27. DFN-Konferenz "Sicherheit in vernetzten Systemen", 24./25. Februar 2020 in Hamburg,
BoD - Books on Demand; Auflage: 1 (23. Januar 2020), ISBN-10: 3750438234, E1-E20.

In 12 Schritten zu mehr Informationssicherheit

Einführung des Informationssicherheitsmanagementsystems ISIS12

an der Otto-Friedrich-Universität Bamberg

Christian Kraus, Hartmut Plehn
Otto-Friedrich-Universität Bamberg
Feldkirchenstraße 21
96052 Bamberg
christian.kraus@uni-bamberg.de
hartmut.plehn@uni-bamberg.de

Zusammenfassung

Informationssicherheit ist für Hochschulen eine wesentliche Voraussetzung für die Erbringung ihrer Aufgaben. Sie ist als strategische Aufgabe der Hochschulleitungen zu verstehen [1]. Ein alle Aspekte der Informationssicherheit umfassender Gestaltungsansatz ist durch einschlägige Management-Frameworks für Informationssicherheit wie ISO/IEC 27001 oder BSI-Grundschutz gegeben. Das Informationssicherheitsmanagementsystem (ISMS) ISIS12 will einen gegenüber diesen Frameworks vereinfachten Einstieg in eine trotzdem möglichst umfassende Behandlung der wesentlichen Aspekte der Informationssicherheit ermöglichen. An der Otto-Friedrich-Universität Bamberg wurde mit der Aussicht auf diesen vereinfachten Einstieg im August 2017 mit der Einführung von ISIS12 begonnen. Im vorliegenden Artikel wird ISIS12 kurz vorgestellt, der bisherige Verlauf des Einführungsprojekts beschrieben und die Eignung von ISIS12 für Hochschulen diskutiert.

1 Einleitung

Die Sicherheit von Informationen, Daten und IT-Systemen wird an den Hochschulen mittlerweile als unabdingbare Grundlage für eine erfolgreiche Lehre und Forschung sehr ernst genommen. Gleichzeitig haben sich mit dem IT-Sicherheitsgesetz [2], der EU-Datenschutzgrundverordnung [3] und E-Government-Gesetzen, siehe beispielweise [4], die rechtlichen Rahmenbedingungen verschärft. Fördermittelgeber, wie beispielsweise die Deutsche Forschungsgemeinschaft, betrachten die Sicherheit von Daten als zentrale Anforderung in Forschung, Studium, Lehre und Verwaltung [5].

Zur Verbesserung der Informationssicherheit, also zur Sicherstellung der Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität, sind viele Aspekte zu betrachten. Auf der technischen, betrieblichen Ebene wird schon seit den Anfängen der elektronischen Informationsverarbeitung an den Hochschulen auch großer Wert auf die IT-Sicherheit gelegt. In anderen Bereichen wie bei den organisatorischen Maßnahmen, der Sensibilisierung der Nutzer oder dem Umgang mit Sicherheitsvorfällen gibt es noch viel zu tun. Der systematische Einstieg in eine ganzheitliche Behandlung der Informationssicherheit stellt für viele Hochschulen angesichts der Breite des Themas und knapper Ressourcen eine große Hürde dar.

In Bayern wurden in Abstimmung zwischen dem Staatsministerium für Wissenschaft und Kunst (StMWK) und den CIO-Runden der beiden Hochschulverbünde Universität Bayern e. V. und Hochschule Bayern e. V. erste Schritte zur Verbesserung der Informationssicherheit an den bayerischen Hochschulen unternommen. Es wurde ein Grundsatzpapier zum aktuellen Stand und zu empfohlenen Maßnahmen erarbeitet [6]. Zentrales Ergebnis war, dass zwar einige organisatorische Maßnahmen wie die Erstellung einer Informationssicherheitsleitlinie sofort umgesetzt werden können und sollten. Da Informationssicherheit in einer umfassenden strategischen Betrachtung aber eine aufwändige Zusatzaufgabe für die Hochschulen darstellt, werden dafür zusätzliche Ressourcen benötigt. Diese wurden beantragt, bisher aber noch nicht bereitgestellt. Als Sofortmaßnahme wurden eine Stabsstelle IT-Recht und eine Stabsstelle Informationssicherheit für die bayerischen staatlichen Hochschulen geschaffen. Die Stabsstellen kümmern sich um übergreifende Fragen, führen Audits durch, erstellen Vorlagen und stehen beratend zur Verfügung.

Die Universität Bamberg gehört mit knapp 13.000 Studierenden zu den mittelgroßen Universitäten und verfügt über ein aus IT-Sicht relativ homogenes Fächerspektrum ohne Naturwissenschaften und Medizin. Im nennenswerten Umfang wird nur in der Fakultät für Wirtschaftsinformatik und Angewandte Informatik eigene forschungsbezogene IT-Infrastruktur

dezentral betrieben. Nach Einschätzung des Chief Information Office (CIO)[1] der Universität ist der Aufwand für Informationssicherheit daher kleiner als bei großen und heterogeneren Universitäten. Dies wurde zum Anlass genommen, einen einerseits möglichst umfassenden, aber andererseits möglichst einfachen Einstieg in das Informationssicherheitsmanagement aus eigener Kraft anzugehen. Für einen derartigen Einstieg bietet sich das ISMS ISIS12 an. Im August 2017 wurde an der Universität Bamberg ein Projekt zur Einführung von ISIS12 zunächst für den nichtwissenschaftlichen Bereich begonnen.

2 Informationssicherheit in 12 Schritten (ISIS12)

Das ISMS ISIS12[2] wurde vom bayerischen IT-Sicherheitscluster e. V.[3] ursprünglich für den Einsatz in kleinen und mittleren Unternehmen (KMU) entwickelt. Im Rahmen einer Analyse des Fraunhofer AISEC wurde festgestellt, dass ISIS12 auch für öffentliche Verwaltungen und Kommunen mit bis zu etwa 500 Arbeitsplätzen geeignet ist [7]. Der Freistaat Bayern fördert die Umsetzung von ISIS12 in bayerischen Kommunen.[4]

ISIS12 verwendet in der Version vom Juni 2018 Maßnahmen aus den BSI IT-Grundschutzkatalogen[5] ergänzt um eigene Maßnahmen für das Thema Datenschutzgrundverordnung (DSGVO). Die Anzahl der Maßnahmen ist im Vergleich zum BSI-Grundschutz aber radikal reduziert. So sind bei ISIS12 nur etwa 400 statt 1100 Maßnahmen umzusetzen. ISIS12 wurde nach dem Grundsatz „So einfach wie möglich – aber nicht einfacher“ konzipiert. In Abbildung 1 werden einige Aspekte der Informationssicherheitsmanagementsysteme „BSI-Grundschutz“, „ISO/IEC 27001“ und „ISIS12“ gegenübergestellt. Die Umsetzung von ISIS12 kann von zertifizierten Beratern begleitet sowie von unabhängigen Auditoren direkt zertifiziert oder als Vorstufe zu einer ISO/IEC 27001- bzw. BSI IT-Grundschutz-Zertifizierung verwendet werden.

---

[1] https://www.uni-bamberg.de/rz/wir/it-organisation/cio/, 11.11.2019.

[2] https://isis12.it-sicherheitscluster.de/, 11.11.2019.

[3] https://www.it-sicherheitscluster.de/, 11.11.2019.

[4] https://isis12.it-sicherheitscluster.de/fuer-kommunen/, 11.11.2019.

[5] Der BSI-Grundschutz wurde 2017 auf ein IT-Grundschutz-Kompendium als Nachfolge der Grundschutzkataloge umgestellt. ISIS12 verwendet aber noch die früheren Grundschutzkataloge.

BSI IT-Grundschutz	ISO/IEC 27001	ISIS12
ca. 4400 Seiten	ca. 30 Seiten	ca. 170 Seiten
ca. 1100 Maßnahmen	ca. 150 „Maßnahmenvorschläge“	ca. 400 Maßnahmen
„ergänzende“ Risikoanalyse	Risikoanalyse fundamental	keine **direkte** Risikoanalyse
konkrete Maßnahmen, Umsetzung erforderlich	allgemeine „Maßnahmen“	konkrete Maßnahmen, Umsetzung erforderlich
Handlungsempfehlung	keine konkrete Handlungsempfehlung	Handlungsempfehlung
hohe Auslastung des ISB	hohe Auslastung des ISB	geringe Auslastung des ISB
Bausteine, Maßnahmen, Gefährdungen	„Maßnahmenziele“	Bausteine, Maßnahmen

Abbildung 1*:* Vergleich des Umfangs von BSI-Grundschutz, ISO/IEC 27001 und ISIS12 [8] sowie des Aufwands für den Informationssicherheits-beauftragten (ISB)

Die Einführung von ISIS12 erfolgt anhand des ISIS12-Handbuchs [9] und ISIS12-Katalogs [10] in 12 Schritten, siehe Abb. 2. Sie kann durch eine speziell entwickelte ISIS12-Software unterstützt werden.

Eine Einschränkung von ISIS12 besteht darin, dass keine direkte Risikoanalyse, sondern eine implizite Risikoanalyse in Form einer Einordnung von Anwendungen und Daten in Schutzbedarfskategorien erfolgt.

Von großem Vorteil ist die systematische Herangehensweise, die ausgehend von den kritischen Anwendungen über die dazugehörigen Systeme und Infrastruktur zu konkreten Maßnahmen führt. Das ISIS12-Vorgehensmodell stellt dadurch sicher, dass alle Aspekte angemessen berücksichtigt und alle Maßnahmen umgesetzt wurden.

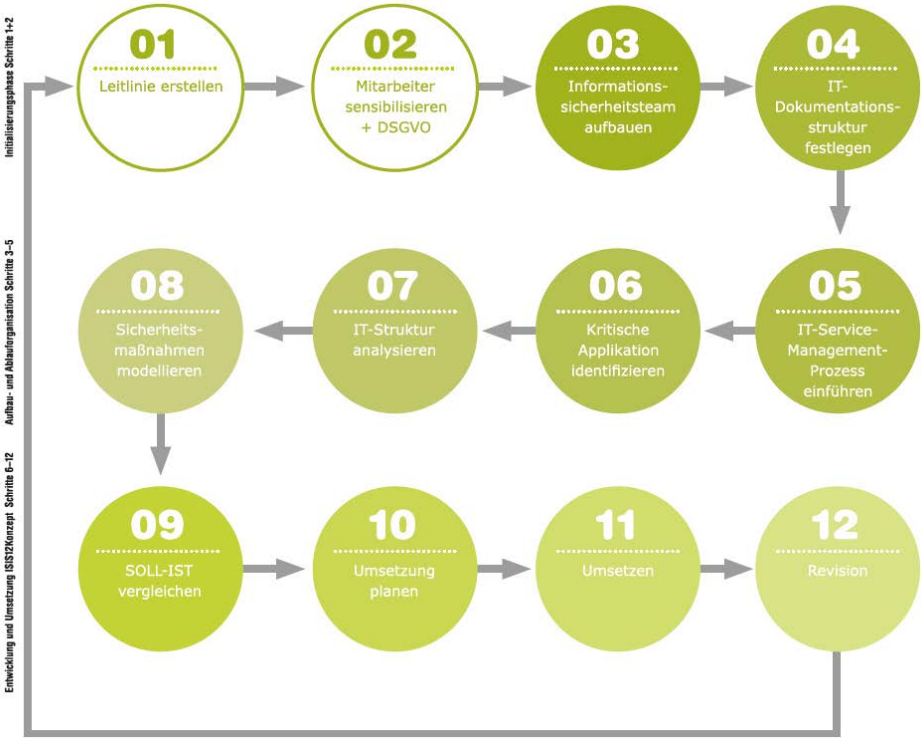

Abbildung 2: Schematische Darstellung der Abfolge der Umsetzung in 12 Schritten mit einer Initialisierungsphase (Schritte 1 und 2), einer Phase zur Aufbau- und Ablauforganisation (Schritte 3 bis 5) und einer Phase zur Entwicklung und Umsetzung der ISIS12-Maßnahmen (Schritte 6 bis 12) [11].

3 Projektverlauf

3.1 Vorarbeiten

ISIS12 wurde für deutlich kleinere Einrichtungen als die Universität Bamberg und ohne Berücksichtigung hochschulspezifischer Randbedingungen konzipiert. Bevor die Entscheidung für das Einführungsprojekt getroffen wurde, wurde daher die Eignung von ISIS12 für

Hochschulen im Rahmen eines Seminars zum Geschäftsprozessmanagement untersucht. Im Ergebnis waren keine grundsätzlichen Hindernisse zu erkennen, ISIS12 für eine Einrichtung von der Größe der Universität Bamberg einzusetzen. Lediglich eine noch stärkere Gruppierung von Geräten in Geräteklassen, als sie von ISIS12 vorgesehen ist, wurde als notwendig betrachtet. Ein Auftragsklärungs-Workshop mit einem ISIS12-Dienstleister kam zum gleichen Ergebnis. Ausgehend von diesem Befund hat das CIO-Gremium im Oktober 2016 der Universitätsleitung die Einführung von ISIS12 empfohlen.

Die Universitätsleitung hat daraufhin zur Unterstützung des Projekts eine Fachinformatikerstelle auf zwei Jahre befristet zur Verfügung gestellt. Die Stelle dient der Entlastung eines Mitarbeiters aus dem Netzbetrieb des Rechenzentrums, der die Projektleitung übernommen hat. Das Bayerische StMWK hat die Finanzierung von Beratungsdienstleistungen im Umfang von 25 Manntagen übernommen, weil die Erkenntnisse aus dem Pilotprojekt von allen bayerischen Hochschulen genutzt werden können. Zu diesem Zweck findet auch eine enge Abstimmung mit der Stabsstelle Informationssicherheit der bayerischen staatlichen Hochschulen statt.

Es wurde festgelegt, dass das Projekt abschließend von unabhängigen Auditoren zertifiziert werden soll. Dabei steht nicht primär das Zertifikat als Nachweis nach außen im Vordergrund, sondern die sich daraus intern ergebende Verbindlichkeit bei der praktischen Umsetzung der Maßnahmen.

3.2 Schrittweise Umsetzung

Im Folgenden werden der Verlauf, der Grad der Umsetzung und die gewonnenen Erkenntnisse für die im Rahmen von ISIS12 durchzuführenden 12 Prozess-Schritte dargelegt.

Schritt 1: IT-Sicherheitsleitlinie erstellen

Die IT-Sicherheitsstrategie der Universität Bamberg [I12] wurde am 17.12.2014 bereits vor den Überlegungen zur Einführung eines ISMS verabschiedet. Diese IT-Sicherheitsstrategie enthält die wesentlichen Vorgaben gemäß ISIS12 bzw. BSI-Maßnahme M 2.192. Konkret werden dort die IT-Sicherheitsorganisation inklusive der Verantwortlichkeiten, die IT-Sicherheitsziele, das angestrebte IT-Sicherheitsniveau sowie IT-Sicherheitsprozesse auf einer abstrakten Ebene festgelegt.

Schritt 2: Mitarbeiter sensibilisieren

Gemäß ISIS12 sollen alle Beschäftigten der betroffenen Einrichtung über das ISIS12-Einführungsprojekt informiert und für das Thema

Informationssicherheit sensibilisiert werden. Das ist an einer Universität nur schwer systematisch umsetzbar. Das Projekt wurde zwar am 09.11.2017 erstmals in einer Personalversammlung vorgestellt. Die Teilnahme an der Personalversammlung ist aber nicht verpflichtend. Außerdem richtet sie sich nur an die nichtwissenschaftlich Beschäftigten.

Die Informationssicherheit ist regelmäßig Thema im Newsletter des Rechenzentrums. Zu spezifischen oder aktuellen Bedrohungen werden immer wieder Rundschreiben an alle Beschäftigten verteilt. Allgemeine Vorträge zur Sensibilisierung für das Thema Informationssicherheit fanden darüber hinaus bereits mehrfach in weiteren Personalversammlungen und Anfang 2018 im gesamtuniversitären Professorium statt.

An der Universität Bamberg finden jährlich für das wissenschaftsstützende Personal verpflichtend Arbeitssicherheitseinweisungen statt. Im Rahmen dieser Veranstaltungen wurde 2019 neben der klassischen Arbeitssicherheit auch die Informationssicherheit behandelt.

Schritt 3: Informationssicherheitsteam aufbauen

ISIS12 empfiehlt zur Umsetzung eines Einführungsprojekts die Bildung eines Informationssicherheitsteams, dem der IT-Sicherheitsbeauftragte, ein Mitglied der Unternehmensleitung, der IT-Leiter, der Datenschutzbeauftragte, eine Fachkraft für Arbeitssicherheit, ein Vertreter des Personalrats sowie ein Vertreter der Haustechnik angehören sollten.

An der Universität Bamberg hat sich in vielen Fällen trotz der Problematik nicht ganz eindeutiger Kompetenzen und Verantwortlichkeiten die Verteilung von Funktionen auf mehrere Personen bewährt. So besteht das Chief Information Office aus 3 Personen.[1] Die Verantwortlichkeit für die IT-Sicherheit obliegt einem IT-Sicherheitsbeauftragten-Team, dem gemäß IT-Sicherheitsstrategie [12] der Vorsitzende des IuK-Beirats[6], der Datenschutzbeauftragte und die IT-Verantwortlichen für den Bereich Lehre und Forschung sowie Verwaltung angehören. Diese Übertragung von Funktionen auf mehrere Personen vereinfacht die Informationsflüsse zwischen den Gremien und kommt der an Hochschulen verbreiteten Diskussionskultur entgegen.

Am 08.08.2017 fand der Projekt-Kickoff u. a. unter Beteiligung der Kanzlerin, des Vizepräsidenten Technologie und Innovation, dem Datenschutzbeauftragten, Vertretern der IT und des Personalrats sowie den externen ISIS12-Beratern statt.

[6] https://www.uni-bamberg.de/rz/wir/it-organisation/beirat/, 11.11.2019.

Schritt 4: IT-Dokumentationsstruktur festlegen

Als Grundlage für die Dokumentation wird eine Reihe von Rahmendokumenten verlangt. Dazu gehören ein Organigramm, aus dem die IT-Organisation hervorgeht, eine IT-Kompetenzmatrix, eine IT-Namenskonvention, eine Dokumentationsrichtlinie und eine Verfahrensanweisung zur Lenkung von Dokumenten. Da diese Dokumente an der Universität Bamberg höchstens in Ansätzen vorhanden waren, mussten sie erarbeitet werden.

Aufbauend auf diesen Rahmendokumenten ist eine Betriebsdokumentation für alle kritischen IT-Systeme zu erstellen. Bereits bestehende Dokumentationen sind im Hinblick auf Namenskonventionen und Richtlinien zur Dokumentation zu überarbeiten bzw. in die neu gegliederte Betriebsdokumentation zu integrieren. Dieser Schritt hat sich im Verlauf des Projekts als äußerst aufwändig herausgestellt, weil die bisherige Dokumentation der Systeme unvollständig, uneinheitlich und auf unterschiedlichste Systeme verteilt war.

Etwas verringern lässt sich der Aufwand, indem gleichartige Systeme gruppiert werden. Beispielsweise werden an der Universität Bamberg nicht alle Server einzeln dokumentiert, sondern alle virtuellen Server mit vergleichbaren Sicherheitsanforderungen werden zu einer Systemgruppe zusammengefasst. Gleiches gilt beispielweise auch für Netzkomponenten und PC-Endgeräte. Unterschieden wird allerdings nach dem ermittelten Schutzbedarf, ob ein PC im wissenschaftlichen Bereich, im Verwaltungsnetz oder in einem PC-Pool bzw. Lesesaal eingesetzt wird. Trotz dieser Vereinfachung wurden über 400 kritische IT-Systeme erfasst.

Darüber hinaus betrachtet ISIS12 eine Notfalldokumentation in Form von Notfall-, Wiederanlauf- und Geschäftsfortführungsplänen als Bestandteil der IT-Dokumentation. Eine vollständige IT-Notfallplanung hätte den Rahmen des Projekts gesprengt. Es wurde sich daher beschränkt auf rudimentäre Wiederanlaufpläne für zentrale Systeme und auf die Dokumentation der Abhängigkeiten der wichtigsten Systeme untereinander. Außerdem wurde bei der Konzeption der Betriebsdokumentation darauf geachtet, dass auch im Notfall alle unabdingbaren Informationen zusätzlich auf unabhängigen Systemen verfügbar sind. Die für eine vollwertige Notfallplanung erforderlichen Tests der Wiederanlaufpläne werden im Rahmen der regulären System- und Wartungsarbeiten sukzessive und möglichst unter Vermeidung von Dienstunterbrechungen durchgeführt.

Als Basis für die Dokumentation wurde SharePoint („On-Premises“) in Kombination mit OneNote gewählt. Strukturierte Informationen wie Identifier, Schutzbedarfskategorien usw. werden in Form von SharePoint-Listen festgehalten. Textuell auszuformulierende unstrukturierte

Informationen werden gemäß der von ISIS12 vorgeschlagenen Gliederung für IT-Systeme in OneNote erfasst. Zur Dokumentation von Änderungen, Wartungen und Störfällen sowie zum Monitoring werden nachgelagerte Systeme wie das Ticketsystem, die Versionsverwaltung, Administrationstools sowie das Monitoringsystem in der jeweiligen Systemdokumentation unter Verwendung der systemübergreifend eindeutigen Identifier verlinkt.

Die Auswahl eines geeigneten Dokumentationssystems ist für die Akzeptanz bei den IT-Administratoren von zentraler Bedeutung. Wichtige Funktionalitäten sind eine einfache und intuitive Bedienung, der ortsunabhängige Zugriff von mehreren Personen gleichzeitig sowie die Versionierung von Inhalten.

Wenn man nicht schon von einer einigermaßen einheitlichen und vollständigen Betriebsdokumentation ausgehend beginnen kann, birgt Schritt 4 die große Gefahr, dass das Projekt ins Stocken gerät. Die Erfassung und Dokumentation aller Systeme kann nur im geringen Umfang zentral unterstützt werden und fordert von den Administratoren einen großen zusätzlichen Aufwand zum Tagesgeschäft. Dieser konnte in dem für den Projektschritt an der Universität Bamberg vorgesehenen Zeitraum nicht aufgebracht werden. Es wurde sich daher zunächst darauf beschränkt, die Dokumentationsstruktur festzulegen und nur die wichtigsten Informationen zu den wesentlichen Systemen nach der dabei vorgegebenen Gliederung zu erfassen. Unabhängig vom ISIS12-Projekt gilt die Vorgabe, dass zukünftig die Dokumentation gemäß Dokumentationsrichtlinie an den festgelegten Stellen zu erfolgen hat.

Schritt 5: IT-Service-Management-Prozesse einführen

Gemäß ISIS12 sind in Schritt 5 die Service-Management-Prozesse für Wartung, Änderung und Störungsbeseitigung festzulegen. Eine konkrete Ausgestaltung wird nicht vorgegeben. An der Universität Bamberg wurden diese Prozesse angelehnt an ITIL[7] bereits vor einigen Jahren eingeführt.

Schritt 6: Kritische Anwendungen identifizieren

Das ISIS12-Rahmenwerk sieht zunächst die Lokalisierung aller Anwendungen vor, mit denen schützenswerte Informationen verarbeitet oder kritische Prozesse unterstützt werden. Hierbei handelt es sich u. a. um Informationen, die durch gesetzliche Vorgaben in Bezug auf die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit zu schützen sind. Für die Universität Bamberg wurden über 120 solcher kritischen Anwendungen erfasst.

[7] https://de.wikipedia.org/wiki/IT_Infrastructure_Library, 11.11.2019.

ISIS12 sieht eine Schutzbedarfsfeststellung für kritische Anwendungen vor. An der Universität Bamberg wurden hierzu drei Schutzbedarfskategorien (A, B, C) für einen normalen, mittleren bzw. hohen Schutzbedarf definiert.

Betrachtet werden in Bezug auf die drei Grundwerte fünf mögliche Beeinträchtigungen: 1) Beeinträchtigung des informationellen Selbstbestimmungsrechts und 2) der Aufgabenerfüllung; 3) Verstoß gegen Gesetze, Vorschriften und Verträge; 4) Negative Außenwirkungen; 5) Finanzielle Auswirkungen. Beispielweise wird ein Ereignis, bei dem höchstens ein geringer Ansehensverlust eines Teilbereichs der Universität bei einer eingeschränkten Öffentlichkeit entstehen kann, der Schadenskategorie A zugeordnet. Droht hoher Ansehensverlust in eingeschränkter Öffentlichkeit trifft Schadenskategorie B, bei hohem Ansehensverlust in der breiten Öffentlichkeit Schadenskategorie C zu. Nur vereinzelt mussten Anwendungen der Schutzbedarfsklasse C zugeordnet werden. Dies ist beispielsweise dann der Fall, wenn bei medizinischen Patientendaten das informationelle Selbstbestimmungsrecht derart beeinträchtigt werden kann, dass die Gesundheit, das Leben oder die Freiheit des Betroffenen beeinträchtigt ist.

ISIS12 weist bei Anwendungen mit sehr hohem Schutzbedarf darauf hin, dass eine nachgelagerte Risikoanalyse erforderlich ist. An der Universität Bamberg wurde daher beschlossen, eine Risikoanalyse in Anlehnung am BSI-Standard 200-3 für die Fälle durchzuführen, die einen hohen Schutzbedarf (C) in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben.

Für jede kritische Anwendung wird eine Verarbeitungstätigkeits-beschreibung nach Art. 30 Abs. 1 DSGVO erstellt. Für Anwendungen, für die im Rahmen der Schutzbedarfsfeststellung ein mittlerer oder hoher Schutzbedarf (B, C) aufgrund der Abschätzung eines möglichen Schadens bei der Beeinträchtigung des informationellen Selbstbestimmungsrechts festgestellt worden ist, erfolgt zusätzlich eine Datenschutz-Folgenab-schätzung gemäß Art. 35 Abs. 1 Satz 1 DSGVO. Dabei kommt die PIA-Software der französischen Datenschutzaufsichtsbehörde[8] zum Einsatz.

Schritt 7: IT-Struktur analysieren

Das ISIS12-Rahmenwerk sieht vor, sämtliche IT-Systeme, Räume und Gebäude zu erfassen, die für den Betrieb der Anwendung notwendig sind. Diese Objekte werden mit den Anwendungen verknüpft, sodass hieraus deren Schutzbedarf abgeleitet werden kann. In einem bereinigten Netzplan sollen schließlich Anwendungen und zugeordnet Objekte gruppiert

[8] https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment, 11.11.2019

dargestellt werden. Die komplexe Netz- und Systemstruktur einer Universität lässt sich nicht in einem Plan gleichzeitig übersichtlich und vollständig darstellen. Daher wurden mehrere Pläne mit unterschiedlichen Abstraktionsniveaus erstellt.

Schritt 8: Sicherheitsmaßnahmen modellieren

Im ISIS12-Katalog sind Maßnahmen aus dem BSI IT-Grundschutz für die Organisation und die unterschiedlichen Kategorien von Anwendungen, IT-Systemen und Infrastrukturkomponenten aufgeführt. Die dort enthaltenen Prüffragen müssen beantwortet werden.

Hierzu werden von Fach- und Systemverantwortlichen jedem Objekt die Maßnahmen der zugehörigen Kategorien zugeordnet.

Schritt 9: Ist-Soll vergleichen

Im Rahmen eines Ist-Soll-Vergleichs soll ein Überblick über den Umsetzungsgrad der in Schritt 8 geforderten Maßnahmen gegeben werden. Der Umsetzungsgrad wird dabei von den Verantwortlichen selbst angegeben. Umgesetzte Maßnahmen müssen dokumentiert werden. Für Maßnahmen, die nicht oder nur teilweise umgesetzt worden sind, müssen Begründungen und verbindliche Revisionstermine angegeben werden.

Der Bearbeitungsstand zu einer Maßnahme wird in einer zentralen Liste dokumentiert. Die Dokumentation zu den Maßnahmen erfolgt in separaten Dokumenten.

In Schritt 9 hat sich gezeigt, dass die Mehrzahl der von ISIS12 bzw. BSI vorgegebenen technischen Sicherheitsmaßnahmen an der Universität Bamberg schon lange bereits berücksichtigt wurden. Defizite gab es insbesondere bei organisatorischen Maßnahmen, bei der Betriebs- und Notfall-Dokumentation sowie bei der Verschriftlichung von Richtlinien und betrieblichen Vorgaben.

Schritt 10: Umsetzung planen

Maßnahmen, die noch nicht umgesetzt worden sind, werden zunächst zusammengefasst und priorisiert. Hierbei spielt der festgestellte Schutzbedarf, die Breitenwirkung der Maßnahme oder die logische Reihenfolge von Maßnahmen eine Rolle.

Sofern vorhandene Ressourcen (Budget, Personal) für die Umsetzung der noch ausstehenden Maßnahmen nicht ausreichen, soll gemäß ISIS12-Rahmenwerk die Leitung über die Umsetzung der Maßnahmen und deren Reihenfolge entscheiden.

Schritt 11: Umsetzen

Gemäß ISIS12-Rahmenwerk soll für jede ausstehende Maßnahme ein Verantwortlicher für die Initiierung und die Umsetzung festgelegt und

ebenfalls ein Datum für Beginn und Fertigstellung der Umsetzung genannt werden. Nach Abschluss der Maßnahme wird ein Überwachungsverantwortlicher informiert.

An der Universität Bamberg wurden die zu den universellen Aspekten von ISIS12 zu zählenden organisatorischen Defizite bereits weitgehend aufgearbeitet: Dokumentationen wurden erstellt, Nutzungsrichtlinien angepasst und darauf aufbauend Konzepte umgesetzt sowie Leitfäden für Nutzende und Systembetreibende auf den Intranetseiten veröffentlicht. Je nach Zielgruppe lassen sich die Dokumente in drei Anwendungsbereiche unterteilen: 1) Dokumente, die die gesamte Universität bzw. alle Angehörigen der Universität betreffen, 2) Dokumente, die Regeln für die Nutzung der IT festlegen, sowie 3) Dokumente, die vorrangig von den Personen zu beachten sind, die selbst IT-Systeme oder IT-Dienste betreiben. Zum Anwendungsbereich 1 zählend wurden an der Universität Bamberg folgende Dokumente entwickelt:

- die IT-Sicherheitsleitlinie [M 2.192]
- ein IT-Betriebskonzept [M 2.214]
- ein IT-Sicherheitskonzept [M 2.195]
- ein „Leitfaden zu Geschäftsgang“ als Ersatz für eine Richtlinie zur Klassifizierung und zum Austausch von Dokumenten [M 2.393]
- eine Cloud-Nutzung-Strategie [M 2.534] und ein IT-Sicherheitskonzept für die Cloud-Nutzung [M 2.539]
- ein Datenschutzkonzept [M 2.503]
- eine Nutzungsrichtlinie [siehe Anwendungsbereich 2]
- eine Richtlinie zur Behandlung von IT-Sicherheitsvorfällen [M 6.121]
- eine Leitlinie zum Notfallmanagement [M 6.111]
- eine WLAN-Strategie [M 2.381]

Die Angaben in eckigen Klammern beziehen sich auf die jeweils zugrundeliegende BSI-Maßnahme. Die Verabschiedung der Dokumente des Anwendungsbereichs 1 durch die universitären Gremien steht zum Teil noch aus.

Gemäß ISIS12 sind auch für den Anwendungsbereich 2 „IT-Nutzer“ Richtlinien für spezifische Nutzungsszenarien zu erstellen. Um zu vermeiden, dass Nutzer bei der Einstellung mit einer Vielzahl von Richtlinien konfrontiert werden müssen, wurde entschieden, alle verbindlichen Vorgaben in abstrahierter Form in die schon vor dem ISIS12-Projekt vorhandenen „Nutzungsrichtlinien für Informationsverarbeitungssysteme“ zu integrieren. Konkrete Handlungsempfehlungen und Hilfe-

stellungen wurden in folgenden Leitfäden zusammengestellt und sind gemäß Nutzungsrichtlinie ebenfalls zu beachten:

- Leitfaden für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten [M 2.398]
- Leitfaden für die Cloud-Nutzung [M 2.535]
- Leitfaden für die mobile IT-Nutzung [M 2.309]
- Leitfaden für die Verwendung von VoIP-Software [M 2.373]
- Leitfaden zur alternierenden Wohnraum- und Telearbeit [M 1.44]
- Leitfaden zur Nutzung von Groupware [M 2.455]
- Leitfaden zur Terminalserver-Nutzung [M 2.464]
- Leitfaden zur VPN-Nutzung [M 2.418]
- Leitfaden zur WLAN-Nutzung M 2.382]

Die Vorgehensweise ist auch im Einklang mit der Grundausrichtung des ISIS12-Projekts, dass IT-Sicherheit nicht durch Androhung von Sanktionen, sondern durch die Verbesserung des Bewusstseins und der Befähigung aller Beteiligten im Umgang mit der IT erhöht werden soll. Die Aufteilung in eine Nutzungsrichtlinie, die durch Leitfäden ergänzt wird, bietet darüber hinaus die Vorteile, dass nur ein Dokument mehrsprachig vorgehalten werden muss und dass Änderungen an den konkreten Empfehlungen laufend und ohne Beteiligung weitere Gremien vorgenommen werden können.

Für den Anwendungsbereich 3 „IT-Systembetreiber“ sind gemäß ISIS12 bzw. BSI-Maßnahmenkatalog folgende Betriebskonzepte und -Anweisungen erstellt worden:

- Datennetze
    - Konzept für die sichere Anbindung und Nutzung des Internets [M 2.457]
    - Netz- und Netzmanagementkonzept für die Universität Bamberg [M 2.141]
    - Konzept für Sicherheitsgateways [M 2.70] sowie Regelungen für den Betrieb von Sicherheitsgateways [M 2.299]
    - Regelungen für den Betrieb der TK-Anlage [M 2.472]
    - Regelungen für den Betrieb von Routern und Switches [M 2.279]
    - Regelungen für ein Client-Server-Netz [M 2.322]
    - Regelungen zum VPN-Betrieb [M 2.416]
- Serverbetrieb
    - Minimaldatensicherungskonzept [M 6.26] und Konzept zur Datensicherung [M 6.33]

  - Notfallkonzept für Cloud Services [M 6.155]
  - Top-Down-Entwurf für die Planung eines Servereinsatzes [M 2.315]
  - Regelungen für den Betrieb eines allgemeinen Servers [M 2.316]
  - Regelungen für den Betrieb von Speichersystemen [M 2.525]
  - Regelungen für den Betrieb von Webservern [M 2.173]
  - Regelungen für die Einrichtung von Datenbankbenutzern und –benutzergruppen [M 2.132]
  - Regelungen für die Nutzung des Verzeichnisdiensts [M 2.405]
- Endgeräte
  - Sicherheitskonzept gegen Schadprogramme [M 2.154]
  - Regelungen für die Übergabe und Rücknahme eines tragbaren PCs [M 2.36]
- Allgemein
  - Notfallkonzept [M 6.114]
  - Regelungen für die Zugriffs- bzw. Zugangskontrolle [M 2.220]
  - Regelungen für die Durchführung von Wartungs- und Reparaturarbeiten [M 2.4]
  - Regelungen für den Einsatz von Fremdpersonal [M 2.226]

Für den Umgang mit IT-Sicherheitsvorfällen und Datenpannen wurden Prozesse modelliert und im Rahmen des Prozessmanagements im Ticketsystem (OTRS) umgesetzt.

Viele kleinere technische Maßnahmen wurden im Projektverlauf „nebenher“ erledigt. Es verbleiben noch eine Reihe von größeren Maßnahmen, die im Rahmen separater Umsetzungsprojekte im Laufe weiterer ISIS12-Revisionen bzw. des kontinuierlichen Verbesserungsprozesses angegangen werden müssen. Dies betrifft bspw. ein zentrales Passwort-Management, ein hochschulweites Drucker-Management oder ein durchgängiges Software- und Lizenz-Management.

Schritt 12: Revision

Das ISIS12-Rahmenwerk sieht vor, dass die Schritte 1 bis 11 einem regelmäßig zu wiederholenden Review unterzogen werden. Für jeden Schritt ist dabei ein Revisionsdatum nebst verantwortlicher Person anzugeben. Zum Abschluss des Zyklus soll ein Bericht verfasst werden, der die Aktivitäten des IT-Sicherheitsbeauftragten, also an der Universität Bamberg des IT-

Sicherheitsbeauftragten-Teams, und eine Zusammenfassung aller Sicherheitsvorfälle beinhaltet. Ebenfalls soll die allgemeine Bedrohungslage dargestellt werden.

4 Handlungsempfehlungen

Aus dem bisherigen Projektverlauf lassen sich einige grundlegende Empfehlungen zum Vorgehen geben:

- Beziehen Sie alle Interessengruppen (wie Personalrat, Datenschutz usw.) frühzeitig ein.
    - Ohne frühzeitige Beteiligung dieser Interessengruppen besteht die Gefahr, dass Aspekte nicht oder zu spät berücksichtigt werden, und dass das Projekt nicht in der Breite mitgetragen wird.
- Stellen Sie sicher, dass das Projekt von der Universitätsleitung nachdrücklich unterstützt wird.
    - Mit der Einführung eines ISMS sind tiefgreifende Eingriffe in Prozesse, Verhaltensregeln und Arbeitsweisen verbunden, die ohne Unterstützung der Universitätsleitung nicht durchsetzbar sind.
- Legen Sie den Geltungsbereich des Projekts fest, halten Sie ihn ein und orientieren Sie sich an der Struktur von ISIS12.
    - Es besteht die Gefahr, dass man sich in Randthemen verliert, weil Informationssicherheit überall eine Rolle spielt.
- Durchlaufen Sie die ISIS12-Schritte aufeinanderfolgend und legen Sie für jeden Schritt den angestrebten Umsetzungsgrad und Abschlusstermin fest.
    - Am Beispiel der IT-Betriebsdokumentation lässt sich leicht nachvollziehen, dass es permanent Potential für Verbesserungen geben wird. Ohne Vorgabe des erforderlichen Umsetzungsgrads und eines festen Termins drohen IT-Systembetreiber dauerhaft in diesem Prozessschritt hängenzubleiben.
- Kommunizieren Sie die Motivation für das ISMS, die Ziele und die Aufgaben in Richtung IT-Systembetreiber möglichst breit und direkt.
    - ISIS12 ist ein umfangreiches und komplexes Rahmenwerk. Beispielsweise wird bei ISIS12 einerseits von „Kritischen

Anwendungen“ gesprochen, mit denen die Geschäftsprozesse gemeint sind, und andererseits von „Anwendungen“, die sich auf die zur kritischen Infrastruktur gehörenden IT-Anwendungen (wie Mail, Office oder Fileservice) beziehen. Diese Komplexität birgt Potential für Missverständnisse. Der ursprüngliche Versuch, die Ziele und Aufgaben über Multiplikatoren zu kommunizieren, ist daher fehlgeschlagen. Dies hat vor allem in Schritt 7 bei einigen Administratoren für viel Frust gesorgt. Erst nach der Etablierung von wöchentlichen Treffen mit den verantwortlichen Administratoren haben alle wieder motiviert am Projekt mitgewirkt.

- Achten Sie darauf, dass die Sicherheitsmaßnahmen in Relation zum Schutzbedarf bzw. Risiko angemessen bleiben. Orientieren Sie sich dabei, soweit es noch vertretbar ist, an den an der Universität bereits etablierten und akzeptierten Regelungen.
    - Die IT ist Mittel zum Zweck. Einhundertprozentige Sicherheit gibt es nicht. Die Maßnahmen dürfen die Anforderungen der Nutzer nicht aus dem Blick verlieren, sonst geht die Akzeptanz verloren. Maßnahmen ohne Akzeptanz führen nicht zu mehr Sicherheit sondern zu Verunsicherung, Angst und Umgehungsstrategien.

5 Fazit

Nach den bisher beim ISIS12-Einführungsprojekt an der Universität Bamberg gewonnenen Erkenntnissen stellt ISIS12 einen sehr umfassenden und geeigneten Einstieg in das Informationssicherheitsmanagement dar. Dieser muss bei besonders kritischen Anwendungen und Daten noch ergänzt werden um Risikobetrachtungen und um über den BSI-Grundschutz hinausgehende technische und organisatorische Maßnahmen. Bei einer Hochschule von der Größe der Universität Bamberg mit über 50 Liegenschaften, etwa 3000 PC-Endgeräten und 300 virtuellen Servern sind einige Abstraktionen und Vereinfachungen erforderlich, um ISIS12 noch handhabbar zu halten. Mit diesen Vereinfachungen ist ISIS12 auch für größere Einrichtungen geeignet. Dies gilt nicht für das ISIS12-Tool, welches die 12 Verfahrensschritte im ISIS12-Prozess abbildet. Das Tool kommt an der Universität Bamberg nicht zum Einsatz, weil es nicht über eine Mehrbenutzerverwaltung verfügt und die Anzahl der verwaltbaren Objekte stark eingeschränkt ist.

Das ISIS12-Rahmenwerk verwendet ausgewählte Maßnahmen aus den BSI IT-Grundschutzkatalogen. Es bietet somit keine Vereinfachung in Form von Umsetzungshinweisen, wie es mit dem IT-Grundschutz-Kompendium der Fall ist. Die Anzahl der Maßnahmen ist bei ISIS12 im Vergleich zum BSI-Grundschutz zwar radikal reduziert. Durch die Struktur des BSI-Maßnahmenkatalogs mit vielen Querverweisen ergibt sich aber indirekt doch die Notwendigkeit, zur Erfüllung einer in ISIS12 geforderten BSI-Maßnahme viele weitere BSI-Maßnahmen ebenfalls zu betrachten. Für die Version 2.0 des ISIS12-Rahmenwerks wird ein vom BSI-Grundschutz unabhängiger Maßnahmenkatalog entwickelt [10].

Im Projektverlauf hat sich das sequentiell in aufeinanderfolgenden Schritten vorgegebene Vorgehen als schwer umsetzbar gezeigt. So wurde beispielsweise bereits bei der Erstellung der Betriebsdokumentation das Erfordernis gesehen, allgemein gültige Vorgaben für den Betrieb von Servern, Netzen, Endgeräten usw. in Richtlinien und Leitfäden festzuschreiben. Eine Einzelbetrachtung aller kritischen Systeme hätte einen unverhältnismäßig großen Aufwand verursacht. Die Erstellung dieser Dokumente ist im regulären ISIS12-Ablauf erst im Rahmen der in Schritt 11 umzusetzenden Maßnahmen vorgesehen. Die Vermischung der Schritte birgt die Gefahr, dass der Projektfortschritt aufgrund von Unklarheiten bezüglich der aktuell konkret anstehenden Aufgaben verlangsamt wird.

Ein wichtiges Argument für die Auswahl von ISIS12 als umzusetzendes ISMS ist neben der Einfachheit der Eindruck, dass ISIS12 sehr konkrete und schrittweise überschaubare Vorgaben für die Umsetzung macht. Aufgrund der Vielfalt an kritischen Anwendungen und Systemen hat sich aber gezeigt, dass konkrete Maßnahmen in abstrahierten Konzepten zusammengefasst werden mussten. Beispielsweise würde die Beschreibung der Backup-Policy für jeden einzelnen Server einen unnötig großen Aufwand verursachen, wenn in einem allgemeinen Backup-Konzept die identische Vorgehensweise für einen großen Teil der Server und das zentrale Speichersystem auf einmal beschrieben werden kann. Insofern führten konkrete Maßnahmen zu verallgemeinerten Konzepten. Dies entspricht der umgekehrten Herangehensweise als beim Vorgehensmodell nach ISO/IEC 27001, bei dem von verallgemeinerten Konzepten ausgegangen wird, die dann konkret umgesetzt werden müssen.

Aus Sicht eines für den IT-Betrieb Verantwortlichen besteht darüber hinaus der größte Vorteil von ISIS12 gegenüber anderen ISMS-Rahmenwerken darin, dass neben der Informationssicherheit weitere organisatorische und betriebliche Aspekte in ausgewogenem Umfang mitbehandelt werden. Dies sind insbesondere die IT-Governance, die IT-Betriebsdokumentation, die

Einführung grundlegender Service-Management-Prozesse sowie Ansätze zur Notfallplanung.
Das ISIS12-Einführungsprojekt ist Ende 2019, d. h. nach 26 Monaten, noch nicht vollständig abgeschlossen. Die Schritte 1 bis 10 sind weitgehend erledigt. Auch große Teile der Umsetzungsmaßnahmen in Schritt 11 wurden bereits ausgeführt oder begonnen. Aktuell wird der Abschluss des Einführungsprojekts in Form eines Audits für Ende 2019 anvisiert. Der Hauptgrund für die Verzögerungen sind zu knappe Personalressourcen. Wesentliche Arbeiten bei der Einführung eines ISMS und bei der Aufrechterhaltung eines angemessenen Sicherheitsniveaus müssen von den IT-Administratoren erbracht werden.
Für eine Hochschule von der Größe der Universität Bamberg werden für ein adäquates Informationssicherheitsmanagement mindestens zwei zusätzliche Personen dauerhaft benötigt: ein hauptamtlicher IT-Sicherheitsbeauftragter und eine Person im operativen IT-Betrieb zur Unterstützung von Sicherheitsmaßnahmen. Ohne Ressourcen in diesem Umfang führt ein ISMS zu nur schwer vertretbaren Abstrichen bei anderen Aufgaben. Sogar Maßnahmen aus dem Bereich der technischen Informationssicherheit wurden an der Universität Bamberg durch das ISIS12-Einführungsprojekt verzögert.

6 Literaturverzeichnis

[1] Informationssicherheit als strategische Aufgabe der Hochschulleitung, https://www.hrk.de/positionen/beschluss/detail/informationssicherheit-als-strategische-aufgabe-der-hochschulleitung/, 11.11.2019.

[2] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf, 11.11.2019.

[3] Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE, 11.11.2019.

[4] Gesetz über die elektronische Verwaltung in Bayern (Bayerisches E-Government-Gesetz – BayEGovG), http://www.gesetze-bayern.de/Content/Document/BayEGovG/True, 11.11.2019.

[5] DFG: Informationsverarbeitung an Hochschulen – Organisation, Dienste und Systeme, Stellungnahme der Kommission für IT-Infrastruktur für 2016–2020, http://www.dfg.de/download/pdf/foerderung/programme/wgi/kfr_stellungnahme_2016_2020.pdf, 11.11.2019..

[6] Informationssicherheit an Bayerischen Hochschulen, unveröffentlicht.

[7] Gutachten zur Anwendbarkeit von ISIS12 in der öffentlichen Verwaltung, Fraunhofer AISEC, https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/16_Sitzung/05_Gutachten%20ISIS12.pdf, 11.11.2019.

[8] Präsentation ISIS12, Bayerischer IT-Sicherheitscluster e. V., unveröffentlicht.

[9] ISIS12-Handbuch, Handbuch zur effizienten Gestaltung von Informationssicherheit für Kleine und Mittlere Organisationen (KMO), Version 1.9 vom Juni 2018, über den IT-Sicherheitscluster (https://isis12.it-sicherheitscluster.de/isis12-downloads/, 11.11.2019) für Kommunen und öffentlich-rechtliche Körperschaften kostenlos erhältlich.

[10] ISIS12-Katalog, Version 1.5.1 vom September 2018, über den IT-Sicherheitscluster (https://isis12.it-sicherheitscluster.de/isis12-downloads/, 11.11.2019) für Kommunen und öffentlich-rechtliche Körperschaften kostenlos erhältlich.

[11] Flyer zu ISIS12, Bayerischer IT-Sicherheitscluster e. V., verlinkt auf https://isis12.it-sicherheitscluster.de/was-ist-isis12/, 11.11.2019.

[12] IT-Sicherheitsstrategie der Otto-Friedrich-Universität Bamberg, https://www.uni-bamberg.de/fileadmin/rz/allgemeines/IT-Sicherheitsstrategie.pdf, 11.11.2019.