Schritt für Schritt zur Zertifizierung

Hochschulen und außeruniversitäre Forschungseinrichtungen geraten aufgrund ihrer teils dezentralen Strukturen immer häufiger ins Visier von Cyberkriminellen. Zur Bekämpfung und Prävention von Sicherheitsvorfällen ist es notwendig, rechtzeitig ein solides Fundament für IT-Sicherheit aufzubauen. Welche Schritte dafür erforderlich sind und warum sich der mitunter beschwerliche und lange Weg lohnt, zeigt als Vorreiter das Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ).

Text: **Stefan Metzger, Miran Mizani, Eda Seval-Munke, Helmut Reiser** (Leibniz-Rechenzentrum, LRZ)

Foto: Fineblick/Adobe Stock

Als wissenschaftliche Einrichtung ist das Leibniz-Rechenzentrum IT-Service Provider für die Universitäten und Hochschulen in München. Sehr früh, bereits im Jahr 2009, trieb das LRZ den Aufbau eines Service- sowie Informationssicherheitsmanagementsystems (ISMS) in Anlehnung an internationale Standards ISO/IEC 20000 und ISO/IEC 27001 massiv voran. Die Motivation bestand darin, Daten, die in wissenschaftlichen Kooperations- und Forschungsprojekten am LRZ gespeichert und verarbeitet werden, zu schützen und darüber hinaus als vertrauenswürdiger Partner aufzutreten.

Heute, 15 Jahre später, ist das Thema IT-Sicherheit dringlicher als je zuvor. Immer häufiger werden unter anderem Hochschulen und Forschungseinrichtungen Opfer von Cyberangriffen, die bei Erfolg den Betrieb massiv beeinträchtigen und für Kosten in Millionenhöhe sorgen können. Das bestätigt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI). In seinem aktuellen Lagebild schätzt das BSI die Sicherheitslage als „angespannt bis kritisch" ein. Zu den häufigsten Angriffsaktivitäten cyberkrimineller Akteure zählen Ransomware und verteilte Denial-of-Service-Angriffe, aber auch Hacktivism.

Regulatorische Vorschriften wie das IT-Sicherheitsgesetz oder die NIS2-Richtlinie sollen Abhilfe schaffen. Stand heute fällt der Hochschulbereich jedoch nicht zwingend in deren Geltungsbereiche. In Bayern legte deshalb das Staatsministerium für Wissenschaft und Kunst (StMWK) fest, dass jede bayerische Hochschule bis 2027 ein wirksames Informationssicherheitsmanagementsystem aufgebaut haben muss.

Der Weg zur Zertifizierung

Gestartet ist das LRZ mit der Etablierung einer definierten Vorgehensweise zur Behandlung von Sicherheitsvorfällen. Nach und nach kamen weitere Sicherheitsrichtlinien hinzu, die beispielsweise den Umgang mit Passwörtern oder mit Logdaten regelten. Im Laufe der Zeit wurde aber deutlich, dass diese auf Einzelmaßnahmen fokussierte Herangehensweise langfristig nicht zum erhofften Erfolg führen würde, da hierzu die Einbettung in einen organisatorischen und risikobasierten Rahmen fehlte.

Im Jahr 2017 beschloss daher die LRZ-Leitung, ein integriertes Service- (SMS) und Informationssicherheitsmanagementsystem (ISMS) aufzubauen und dieses nach den internationalen Normen ISO/IEC 20000 und ISO/IEC 27001 zertifizieren zu lassen. Folgende übergeordnete Zielsetzungen wurden dabei beachtet:

- Erhöhung der Kundenzufriedenheit durch mehr Professionalität, Transparenz und Kommunikation
- Einhaltung rechtlicher Rahmenbedingungen und Compliance-Anforderungen
- Verbesserung der Informationssicherheit durch festgelegte Prozesse
- Verbesserung des Reifegrades der Organisation
- Erfahrungsaufbau zur Wegbereitung anderer Organisationen im Hochschulumfeld

Im Fokus: Anwenderinnen und Anwender sollen darauf vertrauen können, dass mit ihren am LRZ verarbeiteten Daten sorgsam umgegangen wird und dies auch nachgewiesen werden kann. Aber hätte dann nicht auch eine Orientierung an der ISO-Norm ausgereicht? Nein, denn erst mit einer Zertifizierung kann die Einhaltung von Best-Practice-Sicherheitsvorgaben gegenüber Außenstehenden nachgewiesen werden. Zudem wird eine kontinuierliche Weiterentwicklung des ISMS sichergestellt.

47k – das Einführungsprojekt

Mit einer geplanten Laufzeit von 15 Monaten und dem definierten Ziel der Zertifizierung fiel im Januar 2018 der Startschuss für das Einführungsprojekt „47k". Die Projektbezeichnung ergab sich aus der Addition der zugrunde gelegten Normenreihen ISO/IEC 20k und 27k zu „47k". Als Geltungsbereich des integrierten Managementsystems wurden die vier Betriebsabteilungen des LRZ und damit alle angebotenen IT-Dienste festgelegt.

> Die Einführung eines Managementsystems erfordert einiges an Ressourcen.

Wichtig: Die LRZ-Leitung stand von Anfang an hinter dem Vorhaben. Die Projektleitung erhielt Unterstützung durch einen erfahrenen externen Berater und ein etwa 30-köpfiges Projektteam aus motivierten Kolleginnen und Kollegen aus allen Abteilungen. Die Einführung eines Managementsystems erfordert einiges an Ressourcen und stellt einen organisatorischen Umbruch dar, der nicht nur Prozesse und Technik betrifft, sondern insbesondere auch alle Mitarbeitenden. Erst ein gut austariertes magisches Dreieck aus „People, Process und Technology" ermöglicht ein funktionierendes Managementsystem. Keiner dieser Bereiche darf vernachlässigt werden.

Eine initiale Gap-Analyse zeigte, wo noch Abweichungen zu den Normvorgaben bestanden. Aus den identifizierten Defiziten wurden nachfolgend konkrete Maßnahmen abgeleitet. Oberste Prämisse war es, diese so umzusetzen, dass die angestrebte Zertifizierung realisiert werden kann und es gleichzeitig möglich ist, sich an der gelebten betrieblichen Praxis zu orientieren und ausreichend Spielraum für Verbesserungen zu lassen. Zur Veranschaulichung wurden hier die „Holzhütte vs. Schloss Neuschwanstein" gegenübergestellt. Die schlichte Holzhütte unterscheidet sich doch deutlich vom verspielt wirkenden Schloss, welches von Türmen und Erkern geprägt ist. Analog dazu neigen Forschende und Technikleute oft dazu, eine Lösung erst dann als fertig zu akzeptieren, wenn diese 100 Prozent der Anforderungen erfüllt. Zu akzeptieren, dass

zunächst auch 80 Prozent oder sogar weniger ein durchaus gutes und ausreichendes Ergebnis sind, war nicht für alle ganz einfach.

Prof. Dr. Dieter Kranzlmüller
Vorsitzender des Direktoriums des LRZ

Die Zertifizierung war ein Großprojekt, an dem das ganze LRZ, jede Mitarbeiterin und jeder Mitarbeiter, beteiligt waren. Es war ein gemeinsamer Kraftakt, der sich aber auf ganzer Linie ausgezahlt hat. Wir haben intern Prozesse und Dokumentationen, die unsere Arbeit unterstützen, und extern ein Qualitätsmerkmal, das für unsere Kunden in der Wissenschaft einen wichtigen Mehrwert darstellt.

Die prozessuale Vorgabe für den ISMS-Kernprozess, das Risikomanagement, war relativ schnell erstellt. Die Anwendung in der Praxis, zumal ohne dediziertes Tool, gestaltete sich jedoch zunächst schwierig. Betriebsrelevante Dokumentationen zu Server- und Netzkomponenten waren vorhanden. Jedoch mangelte es an Aussagen zu dort verarbeiteten und im Hinblick auf Vertraulichkeit, Integrität und Verfügbarkeit zu schützenden Informationswerten. Diese Informations-„Assets“ wurden daher zunächst eher allgemein, beispielsweise als „Konfigurationsdaten“, erfasst und mit den technischen „Assets“ in Beziehung gesetzt. Nicht nur die physische Netzkomponente, sondern vor allem deren Konfiguration ist vor Offenlegung oder unerlaubten Änderungen zu schützen. Wichtig war, loszulegen und die definierten Verfahren zu testen, inwieweit sie die gewünschten Ergebnisse bereits liefern konnten oder ob sie bei Bedarf nachjustiert werden mussten.

> Das Risikomanagement war relativ schnell erstellt.

Gemeinsam mit der LRZ-Leitung wurden geforderte Richtlinien und Prozessbeschreibungen erstellt, die das Arbeiten am LRZ und den Umgang mit Informationswerten „regelten“ und den Mitarbeitenden Handlungssicherheit gaben (Governance). Daneben wurden Pläne für die interne und externe Kommunikation definiert, ein Schulungs- und Awareness-Programm zum Thema Informationssicherheit aufgebaut und alle Beschäftigten geschult. Ein Kennzahlensystem überprüfte anhand einfacher Ja- oder Nein-Fragen die Normkonformität und gab der Leitung ein hilfreiches Steuerungsinstrument an die Hand.

Ein definierter Prozess regelt bis heute die Lenkung der Vorgabedokumentation, während die Nachweisdokumente (Records) als Freitext oder mit anderen Werkzeugen erfasst werden. Das LRZ nutzt kein dediziertes ISMS-Tool, sondern die allgemein zu Dokumentationszwecken eingesetzte und damit allen Beschäftigten vertraute Software Confluence. Die Erstellung und das Management der Dokumente funktionieren mit dieser nach wie vor sehr gut. In Verbindung mit einem Ticket-Tool und einer selbst entwickelten CMDB (Configuration Management Database) konnte ein dezidiertes ISMS-Tool bislang sehr gut ersetzt werden.

Foto: photoPepp/Adobe Stock

Nach nur knapp einem Jahr Projektlaufzeit waren die Gaps größtenteils geschlossen. Die Vorbereitung auf die angestrebte Zertifizierung konnte damit in Angriff genommen werden. Das vorgeschaltete interne Audit bewertete die erarbeiteten Ergebnisse anhand der Normvorgaben kritisch, größere Defizite fanden sich zum Glück keine mehr. Etwa ein halbes Jahr später, im Juli 2019, wurde die Erstzertifizierung erfolgreich bestanden. Ein sehr schöner Erfolg für das Projektteam und das gesamte LRZ.

Die Aufteilung in themenspezifische Teilprojekte hat sich bewährt. Diese erlaubte, mehrere Themenfelder parallel zu bearbeiten. Das verschaffte der Projektleitung ausreichend Zeit, sich sowohl auf die Koordination des Projekts und die Abstimmung mit

den Fachabteilungen zu konzentrieren als auch sicherzustellen, dass die erarbeiteten Ergebnisse im Einklang mit den festgelegten Anforderungen stehen. Das Hinzuziehen eines erfahrenen Beraters erwies sich ebenfalls als äußerst hilfreich. Ein großes Stück Pragmatismus, Orientierung an bestehenden Abläufen und die Vermeidung unnötigen Beiwerks waren wichtige Schritte zum Erfolg.

Herausforderungen im Betrieb des ISMS

Der Betrieb des Managementsystems endet keinesfalls zum Termin der erfolgreich abgeschlossenen Zertifizierung. Eine kontinuierliche Auseinandersetzung mit diesem, die Verbesserung des Gesamtsystems sowie insbesondere das tagtägliche „Leben" dokumentierter Vorgaben rücken in den Vordergrund.

> Das Hinzuziehen eines erfahrenen Beraters erwies sich ebenfalls als äußerst hilfreich.

Ein Managementsystem versucht Abläufe nicht nur zu strukturieren, sondern auch organisationsweit zu standardisieren. Dienstspezifische Vorgehensweisen, die hiervon abweichen, sind grundsätzlich erlaubt. Am LRZ wurden diese durch Ergänzungen in der Dokumentation abgebildet, infolgedessen litt deren Lesbarkeit und Verständlichkeit. In den jährlichen Reviews wird nun versucht, die Ergänzungen Stück für Stück zu vereinfachen und Richtlinien, Prozesse sowie Verfahren von unnötigem Ballast und aufwendigen Dokumentationspflichten zu befreien.

Häufig wird ein ISMS mit extrem hohem Dokumentationsaufwand verbunden. Aber nicht die Dokumentation, sondern die Umsetzung der Prozesse und Verfahren in der täglichen Praxis und die Integration des ISMS in den betrieblichen Alltag sind das, was zählt. Verlangt wird daher von allen Beteiligten, nur das Notwendigste so ausführlich zu dokumentieren, dass die mit dem ISMS gesteckten Ziele erreicht werden. Statt Dokumentation lediglich als lästige Pflicht zu betrachten, sollte sie als sinnvoll erachtet und nachvollziehbar und zweckdienlich verfasst werden.

Mitarbeitende sehen sich durch das ISMS oft mit Einschränkungen konfrontiert. Dies rührt nicht zwingend aus dem Konzept eines Managementsystems selbst, sondern aus den Regelungen, die eine Organisation erlässt. Für einige zuvor ungeregelte Zustände bzw. Verfahrensweisen, die den Mitarbeitenden viel Freiraum gaben, werden nun explizite Entscheidungen getroffen und so der Wille der Leitung kundgetan. Dies führt oft zu Konflikten aus Präferenz, Gewohnheit oder auch Bequemlichkeit. Eine völlige Freiheit in der Ausgestaltung sicherheitsrelevanter Vorgänge existiert heute nicht mehr. Übliche Beispiele sind die Installation von Software auf dem Arbeitslaptop oder die Nutzung privater Endgeräte für die Erledigung dienstlicher Aufgaben. Eine große Bedeutung kommt hier der Kommunikation und dem Schaffen von Awareness zu. Dabei sollten weniger die Fragen „was" oder „wie" etwas gemacht wird, beantwortet werden, sondern vor allem das „warum" im Mittelpunkt stehen.

Eine weitere und gerade auch im Hochschulumfeld nicht zu vernachlässigende Herausforderung entsteht durch personelle Abgänge und Wechsel sowie damit verbundene Änderungen im Aufgabenspektrum. Das führte am LRZ dazu, dass das ehemals sehr große Projektteam nach und nach schrumpfte. Die Verantwortlichkeiten für die stattliche Anzahl an Richtlinien und Prozessen waren auf einige wenige Schultern zu verteilen, was die Geschwindigkeit der Verbesserung des ISMS und seiner Bestandteile nach und nach bremste. Für das „Leben" des ISMS im Alltag ist es notwendig, dass die Verantwortung hierfür mehr und mehr in die Linienorganisation, also an das zuständige Führungspersonal, übergeht.

Die Pflicht zur kontinuierlichen Verbesserung des Managementsystems birgt die Herausforderung, die gelebte Praxis in Form regelmäßig stattfindender Überwachungsaudits und interner Audits zu überprüfen. Audits werden insbesondere von Mitarbeitenden nicht selten als unnötig und zeitaufwendig erachtet, sind aber durch ihren unabhängigen und objektiven Blick von außen entscheidend dafür, Schwachpunkte im Managementsystem zu identifizieren und ausräumen zu können.

Dr. Oliver Diekamp
Leitung Dezernat Informations- und Kommunikationstechnik der LMU München

Dank der Sicherheitszertifizierung können Forscherinnen und Forscher der LMU, aber auch Drittmittelgeber und andere Partner sich nun auch nachweislich darauf verlassen, dass Daten in der Infrastruktur des LRZ stets nach dem Stand der Technik geschützt werden können. Angesichts der Bedrohung durch Cyberangriffe, aber auch der damit verbundenen zunehmenden Regulierung leistet die Sicherheitszertifizierung des LRZ damit einen wichtigen Beitrag für exzellente Forschungsbedingungen an der LMU.

HOCHSCHULÜBERGREIFENDE IT-SERVICES FÜR INFORMATIONSSICHERHEIT (HITS-IS)

Mit HITS-IS fördert die bayerische Staatsregierung den Aufbau hochschulübergreifender IT-Services für Informationssicherheit. Die Strategie dahinter: Know-how und Dienste im Digitalverbund Bayern zentral aufzubauen und allen Hochschulen in Bayern zur Verfügung zu stellen, um so gezielt Synergien zu schaffen.

Das Angebot umfasst u. a. Unterstützung bei schwerwiegenden IT-Sicherheitsvorfällen und beim Aufbau eines Information Security Management System (ISMS) oder Business Continuity Management (BCM), die Durchführung von Schwachstellenscans, Security-Awareness-Maßnahmen sowie technisches Consulting.

Weitere Informationen finden Sie unter:
https://digitalverbund.bayern/hits/informationssicherheit/

LITERATUR

Aufbau eines Managementsystems – Tools vs. Prozesse: Ausgabe 101:
https://www.dfn.de/wp-content/uploads/2024/01/DFN-Mitteilungen-101.pdf

Praxisbuch ISO/IEC 27001 – Management der Informationssicherheit und Vorbereitung auf die Zertifizierung (Michael Brenner, Nils Gentschen Felde, Wolfgang Hommel, Stefan Metzger, Helmut Reiser, Thomas Schaaf):
Erschienen im Carl Hanser Verlag GmbH & Co. KG

Hat es sich gelohnt?

Nach fünf Jahren Betrieb des integrierten Managementsystems und damit einigen erfolgreichen Voll- und Überwachungsaudits stellt sich die Frage, ob sich der Schritt tatsächlich gelohnt hat.

Von Beginn an wurde der konkrete individuelle Mehrwert für die eigene Arbeit von den Mitarbeitenden kritisch hinterfragt. Für die einzelne Kollegin oder den einzelnen Kollegen kann dieser überschaubar sein, für die Organisation insgesamt ist er jedoch enorm.

Dokumentierte, wiederholbare Prozesse und Verfahren helfen, die eigene Arbeit besser zu strukturieren oder die Arbeitslast teamintern auf mehrere Schultern zu verteilen. Die Behandlung von Sicherheitsvorfällen oder der Umgang mit technischen Schwachstellen erfolgen, wie im ISMS-Kontext genannt, gesteuert. Entscheidungen, etwa eine Schwachstelle zu patchen, werden nicht ad hoc oder nach Bauchgefühl getroffen, sondern nachvollziehbar und nach Abwägen damit verbundener Risiken. Wo früher Einzelmaßnahmen isoliert umgesetzt wurden, existiert nun ein gesamtheitlicher Ansatz, wodurch der Reifegrad der Dienstbringung am LRZ gesteigert werden konnte. Auch die Zufriedenheit der Kunden, die das LRZ jetzt noch stärker als vertrauensvollen Partner und IT-Dienstleister wahrnehmen, erhöhte sich messbar. So genügt in Forschungsprojekten von LRZ-Kunden mit externen Partnern nicht selten der einfache Hinweis auf das bestehende ISO/IEC 27001-Zertifikat oder reduziert zumindest die Anzahl der zu beantwortenden Fragen hinsichtlich umgesetzter Sicherheitsmaßnahmen deutlich. Das ISMS bildet somit ein solides Fundament, auf dem weitergehende Sicherheitsmechanismen, etwa zum Schutz besonders sensibler Daten wie etwa in der Medizin aufbauen.

Es soll aber keinesfalls verschwiegen werden, dass der Aufbau eines ISMS einen organisatorischen Wandel, nicht selten einen Kulturwandel, erfordert. Der Betrieb eines ISMS und die Aufrechterhaltung der Zertifizierung bedeutet täglichen Aufwand, der nicht nur für das zuständige ISMS-Personal, sondern auch in nicht zu unterschätzendem Umfang für die gesamte Belegschaft entsteht. Dieser Aufwand aber lohnt sich! ◆