

Success Story

Spital Bülach

Mit einem externen CISO zu ganzheitlicher Informationssicherheit und wirkungsvollem Datenschutz

Wenn die entscheidenden Verbindungen fehlen, die aus guten Einzelteilen ein noch besseres Ganzes entstehen lassen, lohnt es sich, die Flughöhe zu ändern. Mit der Verpflichtung eines externen CISO (Corporate Information Security Officer) der Swiss Infosec AG hat das Spital Bülach im Jahr 2017 genau dies getan und sich Know-how und Unterstützung in den Bereichen Informationssicherheit und Datenschutz ins Haus geholt. Dank ganzheitlicher Betrachtungsweise und implementierter Governance, dank einem neuen Sicherheitsgremium und konsequenter, bereichsübergreifender Abstimmung der Sicherheitsmassnahmen wurde das Zusammenspiel von Informationssicherheit und Datenschutz erfolgreich verbessert.

Das Spital Bülach – das Spital für die Bevölkerung im Zürcher Unterland

Das Spital Bülach sichert die medizinische Versorgung von 180'000 Menschen im Zürcher Unterland und den angrenzenden Regionen. Jährlich werden rund 84'000 Patientinnen und Patienten stationär und ambulant behandelt und betreut. Ohne Frage steht für ein Spital die Patientensicherheit an oberster Stelle. Das Spital Bülach setzt sich dafür hohe Qualitätsziele, die regelmässig überprüft und als Qualitätsversprechen öffentlich gemacht werden. Für Sicherheitsspezialisten steht die erwähnte Patientensicherheit in engem Zusammenhang mit Informationssicherheit und Datenschutz. Die Art und Weise, wie mit Informationen umgegangen und personenbezogene Daten geschützt wird, ist von grosser Tragweite: für das Wohl der Patientinnen und Patienten genauso wie für die Reputation des Spitals.

Ganzheitliche Informationssicherheit beginnt mit ganzheitlicher Kommunikation

Um die gemeinsame Stossrichtung im Team abzustützen, verschiedene Blickwinkel einzubringen (-> ganzheitliche Betrachtungsweise!) und um sich regelmässig auszutauschen, wurde ein Gremium gebildet, die sogenannte Sicherheitsorganisation. Diese hat sich bestens bewährt und ist etabliert. Ihr gehören neben dem externen CISO der betriebliche Datenschutzverantwortliche (BSDV), der IT-Sicherheitsbeauftragte (IT-SIBE) und der Sicherheitskoordinator (SiKo) an.

Datenschutz – Wirkungsvoll und konform dank den Datenschutzspezialisten der Swiss Infosec AG

Mit der Verpflichtung des externen CISO der Swiss Infosec AG hat das Spital Bülach nicht nur einen ausgewiesenen Fachspezialisten für Informationssicherheit in seinen Reihen, sondern auch alle anderen SpezialistInnen der Swiss Infosec AG. Auf die kann der externe CISO jederzeit zurückgreifen und spezifisches Fachwissen abholen. Das ist besonders beim komplexen Thema Datenschutz ein grosser Vorteil und eine der Stärken der Swiss Infosec AG. Unter Einbezug des Data Privacy und Legal Consulting Teams der Swiss Infosec AG konnten so auch sehr anspruchsvolle Fragestellungen beantwortet werden.

Fazit: Der externe CISO erbringt im Spital Bülach eine verbindende Rolle. Seine langjährige Verpflichtung zeigt, dass der Zuzug externer Spezialisten der Swiss Infosec AG mehr als eine Übergangslösung ist.

Diagnose Informationssicherheit und Datenschutz: es geht noch ganzheitlicher

Der Wichtigkeit von Informationssicherheit, IT-Sicherheit und Datenschutz war man sich im Spital Bülach natürlich schon lange vor dem Einsatz des externen CISO bewusst. Entsprechend waren die notwendigen Strukturen und Personalressourcen vorhanden und insbesondere die IT-Sicherheit auf hohem Niveau. Nicht, dass die einzelnen Akteure ein Inseldasein fristeten, was jedoch fehlte, war der konsequent ganzheitliche Ansatz, eine verbindende und verbindliche Governance und das ausbalancierte Zusammenspiel von Informationssicherheit und Datenschutz. Ein Audit zeigte, dass dadurch die gewählten Massnahmen nicht das ganze Potential entfalten konnten. Die Diagnose – es geht noch ganzheitlicher – war klar, die Therapie auch: der Einsatz eines externen CISO der Swiss Infosec AG.

Klare Strukturen und Abläufe dank Governance

Die Erarbeitung der Governance, das Zusammenfügen und Ergänzen von Weisungen und Vorgaben war ein weiterer Schritt Richtung Ganzheitlichkeit. Prozesse wie Risikomanagement, Security Incident Management, Ausnahmen und Audits werden dabei systematisch dokumentiert und geführt. Anschliessend wurden die Weisungen und Prozesse implementiert. Auch in Sachen Mitarbeiterausbildung kann der externe CISO wertvolle Inputs und vor allem Best Practice beisteuern und so zu einer höheren Sensibilisierung beitragen.



Phillippe Waespe
IT-Leiter, Spital Bülach

«Der Einsatz des externen CISO der Swiss Infosec AG hat uns in allen Bereichen überzeugt: fachlich, interdisziplinär, menschlich. Der externe CISO hat nicht nur dafür gesorgt, dass Informationssicherheit und Datenschutz ganzheitlich betrachtet und konform umgesetzt werden, sondern dass dieser Ansatz tatsächlich Einzug in den Alltag gefunden hat.»

