Hochschulinformationssicherheits-programm – HISP

'Die Hochschulen kennen ihre Informationsrisiken und schaffen durch Informations-sicherheitsmanagement Vertrauen!'

Stabsstelle Informationssicherheit der bayerischen, staatlichen Hochschulen und Universitäten

Version 1.0

Datum	**Kommentar**
26.03.2020	Freigabe CIO Runde Universitäten Bayern
03.04.2020	Freigabe RZ-Leiter/ CIO Runde Hochschulen Bayern
16.07.2020	Information an UniBayern e.V.
20.07.2020	Information an Hochschule Bayern e.V.
10.04.2020	Information an StMWK

Inhaltsverzeichnis

1 Einordnung und Auftrag

Der Ministerratsbeschluss vom 19.1.2011 zur IT-Strategie der bayerischen Hochschulen schrieb fort, dass die Verantwortung für die Weiterentwicklung der IT-Infrastruktur bei den Hochschulen liegt. Demnach sind die Hochschulen und ihre Leitungen für die Gewährleistung der Informationssicherheit verantwortlich.

In Wahrnehmung dieser Verantwortung haben Universität Bayern e.V. und Hochschule Bayern e.V. das „Grundsatzpapier zur Informationssicherheit an bayerischen Hochschulen“ verabschiedet. Ausgehend von der besonderen Bedeutung wissenschaftlicher Daten und Informationen sind hierin die für Hochschulen spezifischen Risiken und die grundsätzlich zur Prävention bzw. zur Minimierung des Schadens im Fall eines Angriffs erforderlichen organisatorischen und technischen Maßnahmen allgemein beschrieben. Darüber hinaus werden die Hochschulen dazu aufgefordert, ein Informationssicherheitsmanagementsystem (ISMS) zu implementieren.

Die Etablierung eines ISMS orientiert sich idealerweise an den anerkannten Standards der ISO 2700X Reihe oder des BSI. In verschiedenen Aufgabenfeldern beschreiben sie das Vorgehen bei Risikoanalyse und -bewältigung und geben sehr konkrete organisatorische und technische Handlungsanweisungen. Ein ISMS unterstützt die nachhaltige Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus, indem es dazu anhält Maßnahmen zur Stärkung der Informationssicherheit zu definieren, umzusetzen und deren Wirkung regelmäßig zu überprüfen und gegebenenfalls anzupassen. Da die Standards technikneutral sind, sind die konzeptionellen Vorgaben für den konkreten Umsetzungsfall der jeweiligen Hochschule entsprechend deren organisatorischen, betrieblichen und technischen Gegebenheiten anzupassen. Hiermit sind für die Hochschulen insbesondere erhebliche organisatorische Aufwendungen verbunden.

Zur Unterstützung der Hochschulen bei der Einführung eines ISMS und Umsetzung konkreter Maßnahmen zur Gewährleistung der Informationssicherheit wurde die Stabstelle Informationssicherheit eingerichtet. Damit diese ihre Aufgaben strukturiert und − für die Hochschulen − möglichst ressourcenschonend wahrnehmen kann, wird die Einrichtung eines Hochschulinformationssicherheitsprogramms (HISP) vorgeschlagen, an dem sich die Hochschulen bei der Etablierung des ISMS richten sollen.

Das Hochschulinformationssicherheitsprogramm (HISP) beschreibt die Schritte zur Implementierung eines Informationssicherheitsmanagementsystems (ISMS) an Hochschulen und soll den Status und Umsetzungsgrad an den einzelnen Einrichtungen verfolgen.

Hierbei orientiert sich das HISP in seinem Aufbau an den Phasen, wie sie typischerweise für die Etablierung eines ISMS zu durchlaufen sind. Entsprechend den unterschiedlichen spezifischen Rahmenbedingungen kann der Einstieg der Hochschulen in diesen idealen Ablauf wahlfrei erfolgen. Das HISP gewährleistet, dass innerhalb eines überschaubaren Zeitraums grundsätzlich alle Phasen von allen Hochschulen abgearbeitet sind und damit die Vollständigkeit des lokalen hochschulspezifischen ISMS gewährleistet ist.

Dieses Programm versteht sich nicht als Alternative zu bisher von einzelnen Hochschulen ergriffenen Schritten, sondern als deren Weiterführung und Detaillierung in den komplexen Umgebungen von Hochschulen mit ihren teilweise hohen Schutzanforderungen.

2 HISP - Programmschritte

2.1 Überblick

Sicherheit definiert sich als individuell erfahrener Zustand des Vertrauens und kann nicht allgemeingültig definiert werden. Es gibt Best Practice Ansätze, die dieses Vertrauen, das Richtige zu tun, stärken.

Folgt die Hochschulleitung diesem Sicherheitsprogramm der bayerischen Hochschulen, so wird sie zweckmäßigerweise alle definierten Schritte konsequent durchführen. Das Verharren in den ersten Schritten oder die Auswahl von leicht erreichbaren Zielen trägt zur kurzfristigen Verbesserung in Teilen bei, erzeugt aber keinen durchgängigen Prozess zur Gewährleistung der Informationssicherheit.

Beratende Unterstützung bei der Einführung und aktive Unterstützung in Form von Musterdokumenten und -prozessen sind über die zentrale Stabsstelle Informationssicherheit verfügbar. Diese Unterstützung ist als Hilfestellung gedacht und entbehrt nicht der lokalen Erstellung von Informationssicherheitskonzepten und Vor-Ort-Organisation der Informationssicherheit.

Das Sicherheitsprogramm gliedert sich in mehrere Schritte, die im Folgenden näher betrachtet werden.

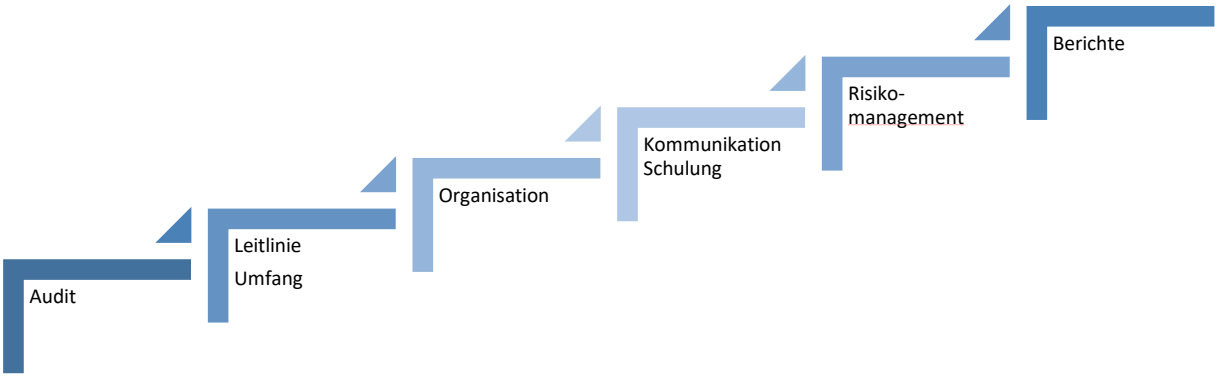

Abbildung 1: Programmschritte HISP

Das HISP unterstützt damit die vom BSI Grundschutz geforderten organisatorischen Anforderungen aus ‚ISMS.1: Sicherheitsmanagement' und ‚Organisation und Personal' (Bausteine ORP.1-3) und erlaubt die Anwendung weiterer Bausteine zur Erfüllung notwendiger Maßnahmen. Deren Umfang muss in der Schutzbedarfsanalyse im Rahmen des Risikomanagements festgelegt werden.

2.2 Bestandsaufnahme (Audits)

Zu Beginn der Einführung eines Informationssicherheitsmanagementsystems wird empfohlen ein optionales Audit (primäre Bestandsaufnahme) durchzuführen. Die daraus resultierenden Erkenntnisse über kritische oder bereits ausgereifte Strukturen können Aufschluss über zu priorisierende Brennpunkte liefern und dabei helfen ein Verständnis zur Sichtweise des Standards zu entwickeln. Seit 2017 hat die Stabsstelle Informationssicherheit an einem Drittel der Hochschulen erste Bestandsaufnahmen zur Informationssicherheit durchgeführt.

Nachfolgende Audits sollten an allen Hochschulen in einem 2-3 Jahresrhythmus obligatorisch stattfinden, um eine unabhängige Überprüfung zum Stand der Informationssicherheit zu

gewährleisten. Idealerweise werden diese Audits, neben der Stabstelle IT-Sicherheit, zusätzlich von hochschulansässigen ISO27001 Auditoren (derzeit LRZ, Univ. Bayreuth, Stabsstelle Informationssicherheit) alternierend durchgeführt.

2.3 Leitlinie

Im Arbeitskreis Informationssicherheit wurde gemeinsam von den Informations- / IT-Sicherheitsbeauftragten ein Leitlinienmuster entwickelt. Selbst wenn eine entsprechende Leitlinie vorhanden ist, sollte diese gegen das Muster auf Aktualität geprüft werden.

Damit einhergehend muss ein Projektauftrag zur Entwicklung eines an die eigene Einrichtung angepassten ISMS erteilt werden. Als Basis für den Grobprojektplan können die Schritte des HISP dienen.

Die Leitlinie soll die gesamte Hochschule erfassen und alle Hochschulangehörige einbeziehen. Dieser große Umfang kann bei der Einführung eines ISMS mit resultierenden Umsetzungsmaßnahmen hinderlich sein. Daher wird empfohlen mit notwendigen, etablierten und möglichst zentralen IT-Dienstleistungen bzw. Verfahren der Informationsverarbeitung (wie zentrale Benutzerverwaltung, Netzwerkmanagement und Campusmanagement) zu beginnen und das ISMS für einen begrenzten kontrollierbaren Bereich einzuführen.

2.4 Organisation

Es sind Voraussetzungen und Eckpunkte für das zu erreichende Schutzniveau festzulegen, da Sicherheitsmaßnahmen sich nach dem Wert oder Schutzbedarf von Informationen richten. Diese Aufgaben können von der Hochschulleitung an eine in der Hochschule etablierte oder festzulegende Organisationstruktur delegiert werden. Diese Struktur mit Funktionen (wie Informationssicherheitsbeauftragter), Gremien und Aufgaben muss in einer Regelung dokumentiert und anerkannt werden.

Eine Musterregelung wird von der Stabsstelle Informationssicherheit zur Verfügung gestellt und muss lokal überarbeitet und anpasst werden.

2.5 Kommunikation / Schulung

Sicherheit wird durch technische und organisatorische Maßnahmen erreicht. Es sind Schulungen und Kommunikationskanäle der Informationssicherheitsmaßnahmen zu etablieren, damit ein sicherheitsbewusster Betrieb von beteiligten Personen unterstützt wird.

Die Stabsstelle Informationssicherheit stellt dafür ein Schulungs- und Datenschutzkonzept zur Verfügung. Diese können in bestehende Lernprogramme (Moodle) integriert werden. Die Verbindlichkeit an der Teilnahme derartiger Schulungsangebote ist an der jeweiligen Einrichtung festzulegen.

2.6 Risikomanagement

Der späte Einstieg in das Risikomanagement begründet sich in der Erkenntnis aus der Bestandsaufnahme von 2017, dass an allen überprüften Hochschulen Ansätze zum Umgang mit Risiken vorhanden sind und das Thema prinzipiell informell und nach Maßgabe der handelnden Personen gehandhabt wird. Die dazu vorhandenen Maßnahmen werden im Programmablauf von HISP im Schritt 1 ‚Audit' entsprechend beurteilt.

Basis für die Identifizierung, Erfassung, Bewertung und Behandlung der Risiken der eigenen Hochschule müssen eine Schutzbedarfsanalyse und die dokumentierten Bedrohungs-

szenarien sein. Als Ergebnis werden neue oder verbesserte Maßnahmen geplant. Eine Unterstützung für konkrete Maßnahmen kann aus dem BSI IT-Grundschutzprofil für Hochschulen entnommen werden.

Erfahrungen aus verschiedenen Risikomanagementwerkzeugen werden von der Stabsstelle Informationssicherheit zur Verfügung gestellt und bei Bedarf kann ein Rahmenvertrag für alle oder sich beteiligende Hochschulen in Bayern ausgehandelt werden.

2.7 Berichte, Verbesserung

Bereits im Aufbau des ISMS ist auf mögliche Berichtspunkte Rücksicht zu nehmen. Sinnvolle Kontrollen zur Wirksamkeit der verschiedenen Prozesse und Maßnahmen sind auszuwählen und regelmäßig zu überprüfen. Eine Hilfestellung bei der Auswahl geeigneter Schlüsselindikatoren wird von der zentralen Stabsstelle Informationssicherheit zur Verfügung gestellt. Alternativ hilft der ISO27004 Standard bei der Entwicklung von Kennzahlen.

Für unabhängige interne Audits wird empfohlen, einen Pool an ISO27001 Auditoren innerhalb der Hochschulen Bayerns zur gegenseitigen Unterstützung bei der Außenbetrachtung aufzubauen. Zur Bewertung des Umsetzungsgrades an den jeweiligen Hochschulen und zur besseren Vergleichbarkeit der bayerischen Hochschulen untereinander (‚Sicherheitslandkarte') wird ein allgemeines Reifegradmodell (siehe ‚3.1 Reifegradmodell') verwendet.

2.8 Sukzessiver Aufbau eines hochschulweiten ISMS

Ein betriebenes ISMS kann schrittweise auf die gesamte Hochschule implementiert werden, indem erfolgreich entwickelte Punkte des Managementsystems aus den Start-/Referenzeinrichtungen auf andere Bereiche ausgeweitet werden.

Darüber hinaus stellt ein gelebter, kontinuierlicher Verbesserungsprozess sicher, dass bei der Einführung des ISMS vorrangig Brennpunkte behoben werden und im weiteren Verlauf eine Vertiefung hinsichtlich eines erhöhten Schutzstandards stattfindet.

Bei aufkommenden neuen Anforderungen müssen diese bewertet und notwendige Änderungen im Referenzbereich – und später auf alle anderen Bereiche - umgesetzt werden. Notwendige Abweichungen der erstellten Informationssicherheitskonzepte sind entsprechend der Vorgaben des Risikomanagements zu bewerten und dokumentieren.

3 Rahmenbedingungen zur Feststellung des Fortschritts

3.1 Reifegradmodell

2017 wurden an einem Drittel der Hochschulen Kurzaudits zur Bestandsaufnahme durchgeführt. Es konnten folgende Rückschlüsse gezogen werden:

Die Hochschulen bieten zentrale Dienste und Unterstützung im Betrieb von IT-Systemen für den Lehr- und Forschungsbetrieb sowie der Verwaltung an. Systematische oder organisatorisch für die gesamte Hochschule umfassende Vorgehensweisen sind kaum umgesetzt. Es liegt derzeit an einzelnen Informations-/IT-Sicherheitsbeauftragten (oder nahestehenden RZ-Leitern) eine Organisationsänderung zu erreichen oder Arbeitsabläufe nach Informationssicherheitsgesichtspunkten zu strukturieren und zu dokumentieren. Technische Verbesserungen und Fortschritt finden im Rahmen der jeweiligen Möglichkeiten (Budget) und des individuellen Know-Hows (Wissensstand der einzelnen Administratoren) statt. So sind vor allem technisch gut entwickelte Lösungen entstanden, die oft auf dem Wissen Einzelner ruhen. Dies gilt im gleichen Maße für IT-Sicherheitslösungen.

Inzwischen ist es dringend notwendig, einen kontinuierlichen und vor allem umfassenden Verbesserungsprozess zu starten, der nicht auf Insellösungen von Einzelnen beruht, sondern der flächendeckend auf die gesamte Hochschule ausgebreitet wird. Nur durch die Einführung eines Informationssicherheitsmanagementsystems (ISMS) kann ein derart strukturiertes Vorgehen gewährleistet werden.

In der Folge werden die zukünftigen Audits zur regelmäßigen Bestandsaufnahme (extern oder Selbsteinschätzung) mit dem Reifegradmodell nach ISO/IEC 21827 bewertet und in den CIO Runden zur Verfügung gestellt (‚Sicherheitslandkarte'). Diese Vorgehensweise wird eine Vergleichbarkeit untereinander und einen übersichtlichen Status im Detail unabhängig von der umgesetzten Norm erlauben.

Basierend auf der ISO/IEC21827:2008 (System Security Engineering – Capability Maturity Modell, kurz: SSE-CMM) sieht das Reifegradmodell wie folgt aus:

Reifegrad	**Bedeutung n. ISO21827**
Nicht vorhanden	Keine Sicherheitsmaßnahmen oder Pläne sind vorhanden.
Informell	Grundlegende Schutzmaßnahmen sind vorhanden und werden **ad hoc** umgesetzt. Es gibt allgemeine Regelungen zur Durchführung bestimmter Tätigkeiten. Es gibt keine Anpassung, Verfolgung oder Berichte darüber.
Geplant	Grundlegende Schutzmaßnahmen werden geplant, eingeführt und sind **wiederverwendbar**.
Dokumentiert	Zusätzlich zur Planung und Verfolgung gibt es **dokumentierte, genehmigte** und **hochschulweit** implementierte Prozesse.
Quantitativ überwacht	Zusätzlich zur Dokumentation sind die Prozesse **messbar** und **überprüft** (z.B. Audit)
Kontinuierlich verbessert	Die Prozesse werden **regelmäßig überprüft** und **angepasst**. Verbesserungen erfolgen als Antwort auf erkannte Auswirkungen von Schwachstellen

Abbildung 2: Übersicht über die Reifegradstufen nach SSE-CMM (ISO21827:2008)

3.2 Meilensteine

Das HISP ist an anerkannten Standards orientiert und gliedert sich in mehrere Schritte. Basierend auf den Erkenntnissen der Bestandsaufnahme von 2017 werden folgende Meilensteine definiert (Anm.: Die Jahreszahlen stellen Orientierungsgrößen für die Stabsstelle Informationssicherheit dar). Jede Hochschule kann parallel dazu oder abweichend Schritte zur Einführung treffen. Da der Status bei den einzelnen Hochschulen sehr unterschiedlich ist, wäre eine Bindung nicht zielführend.

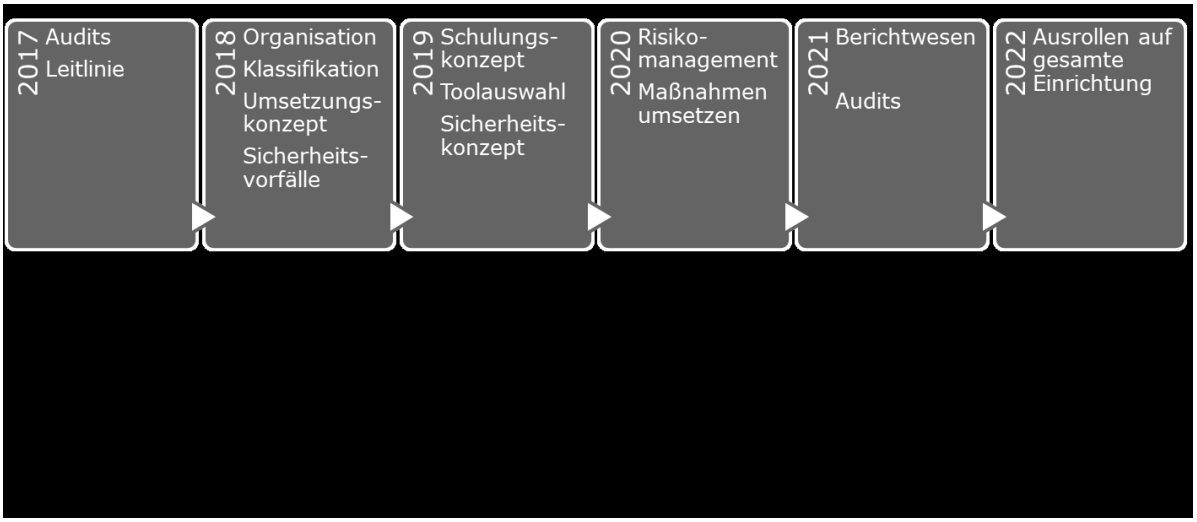

Abbildung 3: Meilensteine des Hochschulinformationssicherheitsprogramms

3.3 Verbesserung

Da das HISP einer mittelfristigen Laufzeit unterliegt, steht zu erwarten, dass sich Änderungen oder gemeinsame hochschulübergreifende Projekte oder Ausschreibungen entwickeln, um Synergien zu fördern. Die Zustimmung zu diesem Programm ermöglicht den Hochschulen die Teilnahme an entsprechenden Umsetzungsprojekten und zum Erwerb entsprechender Produkte, verpflichtet sie jedoch in keiner Weise. Der konkrete Bedarf und die Teilnahme an diesen ist im Rahmen der hochschulspezifischen Projektplanung zu erheben und soll die Weiterführung an einzelnen Hochschulen nicht behindern. Bei geänderten Rahmenbedingungen muss das Programm an neue Ziele und Anforderungen (wie Änderungen in zugrundeliegenden Standards) angepasst werden. Diese Überprüfung sollte in einem jährlichen zusammenfassenden Bericht an die CIO Runden stattfinden.

4 Weitere Schritte, Governance

Ein ISMS ist als kontinuierlicher Verbesserungsprozess der Informationssicherheit an Hochschulen zu verstehen. Um ein adäquates ISMS an einer Hochschule aufzubauen ist es unerlässlich, dass die jeweilige Hochschulleitung Prozesse zur Bewertung, Steuerung und Überwachung etabliert.

So kann eine Informationssicherheitsgovernance in Verbindung mit der IT-Strategie zur effektiven Steuerung von Ressourcen etabliert werden (siehe ISO27014:2013 Standard).

Dabei sind folgende Prinzipien zu beachten:

- Letztendlich Einführung für die gesamte Hochschule
- Risikobasierter Ansatz
- Steuerung von Ausgaben
- Übereinstimmung mit internen und externen Anforderungen
- Fördern eines sicherheitsbewussten Umfelds
- Überprüfung der Wirksamkeit im Verhältnis zu Anforderungen

Die Stabsstelle Informationssicherheit bietet bei der Implementierung eines ISMS und den daraus resultierenden Umsetzungsmaßnahmen gezielte Angebotsleistungen an, um die Hochschulen bei der Einführung zu unterstützen. Die Leistungen umfassen etwa die Bereitstellung von Dokumentvorlagen, die Abstimmung bei der Bewertung von Risiken mit Blick auf die Festlegung angemessener Schutzmaßnahmen oder die Koordinierung bei der Auswahl von Softwarewerkzeugen. Darüber hinaus können Auditierungen zur Erfassung des erreichten Status der Informationssicherheit durchgeführt, bzw. angeleitet werden. Die kontinuierliche Fortschreibung dieses Angebots liegt in der Verantwortung der Stabstelle.