H-CSC Vereinsprofil

Stand: Februar 2026

1 Einführung

Das «Healthcare Cyber Security Center (H-CSC)» ist eine nationale Cybersicherheitsorganisation. Sie dient dem Wissensaustausch und der Zusammenarbeit zwischen Gesundheitseinrichtungen. Ihr Ziel ist es, bestehende Fähigkeiten auszubauen und Synergien zu schaffen, sodass Prävention, Erkennung und Eindämmung von Cybervorfällen nachhaltig gestärkt werden.

Die aktive Teilnahme und enge Zusammenarbeit der Mitglieder stehen im Mittelpunkt der Aktivitäten des H-CSC. Daraus wächst eine Gemeinschaft von Spezialistinnen und Spezialisten der Informationssicherheit, die auf gegenseitigem Vertrauen basiert, wo Spezilist:innen voneinander lernen und sich gemeinsam für die Resilienz des Schweizer Gesundheitswesens einsetzen.

2 Der Verein

Der gemeinnützige Verein H-CSC wurde am 28. August 2025 von 18 Schweizer Spitälern gegründet, die sich zum Ziel gesetzt haben, eine gemeinsame Cybersicherheitsbasis für den gesamten Gesundheitssektor aufzubauen.

Abbildung 1: Logos der Gründungsmitglieder

Das H-CSC wurde auf Empfehlung des Bundesamtes für Cybersicherheit (BACS) gegründet und trägt direkt zur Umsetzung der Nationalen Cybersicherheitsstrategie (NCS) des BACS bei. Dabei steht das strategische Ziel im Vordergrund, sichere digitale Dienste und Infrastrukturen im umfassenden Sinne von Vertraulichkeit, Verfügbarkeit und Integrität zu gewährleisten.

Die Statuten des Vereins H-CSC können von der Webseite www.h-csc.ch heruntergeladen werden.

2.1 Ziele des H-CSC Vereins

Das H-CSC verfolgt folgende Ziele:

- Förderung der Zusammenarbeit zwischen den Cybersicherheitsteams der Schweizer Gesundheitseinrichtungen
- Bereitstellung sektorspezifischer Cybersicherheitslösungen für die Bedürfnisse der Schweizer Gesundheitseinrichtungen, einschliesslich derjenigen im Bereich Medizintechnik
- Reduzierung der Abhängigkeit von externen Anbietern von Sicherheitslösungen durch den Aufbau sektorspezifischer Expertise
- Schaffung von organisatorischen Strukturen für den kontinuierlichen Austausch von Bedrohungsinformationen und Best Practices
- Ermöglichung gemeinsamer Beschaffungen zur Stärkung der Verhandlungsmacht und zur Senkung von Kosten und Aufwand
- Stärkung der Cybersicherheit in mittelgrossen und kleinen Gesundheitseinrichtungen
- Bereitstellung von Dokumenten und Weitergabe von Erfahrungen an andere Gesundheitseinrichtungen zur Steigerung der Kompetenz im Bereich Cybersicherheit.

2.2 Organe des Vereins

Der Verein H-CSC stützt sich auf ein transparentes und partizipatives Governance-Modell, das strategische Orientierung, operative Effizienz und aktive Beteiligung der Mitglieder fördert.

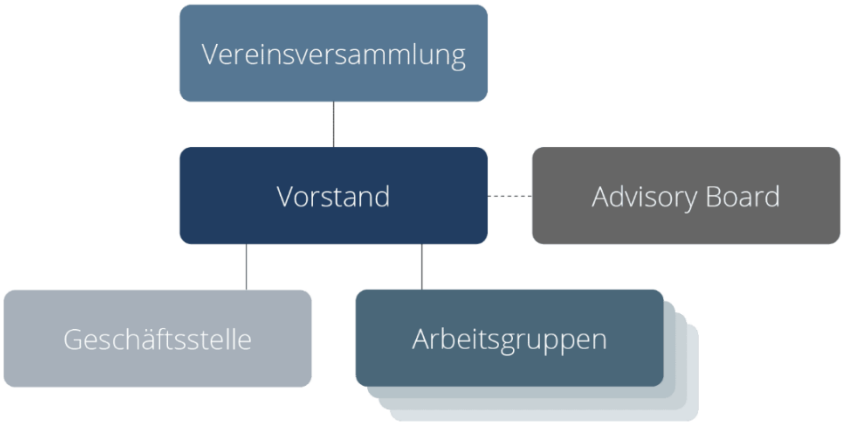

Abbildung 2: Organe des Vereins H-CSC

Die Vereinsversammlung besteht aus Delegierten aller Mitgliedsinstitutionen. Sie wählt den Vereinsvorstand, genehmigt Ergebnisse und entscheidet über Fragen wie Leistungserweiterungen.

Der Vorstand übernimmt die strategische Führung. Er besteht aus sieben gewählten Mitgliedern, legt die Entwicklung des Vereins fest, beaufsichtigt die Geschäftsstelle und koordiniert die Arbeit der Expertengruppen.

Die Geschäftsstelle führt den operativen Betrieb des Vereins und dient als Koordinationsstelle für Mitglieder, Partner und Behörden. Sie unterstützt die Expertengruppen und stellt den reibungslosen Ablauf aller organisatorischen Aktivitäten sicher.

Das Advisory Board stellt den regelmässigen Austausch zwischen dem Verein H-CSC und seinen Mitgliedern sicher. In diesem Gremium werden Rückmeldungen zur Effizienz und Effektivität von H-CSC diskutiert sowie konkrete Anliegen, Wünsche und Fragestellungen der Mitglieder aufgenommen.

Die Arbeitsgruppen bestehen aus Cybersicherheitsspezialist:innen aus den Mitgliedsorganisationen. Das Tech Team stellt die Entwicklung und Bereitstellung der technischen Services des Vereins sicher und unterstützt die Mitglieder bei deren Nutzung.

2.3 Partner

Um Synergien zu nutzen und Doppelspuigkeiten zu vermeiden, arbeitet der Verein H-CSC mit mehreren wichtigen Partnern aus dem Gesundheitssektor und der Cybersicherheitsbranche zusammen. Zu den Partnern gehören im Moment die Vereinigung Gesundheitsinformatik Schweiz (VGI.ch), das Bundesamt für Cybersicherheit (BACS) und der Infrastruktur Hospital Schweiz (IHS). Mit weiteren möglichen Partnern laufen Gespräche.

2.4 Mitglieder

Die Mitgliedschaft steht derzeit Schweizer Spitälern und Kliniken mit öffentlichem Leistungsauftrag offen. Dazu gehören Akutkliniken, psychiatrischen Kliniken und Rehabilitationskliniken, wie sie vom Bundesamt für Gesundheit (BAG) und den jeweiligen Kantonen definiert sind. Langfristig soll die Mitgliedschaft auf alle Akteure im Gesundheitswesen in der Schweiz ausgeweitet werden, damit ein einheitliches und widerstandsfähiges nationales Ökosystem entsteht.

Um Mitglied zu werden, entrichten Schweizer Spitäler und Kliniken einen jährlichen Mitgliederbeitrag für die Deckung der Kosten der zur Verfügung gestellten Services. Das Mitgliedschaftsprozess findet man auf die Webseite www.h-csc.ch. Das Beitragsreglement des Vereins H-CSC und die Geheimhaltungserklärung können ebenfalls von der Webseite heruntergeladen werden.

3 Hintergrund zur Gründung des H-CSC

3.1 Globale Bedrohungen

In einem zunehmend digitalisierten Gesundheitssystem sind Technologie und Daten entscheidend für eine Gesundheitsversorgung. Bei der Gewährleistung der Patientensicherheit, Behandlungseffektivität und beim Schutz der Abläufe im Gesundheitswesen spielt die Cybersicherheit eine zentrale Rolle, denn weltweit nehmen Cyberkriminelle zunehmend auch Gesundheitseinrichtungen ins Visier.

Gesundheitseinrichtungen sind attraktive Ziele aufgrund ihrer Abhängigkeit von vernetzten Systemen, zeitkritischen Abläufen und der Gefährdung der Patientensicherheit. Zudem steigt der Einsatz von Cyberoperationen in bewaffneten Konflikten, wobei kritische zivile Infrastrukturen – wie Gesundheitseinrichtungen – immer häufiger ins Visier geraten. In den letzten Jahren wurden sowohl der medizinische Sektor als auch humanitäre Organisationen gezielt attackiert, was ihre Verwundbarkeit als Teil moderner digitaler Kriegsführung verdeutlicht.

Während Cyberangriffe mit Ransomware oder Malware in den meisten kritischen Infrastrukturen in erster Linie sensible Daten und die Infrastruktur gefährden, können sie im Gesundheitswesen auch Menschenleben bedrohen. Angesichts dieser Bedrohungen ist es entscheidend, dass Schweizer

Gesundheitseinrichtungen ihre Cyberresilienz stärken und schnell und effektiv auf Angriffe reagieren können. Wegen den begrenzten Ressourcen ist dabei eine Zusammenarbeit zwischen den Gesundheitseinrichtungen zwingend.

3.2 Herausforderungen in der Schweiz

Begrenzte sektorspezifische Expertise: Allgemeine Cybersicherheitsrichtlinien gehen nicht ausreichend auf Bedrohungen ein, die spezifisch für Gesundheitseinrichtungen gelten. Beispielsweise Schwachstellen in zertifizierten Medizinprodukten, den Schutz medizinisch hervorragender klinischer Systeme mit nicht mehr unterstützten Softwarebestandteilen oder den korrekten Umgang mit sensiblen und stark regulierten Daten unter dauerndem Zeitdruck (z.B. im Rettungswagen, im Notfall, auf Intensivstation etc.)

Hohe Kosten und Aufwände in Beschaffungsprozessen: Zur Evaluation von IT-Sicherheitssystemen und Dienstleistungen verfassen alle Gesundheitseinrichtungen praktisch identische Anforderungsunterlagen. Solche Unterlagen können zukünftig über das H-CSC gemeinsam erstellt und den Mitgliedern als Vorlagen abgegeben werden. Dies entlastet die Sicherheitsverantwortlichen, spart Geld und Zeit und erhöht die Qualität der Dokumente, da aus den Fehlern der anderen gelernt werden kann.

Der Verein H-CSC begegnet diesen Herausforderungen und stärkt die Cybersicherheitsfähigkeiten der Schweizer Gesundheitseinrichtungen, indem er sektorspezifische Dienstleistungen bereitstellt und eine strukturierte Zusammenarbeit im gesamten Sektor fördert.

4 Services

Der Verein H-CSC stellt seinen Mitgliedern eine breite Palette an Services zur Verfügung, um sie bei der Verbesserung ihrer Cybersicherheitsresilienz zu unterstützen – unabhängig von ihrem aktuellen Reifegrad. Diese Services werden gemeinsam mit den Mitgliedern und für die Mitglieder entwickelt, um sicherzustellen, dass sie auf die spezifischen Bedürfnisse des Gesundheitssektors zugeschnitten sind.

Aktuell stehen den Mitglieder 10 Services zur Verfügung, deren Kosten mehrheitlich in den Mitgliederbeiträge enthalten sind. Die meisten Services werden auf Deutsch, Französisch und Italienisch angeboten. Gewisse Services sind nur auf Englisch verfügbar.

Abbildung 3: Übersicht der H-CSC Services

4.1 Übersicht der bestehenden Services

- Threat Intelligence Collaboration & Sharing: Plattform für den sicheren und koordinierten Austausch von Informationen zu Cyberbedrohungen, IoCs und Schwachstellen. Mitglieder profitieren von einem gemeinsamen Lagebild und einer einfacheren Integration in bestehende Sicherheitslösungen.
- Threat Intelligence Management: Zentraler Zugang zu geprüften, sektorrelevanten Informationen zu aktuellen Cyberbedrohungen. Der Service unterstützt eine schnellere Erkennung und wirksame Prävention von Angriffen. Manuelle Aufwände werden reduziert und die individuelle sowie gemeinsame Cyber-Resilienz der Mitglieder wird gestärkt.
- Darknet-Monitoring: Kontinuierliche Überwachung relevanter Darknet-Quellen auf kompromittierte Zugangsdaten und sensible Informationen. Potenzielle Sicherheitsvorfälle werden frühzeitig erkannt und gemeldet, sodass betroffene Gesundheitseinrichtungen rechtzeitig geeignete Schutz- und Gegenmassnahmen einleiten können.
- Hersteller-Austauschkanal: Gezielter Erfahrungsaustausch zu einzelnen Herstellern, Produkten und Dienstleistungen im Bereich Cybersicherheit. In dedizierten Channels teilen Mitglieder Best Practices und fundierte Einschätzungen aus der Praxis.
- Beschaffungsrichtlinien: Bündelung der Sicherheitsanforderungen der Mitglieder zur Schaffung einer starken gemeinsamen Marktstimme. Informationssicherheit wird frühzeitig in Beschaffungsprozessen berücksichtigt und trägt langfristig zu sichereren Lösungen im Gesundheitswesen bei.
- Awareness-Kampagnen: Zentrale Sammlung bewährter Awareness-Kampagnen von Mitgliedern mit Informationen zu Nutzen, Aufwand, Materialien und Kontaktpersonen. Mitglieder finden rasch passende Ansätze und reduzieren ihren eigenen Vorbereitungsaufwand.
- H-CSC Konferenz: Jährlicher Anlass für Vernetzung, Erfahrungsaustausch und Weiterbildung durch Fachvorträge und Diskussionen.
- Monatliche Webinare: Regelmässiger fachlicher Austausch zu Services, Positionen des H-CSC sowie Erfahrungsberichten von Mitgliedern rund um Cybersicherheit im Gesundheitswesen.
- ERFA-Gruppe Informationssicherheit: Strukturierter und vertraulicher Erfahrungsaustausch für Verantwortliche der Informationssicherheit in Gesundheitseinrichtungen. Die Gruppe richtet sich an CISOs und IT-Sicherheitsverantwortliche.
- Bibliothek: Zentrale Sammlung bewährter Vorlagen, Richtlinien und Beispieldokumente aus Mitgliedorganisationen zu ISMS, IT-Grundschutz und Awareness.