membri esistenti (generalmente i CISO o i responsabili informatici degli ospedali più grandi).

  Tali gruppi offrono non soltanto una piattaforma per lo scambio di conoscenze ed esperienze, ma permettono anche di compiere azioni condivise. Ad esempio, un gruppo unito di ospedali può esercitare una maggiore influenza sui produttori affinché diano priorità all'implementazione di funzionalità rilevanti per la sicurezza. È esattamente ciò che è stato conseguito con successo da diversi ospedali nell'ambito del presente progetto. Inoltre, si possono ripartire i costi e le risorse attraverso progetti comuni. Ad esempio, è possibile commissionare in gruppo l'analisi della sicurezza di un'applicazione standard utilizzata da molti ospedali, in modo che i risultati vadano a beneficio di tutte le organizzazioni partecipanti.

- **Prevedere specialisti di cibersicurezza negli ospedali**

  Le responsabilità in relazione alla tutela della riservatezza dei dati dei pazienti e della garanzia della disponibilità informatica dovrebbero essere definite chiaramente. A tal fine, è necessario stanziare risorse umane e finanziarie adeguate. Nello scambio con gli ospedali è emerso chiaramente che in molte strutture, soprattutto in quelle più piccole, le responsabilità in tema di cibersicurezza non sono definite chiaramente e spesso mancano le risorse necessarie. Alla luce della crescente digitalizzazione nel settore sanitario, si tratta di un problema serio.

- **Reperire informazioni importanti dal Cyber Security Hub dell'UFCS**

  Le persone responsabili della cibersicurezza negli ospedali dovrebbero avere accesso al Cyber Security Hub (CSH). Il CSH è un sistema di informazioni centrale dell'Ufficio federale della cibersicurezza (UFCS) che funge da strumento di scambio e di gestione delle informazioni sulle ciberminacce, sui ciberincidenti e sui consigli in tema di cibersicurezza. Anche in questo caso sono state distribuite agli ospedali attraverso il CSH informazioni importanti relative alle vulnerabilità identificate. Ciò consente di valutare correttamente la criticità e la scelta degli interventi più adatti.

  L'accesso al CSH è gratuito e può essere richiesto al seguente link: https://www.ncsc.admin.ch/ncsc/it/home/infos-fuer/infos-it-spezialisten/informationen-csh.html

- **Rifiutare le dichiarazioni di riservatezza unilaterali a favore dei produttori**

  Gli accordi di riservatezza non dovrebbero essere sottoscritti se non sono finalizzati a tutelare i dati dei pazienti, bensì unilateralmente gli interessi dei produttori. Si conoscono casi in cui gli ospedali hanno sottoscritto tali accordi e come conseguenza non sono stati autorizzati a fornire informazioni sulle vulnerabilità riscontrate né ad altri ospedali, neppure all'interno dello stesso Cantone e dello stesso organo responsabile, né alle autorità competenti. Limitazioni di questo tipo ostacolano la discussione aperta e costruttiva volta a migliorare la cibersicurezza.