

ESAMIT als Schlüssel zu KRITIS

Mathias-Stiftung Rheine stellt nach Audit IT-Sicherheit neu auf

„Für uns ist der gesamte Bereich der IT-Sicherheit, besonders was Angriffe über E-Mail-Anhänge und das Fishing betrifft, eine große Herausforderung“, beschreibt Dirk Hoffmann, IT-Leiter der Mathias-Stiftung Rheine, was ihn und seine 16 Mitarbeiter fast täglich umtreibt. „Immer mehr Systeme sind mit dem Internet verknüpft, das Arbeiten im World Wide Web ist selbstverständlich geworden. Unsere Aufgabe ist es dafür Sorge zu tragen, dass unser Netzwerk sauber und sicher bleibt.“ Allgemein genießt die IT-Sicherheit einen hohen Stellenwert in der Stiftung.

Die Mathias-Stiftung Rheine besteht aus insgesamt 50 Einrichtungen. Dazu gehören sieben Akut-Krankenhäuser, die sich über fünf Standorte verteilen, Institute, Gesundheitszentren, Fachpraxen sowie Einrichtungen der Altenhilfe und Aus- und Weiterbildung. Alle Einheiten befinden sich im Umkreis von 25 Kilometer um Rheine.

Als die Diskussion um KRITIS, also kritische Infrastrukturen, zu denen abhängig von den Fallzahlen auch Krankenhäuser gerechnet werden, aufkam, wollte Hoffmann die Arbeit seiner Abteilung von externer Seite begutachten lassen. Zusammen mit der Geschäftsleitung hat er Gespräche mit drei Firmen geführt. Die

Frage: Was können wir im Bereich KRITIS tun? Nach verschiedenen Präsentationen fiel die Entscheidung schließlich auf CETUS Consulting aus Münster. „Uns haben die tiefe Fachkenntnis und die Art, wie Frederik Vrielink die Themen angeht, sehr gut gefallen. Es war gleich ein gutes Gefühl da“, blickt Hoffmann zurück. Mit CETUS hat der IT-Leiter dann auch erstmals vom ESAMIT-Audit gehört, einer Prozessarchitektur für den medizinischen IT-Betrieb, die die Vorzüge verschiedener Normen zum IT-Servicemanagement, zum Risikomanagement und zur Informationssicherheit passgenau für Gesundheitseinrichtungen verbindet. Das war gut für die Stiftung, die sich auch unabhängig von KRITIS besser organisieren wollte.

Man merkt die große Erfahrung, die die Berater aus anderen Projekten mitbringen und die uns sehr hilft.

Dirk Hoffmann, Leiter IT

Vergleichsweise gut gestellt

Im Jahr 2015 hat CETUS dann das ESAMIT-Audit in der Mathias-Stiftung Rheine durchgeführt und den Ist-Stand der IT erhoben. An den festgestellten Schwächen sollte gemeinsam gearbeitet werden, so die Verabredung, mit dem Ziel, binnen von drei Jahren KRITIS-fähig zu sein. „Das letzte Jahr ist angebrochen, wir haben bereits sehr viele Dinge umgesetzt, die letzten sollen spätestens im Dezember abgeschlossen sein“, zieht Hoffmann ein Zwischenfazit.

Erster Teil des Audits war ein zweitägiger Workshop in Rheine. Neben Hoffmann als IT-Leiter haben daran die Leiter Medizintechnik und Haustechnik sowie Vertreter der Geschäftsleitung teilgenommen. Das Ergebnis laut Bericht: Mit einer Gesamterreichung von 42 Prozent der umsetzbaren Strukturen ist die IT-Organisation der Mathias-Stiftung im oberen Drittel der ver-

gleichbaren Krankenhäuser anzusiedeln.

Mithin ist der erreichte Reifegrad von durchschnittlich „2“ je nach betrachteter Domäne, bereits gut. Stufe 2 heißt, dass die Prozesse anhand von Ergebniskennzahlen gesteuert und gemessen werden. Diese Dimensionen sind jedoch nicht nachvollziehbar dokumentiert. Im Einzelnen bedeutet das: Es existiert eine Sicherheitspolitik, in der die Ziele des Unternehmens hinsichtlich des Informationsschutzes definiert sind. Sie ist von der Geschäftsführung unterschrieben. Die Sicherheitspolitik und Richtlinien/Regelungen zur Informationssicherheit werden jedem Mitarbeiter des Unternehmens zentral, in diesem Fall im Intranet, zur Verfügung gestellt. Für den Prozess der Erstellung und Pflege der Sicherheitspolitik und Richtlinien/Regelungen zur Informationssicherheit sind Verantwortliche benannt. Diesen Prozessverantwortlichen stehen ausreichend Ressourcen zur Verfügung. Einen großen Nutzen von ESAMIT sieht Hoffmann in der detaillierten Ausformulierung und der Vergleichbarkeit gegenüber anderen, vergleichbaren Gesundheitseinrichtungen.

Schritt für Schritt zum Ziel

Aus dem Audit hat CETUS dann einen konkreten Maßnahmenplan für die Stiftung abgeleitet. Die wesentlichen Punkte waren die Einführung eines Managementsystems für Informationssicherheit (ISMS), das Etablieren einer verzahnten und bereichsübergreifenden Service-Management Organisation gemeinsam mit technischer Abteilung und Medizintechnik, regelmäßige Schulung und eine Sensibilisierung der Mitarbeiter sowie die Einführen eines Business Continuity oder Notfallmanagements für die IT.

„Mit dem ISMS sind wir bereits weit gekommen“, sagt Hoffmann. Es ist ein Werkzeug, das alle Belange der IT-Sicherheit im Unternehmen regelt. Die Basis bildet ein Handbuch mit einem Hauptdokument und 23 Anweisungen. Dort wird beispielsweise der Umgang mit dem Outsourcing von Leistungen oder die private Nutzung mobiler Endgeräte festgelegt. „CETUS hat uns nach deren Erfahrung eine Vorlage geliefert, die wir dann diskutiert und gemeinsam nach unseren individuellen Erfordernissen angepasst und finalisiert haben“, beschreibt der IT-Leiter den Prozess.

Ein offener Punkt ist noch die Beschreibung einer verzahnten IT-Organisation. Zentraler Aspekt dabei ist der Aufbau eines Ticketsystems für Fehlermeldungen aus den einzelnen Einrichtungen und die Etablierung eines Workflows zum Abarbeiten. „Die Schulung und Sensibilisierung unserer Mitarbeiter machen wir seit einem Jahr“, stellt Hoffmann heraus. „Dazu sind der IT-Sicherheitsbeauftragte und ich quartalsweise in den verschiedenen Häusern.“

Ein Notfallmanagement für die IT soll bis Ende 2018 etabliert sein. „Es geht im Kern darum, ein Notfallhandbuch mit den entsprechenden Ablaufplänen zu verfassen“, erklärt der IT-Leiter. Größtenteils steht das, allerdings müssen wir noch für die Stationen beschreiben, wie arbeiten sollen, wenn die IT-Systeme einmal ausgefallen sind.“ Danach geht es an den Verantwortlichen für das Qualitäts- und Risikomanagement, der es schließlich freigibt. Alle Einzelschritte hin zur KRITIS-Tauglichkeit vollzieht die Mathias-Stiftung Rheine mit CETUS als Partner an der Seite. „Man merkt die große Erfahrung, die die Berater aus anderen Projekten mitbringen und die uns sehr hilft“, ist Hoffmann voll des Lobes.

Veränderungen in den Strukturen

Die Veränderungen in der IT der Mathias-Stiftung sind nicht nur auf dem Papier festgehalten, sie manifestieren sich auch in den Strukturen und der Organisation der Abteilung. „Anfangs haben wir in zwei Teams – eines hieß Technik und das andere ORBIS für unser Krankenhaus-Informationssystem – gearbeitet. Seit dem 1. Januar 2018 sind wir in drei Teams tätig, von dem eines mit zwei Leuten für den Bereich IT-Sicherheit und Infrastruktur verantwortlich ist“, beschreibt Hoffmann eine Änderung. Zudem wurden alle 140 IT-Services genau definiert und ein IT-Service-Verantwortlicher samt Vertreter benannt. „Das wurde vorher zwar bereits gelebt, war aber nirgendwo festgeschrieben“, sagt der IT-Leiter. Aktuell führt die Stiftung einen Prozess für das Change- und Update-Management ein.

Der Weg ist in Rheine nicht das Ziel. Ziel ist die Zertifizierung nach DIN ISO 27001 im Laufe des kommenden Jahres. Momentan fallen die Häuser zwar noch nicht unter KRITIS, das können sich jedoch ändern, sagt Dirk Hoffmann: „Zum einen wollen wir die Fallzahlen steigern, zum zweiten könnten wir künftig auch als Verbund betrachtet werden. Beides führt dazu, dass wir zur kritischen Infrastruktur gehören würden. Und mit der Zertifizierung sind wir dann auf einem guten Weg.“

Kontakt:

CETUS Consulting GmbH
Mendelstraße 11

48149 Münster

0251- 980 1620

info@cetus-consulting.de

