Profilo dell'associazione H-CSC

Stato: febbraio 2026

1 Introduzione

L' «Healthcare Cyber Security Center (H-CSC)» è un'organizzazione nazionale di cybersicurezza. Serve allo scambio di conoscenze e alla collaborazione tra le strutture sanitarie. Il suo obiettivo è sviluppare ulteriormente le capacità esistenti e creare sinergie, affinché la prevenzione, il rilevamento e il contenimento degli incidenti informatici siano rafforzati in modo sostenibile.

La partecipazione attiva e la stretta collaborazione dei membri sono al centro delle attività dell'H-CSC. Da ciò nasce una comunità di specialiste e specialisti della sicurezza delle informazioni, basata sulla fiducia reciproca, in cui gli specialisti imparano gli uni dagli altri e si impegnano insieme per la resilienza del sistema sanitario svizzero.

2 L'associazione

L'associazione senza scopo di lucro H-CSC è stata fondata il 28 agosto 2025 da 18 ospedali svizzeri, con l'obiettivo di costruire una base comune di cybersicurezza per l'intero settore sanitario.

Figura 1: Loghi dei membri fondatori

L'H-CSC è stato fondato su raccomandazione dell'Ufficio federale della cibersicurezza (UFCS) e contribuisce direttamente all'attuazione della Ciberstrategia nazionale (CSN) dell'UFCS. L'obiettivo strategico principale è garantire servizi e infrastrutture digitali sicuri, nel senso globale di riservatezza, disponibilità e integrità.

Lo statuto dell'associazione H-CSC può essere scaricato dal sito web www.h-csc.ch.

2.1 Obiettivi dell'associazione H-CSC

L'H-CSC persegue i seguenti obiettivi:

- Promuovere la collaborazione tra i team di cybersicurezza delle strutture sanitarie svizzere
- Fornire soluzioni di cybersicurezza specifiche per il settore, adeguate alle esigenze delle strutture sanitarie svizzere, comprese quelle nel campo della tecnologia medica
- Ridurre la dipendenza da fornitori esterni di soluzioni di sicurezza attraverso lo sviluppo di competenze settoriali specifiche
- Creare strutture organizzative per lo scambio continuo di informazioni sulle minacce e di best practice
- Consentire approvvigionamenti congiunti per rafforzare il potere di negoziazione e ridurre costi e oneri
- Rafforzare la cybersicurezza nelle strutture sanitarie di medie e piccole dimensioni
- Mettere a disposizione documenti e condividere esperienze con altre strutture sanitarie al fine di aumentare le competenze nel campo della cybersicurezza

2.2 Organi dell'associazione

L'associazione H-CSC si basa su un modello di governance trasparente e partecipativo che promuove orientamento strategico, efficienza operativa e partecipazione attiva dei membri.

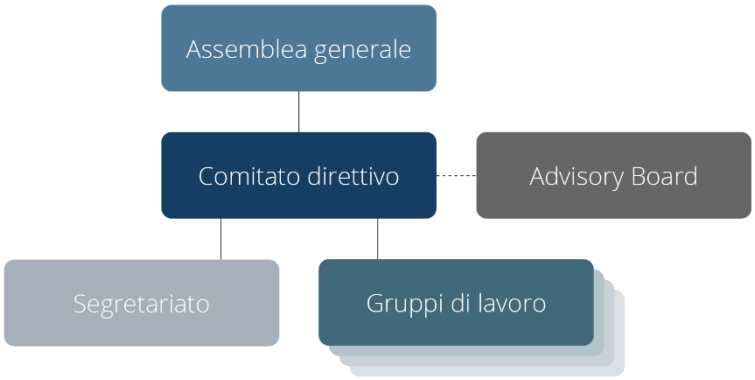

Figura 2: organi dell'associazione H-CSC

L'assemblea generale è composta dai delegati di tutte le strutture ospedaliere membri. Essa elegge il comitato direttivo, approva i risultati e decide su questioni quali l'ampliamento delle prestazioni.

Il comitato direttivo è responsabile della guida strategica. Composto da sette membri eletti, definisce lo sviluppo dell'associazione, supervisiona il segretariato e coordina il lavoro dei gruppi di esperti.

Il segretariato gestisce le attività operative quotidiane e funge da punto di coordinamento tra membri, partner e autorità. Supporta i gruppi di lavoro e garantisce il corretto svolgimento di tutte le attività organizzative.

L'Advisory Board assicura uno scambio regolare tra l'associazione H-CSC e i suoi membri. In questo organo vengono discussi i feedback sui servizi e sulle prestazioni dell'H-CSC, nonché raccolte esigenze, desideri e domande concrete dei membri.

I gruppi di lavoro sono composti da specialisti di cybersicurezza delle organizzazioni membri. Il gruppo tecnico garantisce lo sviluppo e la fornitura dei servizi tecnici dell'associazione e supporta i membri nel loro utilizzo.

2.3 Partner

Per sfruttare le sinergie ed evitare duplicazioni, l'associazione H-CSC collabora con diversi importanti partner del settore sanitario e della cybersicurezza. Attualmente i partner includono la Vereinigung Gesundheitsinformatik Schweiz (VGI.ch), l'Ufficio federale della cibersicurezza (UFCS) e Infrastructure Hôpital Suisse (IHS). Sono inoltre in corso colloqui con altri potenziali partner.

2.4 Membri

L'adesione è attualmente aperta agli ospedali e alle cliniche svizzere con mandato di prestazioni pubbliche. Tra questi figurano ospedali per cure acute, cliniche psichiatriche e cliniche di riabilitazione, come definiti dall'Ufficio federale della sanità pubblica (UFSP) e dai rispettivi Cantoni. A lungo termine, l'adesione sarà estesa a tutti gli attori del sistema sanitario svizzero al fine di creare un ecosistema nazionale uniforme e resiliente.

Per diventare membri, gli ospedali e le cliniche svizzere versano una quota associativa annuale destinata a coprire i costi dei servizi forniti. La procedura di adesione è disponibile sul sito web www.h-csc.ch. Anche il regolamento delle quote associative dell'H-CSC e l'accordo di riservatezza possono essere scaricati dal sito web.

3 Contesto della fondazione dell'H-CSC

3.1 Minacce globali

In un sistema sanitario sempre più digitalizzato, la tecnologia e i dati sono fondamentali per garantire cure efficaci. La cybersicurezza svolge un ruolo centrale nel garantire la sicurezza dei pazienti, l'efficacia dei trattamenti e la protezione dei processi sanitari, poiché gli ospedali sono sempre più presi di mira dai criminali informatici a livello mondiale.

Le strutture sanitarie rappresentano obiettivi attraenti a causa della loro dipendenza da sistemi interconnessi, dei processi critici in termini di tempo e dei rischi per la sicurezza dei pazienti. Inoltre, è in aumento l'uso di operazioni informatiche nei conflitti armati, con infrastrutture civili critiche – come gli ospedali – sempre più spesso nel mirino. Negli ultimi anni sia il settore medico sia le organizzazioni umanitarie sono stati attaccati deliberatamente, a dimostrazione della loro vulnerabilità nel contesto della moderna guerra cibernetica.

Mentre nella maggior parte delle infrastrutture critiche gli attacchi informatici con ransomware o malware mettono principalmente a rischio i dati sensibili e le infrastrutture, nel settore sanitario possono anche minacciare vite umane. Di fronte a queste minacce, è fondamentale che le strutture sanitarie svizzere rafforzino la propria resilienza informatica e siano in grado di reagire rapidamente ed efficacemente agli attacchi. A causa delle risorse limitate, la collaborazione tra le strutture sanitarie è essenziale.

3.2 Sfide in Svizzera

Limitata competenza settoriale specifica: Le linee guida generali di cybersicurezza non affrontano in modo sufficiente le minacce specifiche delle strutture sanitarie, come le vulnerabilità nei dispositivi medici certificati, la protezione di sistemi clinici critici con componenti software non più supportati o la gestione corretta di dati sensibili e fortemente regolamentati sotto costante pressione temporale (ad esempio nelle ambulanze, nei pronto soccorso o nelle unità di terapia intensiva).

Costi e oneri elevati nei processi di approvvigionamento: Per la valutazione dei sistemi e dei servizi di sicurezza IT, quasi tutte le strutture sanitarie redigono documenti di requisiti praticamente identici. In futuro tali documenti potranno essere elaborati congiuntamente tramite l'H-CSC e forniti ai membri come modelli. Ciò alleggerisce il carico dei responsabili della sicurezza, consente di risparmiare tempo e costi e migliora la qualità dei documenti, poiché permette di apprendere dagli errori degli altri.

L'associazione H-CSC affronta queste sfide e rafforza le capacità di cybersicurezza delle strutture sanitarie svizzere fornendo servizi specifici per il settore e promuovendo una collaborazione strutturata a livello dell'intero settore.

4 Servizi

L'associazione H-CSC mette a disposizione dei propri membri un'ampia gamma di servizi per supportarli nel miglioramento della loro resilienza in materia di cybersicurezza, indipendentemente dal loro attuale livello di maturità. Questi servizi sono sviluppati insieme ai membri e per i membri, per garantire che siano adattati alle esigenze specifiche del settore sanitario.

Attualmente sono disponibili 10 servizi per i membri, i cui costi sono in gran parte inclusi nella quota associativa. La maggior parte dei servizi è offerta in tedesco, francese e italiano; alcuni servizi sono disponibili solo in inglese.

Figura 3: panoramica die servizi offerti dall'H-CSC ai suoi membri

4.1 Panoramica dei servizi esistenti

- Threat intelligence collaboration & sharing: piattaforma per lo scambio sicuro e coordinato di informazioni su minacce informatiche, IoC e vulnerabilità. I membri beneficiano di una visione situazionale condivisa e di una più semplice integrazione nelle soluzioni di sicurezza esistenti.
- Threat intelligence management: accesso centrale a informazioni verificate e rilevanti per il settore sulle minacce informatiche attuali. Il servizio supporta un rilevamento più rapido e una prevenzione

efficace degli attacchi, riduce il lavoro manuale e rafforza la cyber-resilienza individuale e collettiva dei membri.

- Monitoraggio del darknet: monitoraggio continuo di fonti darknet rilevanti alla ricerca di credenziali compromesse e informazioni sensibili. I potenziali incidenti di sicurezza vengono individuati e segnalati tempestivamente, consentendo alle strutture sanitarie interessate di adottare adeguate misure di protezione e contromisure.
- Canale di scambio sui fornitori: scambio mirato di esperienze su produttori, prodotti e servizi nel campo della cybersicurezza. Nei canali dedicati, i membri condividono best practice e valutazioni basate sull'esperienza pratica.
- Linee guida per l'approvvigionamento: aggregazione dei requisiti di sicurezza dei membri per creare una forte voce comune sul mercato. La sicurezza delle informazioni viene integrata fin dalle prime fasi dei processi di approvvigionamento, contribuendo nel lungo periodo a soluzioni più sicure nel settore sanitario.
- Campagne di sensibilizzazione: raccolta centrale di campagne di sensibilizzazione consolidate provenienti dai membri, con informazioni su benefici, impegno richiesto, materiali e contatti. I membri possono individuare rapidamente approcci adeguati e ridurre il proprio lavoro preparatorio.
- Conferenza H-CSC: evento annuale dedicato al networking, allo scambio di esperienze e alla formazione continua attraverso presentazioni specialistiche e discussioni.
- Webinar mensili: scambio tecnico regolare sui servizi, sulle posizioni dell'H-CSC e su esperienze dei membri relative alla cybersicurezza nel settore sanitario.
- Gruppo di scambio ERFA sulla sicurezza delle informazioni: scambio di esperienze strutturato e riservato per i responsabili della sicurezza delle informazioni nelle strutture sanitarie, rivolto a CISO e responsabili della sicurezza IT.
- Biblioteca: raccolta centrale di modelli, linee guida e documenti di esempio provenienti dalle organizzazioni membri relativi a ISMS, protezione di base IT e sensibilizzazione.

Nota linguistica: Questo documento è disponibile in diverse versioni linguistiche. In caso di discrepanze o interpretazioni divergenti, fa fede esclusivamente la versione tedesca.