Konzepteinreichung HITS IS

Inhaltsverzeichnis

1 Informationssicherheit mit HITS IS

Die Hochschulen befinden sich, als wesentlicher Teil der Informationsgesellschaft, mit den bei ihnen verfügbaren Informationen, Datensammlungen und vor allem Forschungsergebnissen zunehmend im Fokus von Angreifern und werden zunehmend mit professionalisierten und individualisierten Angriffen auf ihre IT konfrontiert. Aufgrund ihrer Nutzerstruktur, ihrer Anforderungen aus Lehre und Forschung sowie ihrer für Angreifer interessanten Infrastruktur ergeben sich für die Hochschulen besondere Herausforderungen zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit der Informationen.

Gleichzeitig nimmt die Komplexität der Erfordernisse zur Gewährleistung der Informationssicherheit stetig zu, was die Hochschulen auf der Basis begrenzter Ressourcen und bei gleichzeitig wachsendem IT-Einsatz in Forschung, Lehre, Studium und Verwaltung ohne zusätzliche Unterstützung vor kaum lösbare Herausforderungen stellt.

Durch die Etablierung eines hochschulübergreifenden IT-Services für Informationssicherheit (HITS IS) können Kompetenzen, die an allen Hochschulstandorten benötigt werden, gebündelt aufgebaut und den an den einzelnen Hochschulstandorten mit der Informationssicherheit betrauten Beschäftigten der Hochschulen als Serviceleistung zur Verfügung gestellt werden.

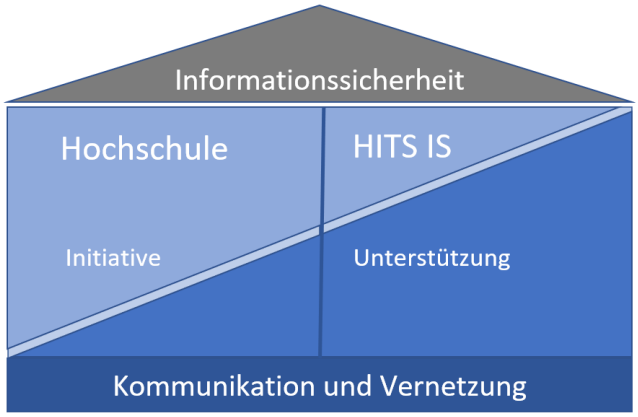

Abbildung 1: Zusammenarbeit HITS IS und Hochschulen

Das vorgeschlagene HITS IS koordiniert die bayernweite Kommunikation im Themenfeld der Informationssicherheit, stellt technisches und prozessorientiertes Spezialwissen zur Informationssicherheit zur Verfügung und fördert und fordert sowohl den Wissensaufbau als auch den Wissensaustausch in einem bayernweiten Netzwerk der Informationssicherheitsspezialisten der Hochschulen. Es unterstützt Hochschulen einerseits auf deren Anfrage, andererseits agiert es selbst initiativ.

Konkrete Unterstützungsleistungen für die Hochschulen sind zunächst:

- Eine Hochschule möchte die Informationssicherheit durch den Aufbau eines ISMS stärken
  - das HITS IS ist Ansprechpartner, unterstützt bei den Prozessen und bei der Koordination. Technische Dienstleistungen können genutzt werden.
- Eine Hochschule möchte ihre Netze und kritischen Systeme auf Schwachstellen prüfen
  - das HITS IS hilft bei der Planung, führt Schwachstellenscans durch und arbeitet bei der Verbesserung (Prozesse und Technik) mit.
- Ein (schwerwiegender) Sicherheitsvorfall tritt ein
  - das HITS IS unterstützt in der Aufarbeitung, Kommunikation, Analyse und Behebung des Sicherheitsvorfalls.

Neben den unterstützenden Leistungen agiert das HITS IS vorerst initiativ bei:

- Empfehlungen für Maßnahmen zum Umgang mit aktuellen Gefahren werden erarbeitet und kommuniziert
- Wichtige übergreifende Themenfelder und Zukunftsthemen werden betrachtet, in Studien ausgearbeitet und weiterbearbeitet, z.B. Managed Firewall.

Wie das HITS IS mit den Hochschulen zusammenarbeitet, zeigt exemplarisch der folgende Ablauf zur Bearbeitung eines hypothetischen Sicherheitsvorfalls, von dem gleichzeitig mehrere Hochschulen betroffen sind.

(Schwerwiegender) Vorfall tritt ein --> HITS Unterstützung in Ausarbeitung, Kommunikation, Analyse und Behebung	Führung durch
Die Hochschule ergreift erste Maßnahmen anhand des lokalen Maßnahmenplans der Hochschule.	HS
Der Verantwortliche an der Hochschule informiert innerhalb der eigenen Hochschule und informiert das HITS IS.	HS
HITS IS erfasst und dokumentiert den von der betroffenen Hochschule gemeldeten Vorfall.	HITS IS
Das HITS IS bietet ergänzende Unterstützungsmaßnahmen an und spricht Empfehlungen aufgrund der bisherigen Erfahrungen und Best Practices aus (Einschätzung des Vorfalls und der Auswirkungen, wirksame Maßnahmen zur Mitigation, insbesondere Isolation betroffener Systeme zum Schutz noch nicht betroffener Systeme und der dort verarbeiteten Daten, die Verhinderung der Ausweitung der Angriffe, die Beseitigung von Schäden, Aktivieren von Wiederanlaufplänen).	HITS IS
Die Umsetzung der empfohlenen lokalen Maßnahmen erfolgt unter der Verantwortung der Hochschule.	HS
Aufgrund weiterer Hinweise anderer bayerischer Hochschulen stellt das HITS IS fest, dass es sich um einen Vorfall handelt, von dem mehrere Hochschulen betroffen sind. Aus diesem Grund priorisiert das HITS IS den Vorfall und leitet zusammen mit dem für Informationssicherheit zuständigen Personal der Hochschulen gemeinsame bayernweite Maßnahmen ein und übernimmt für diese die hochschulübergreifende Koordination, Kommunikation und technische Unterstützung.	HITS IS
Die Umsetzung der empfohlenen lokalen Maßnahmen erfolgt unter der Verantwortung der Hochschule.	HS
Die Erkenntnisse fließen in das Lagebild, in einen Tätigkeitsbericht und Empfehlungen ein, um ähnliche Vorfälle in der Zukunft zu vermeiden.	HITS IS

Tabelle 1: Beispiel der Zusammenarbeit Hochschulen <-> HITS IS

1.1 HITS IS – Zusammenwirken von LRZ, HSA und UniA

Das vorgeschlagene HITS IS ist über die Einrichtungen Leibniz-Rechenzentrum, Hochschule Augsburg und Universität Augsburg verteilt. Diese drei Partner bringen eine übergreifende Expertise im Bereich der Informationssicherheit (siehe unten) ein.

Gute Informationssicherheit erfordert stets ein enges Zusammenspiel von Organisationen, Prozessen und den gewählten technischen Verfahren. Das HITS IS wird dem durch seine stark vernetzte und aufeinander aufbauende Arbeitsweise intern sowie in der einheitlichen Wirkungsweise nach außen Rechnung tragen. Auch wenn das HITS IS über die genannten drei Partnereinrichtungen verteilt ist, sollen die bayerischen Hochschulen als Kunde immer durchgängige Leistungen erhalten.

Zur Kommunikation zwischen HITS IS und den Hochschulen werden seitens der Hochschulen spezifische Ansprechpartner benannt. In der Regel sind dies die Informationssicherheits-beauftragten (ISB) bzw. CISOs der jeweiligen Hochschulen.

Das HITS IS ist technisch (SOC) und prozessorientiert (ISMS) ausgerichtet, mit jeweils gutem gegenseitigem Verständnis beider Aufgabenbereiche.

So werden z.B. Schwachstellenscans organisatorisch geplant, technisch mit ausgewählten Tools durchgeführt, ausgewertet und anschließend in konkrete Verbesserungen an den Prozessen oder der eingesetzten Technik überführt.

Das HITS IS unterstützt sowohl durch die ihm zur Verfügung stehenden Ressourcen als auch durch die Steuerung der Zusammenarbeit zwischen den Hochschulen und dem LKA, LSI, CAZ und anderen behördennahen Einrichtungen. Ferner wird die sensible Kommunikation gesteuert.

Vorteile durch die vorgeschlagene Struktur des HITS IS:

- Bewährte Stabsstelle Informationssicherheit, integriert in den Hochschulstandort Augsburg wird weitergeführt.
- Weitreichender Abdeckungsgrad
    - Unterschiedliche Größen (Studenten und RZ) werden abgedeckt
    - HAWs und Universitäten sind berücksichtigt
    - Räumliche Nähe untereinander
- Befähigungen in der Informationssicherheit
    - Erfahrene und zertifizierte Mitarbeiter (ISO27001 Auditor, DSB, Datenschutz-Auditor)
    - Sicherheitscluster HSA_innos befindet sich an der HSA
    - Lehrstühle mit Sicherheitsfokus
    - Gute Vernetzung mit Sicherheitsstellen, auch im privatwirtschaftlichen Bereich
    - Aktuelles Neubauprojekt Rechenzentrum (UniA) mit geplanter Zertifizierung nach DIN EN 50600
- Weitere Befähigungen
    - Medienlabore zur professionellen Erstellung von Trainingsmaterial
    - Pädagogik und Didaktik Lehrstühle
    - Bewährte Zusammenarbeit zw. HSA und UniA
    - Nähe zur Universitätsmedizin (UniA)
- Bayernweite Projekte und Dienste
    - Bayern-SOC, DNSSEC/DANE
    - BayernShare
    - HITS IT-Beschaffung
- Europäische Forschungsprojekte
    - GÉANT (u.a. Security-Baseline, DDoS-Abwehr mit Firewall-on-demand, Vulnerarbility Management as a service)
    - CONCORDIA (u.a. Cyber-Ranges, Virtual Labs und Security-Tools)

1.2 Commitment und Unterstützung der Leitungen

Die zur Einrichtung des HITS IS ausgewählten Partner Hochschule Augsburg, Leibniz Rechenzentrum und Universität Augsburg haben intensiv an der Ausgestaltung der bayerischen IT-Strategie beteiligt und geben im Zuge ihrer Beteiligungszusage zum HITS IS ein klares Commitment zur bayerischen IT-Strategie sowie zum zukünftigen, im Rahmen der Umsetzung der IT-Strategie einzurichtenden Digitalverbund der bayerischen Hochschulen ab.

Die drei Partnereinrichtungen unterstützen den hochschulübergreifenden IT-Service Informations-sicherheit, greifen nicht unmittelbar in dessen Governance ein und stellen an den jeweiligen Standorten adäquate Arbeitsrahmenbedingungen für die Mitarbeiter des HITS IS zur Verfügung.

2 Aufgaben des HITS IS

2.1 Aufgabenbereiche und Zusammenarbeit

Der Austausch und die Vernetzung der technischen (SOC) und organisatorischen Aufgabenbereiche (ISMS) ist notwendig, um eine ganzheitliche Sicht zur Bedarfslage der bayerischen Hochschulen zu erhalten. Die technischen und organisatorischen Aufgabenbereiche sind komplementär für die Umsetzung der Informationssicherheitsaufgaben notwendig. Ohne Einbettung von technischen Maßnahmen, wie Schwachstellenscans in eine hochschulweite Informationssicherheitsorganisation, ist der Effekt von technischen Erkenntnissen zur Behebung von Sicherheitsproblemen fraglich.

Ein interner Austausch ist daher wichtig und wird durch die HITS interne Steuerung über die bestehende Stabsstelle Informationssicherheit in Zusammenarbeit mit Forschern der Hochschule Augsburg dem Rechenzentrum der Universität Augsburg und dem LRZ sichergestellt.

Die nachfolgende Grafik veranschaulicht die übergreifenden Aufgabenbereiche und intern notwendige Zusammenarbeit im HITS IS:

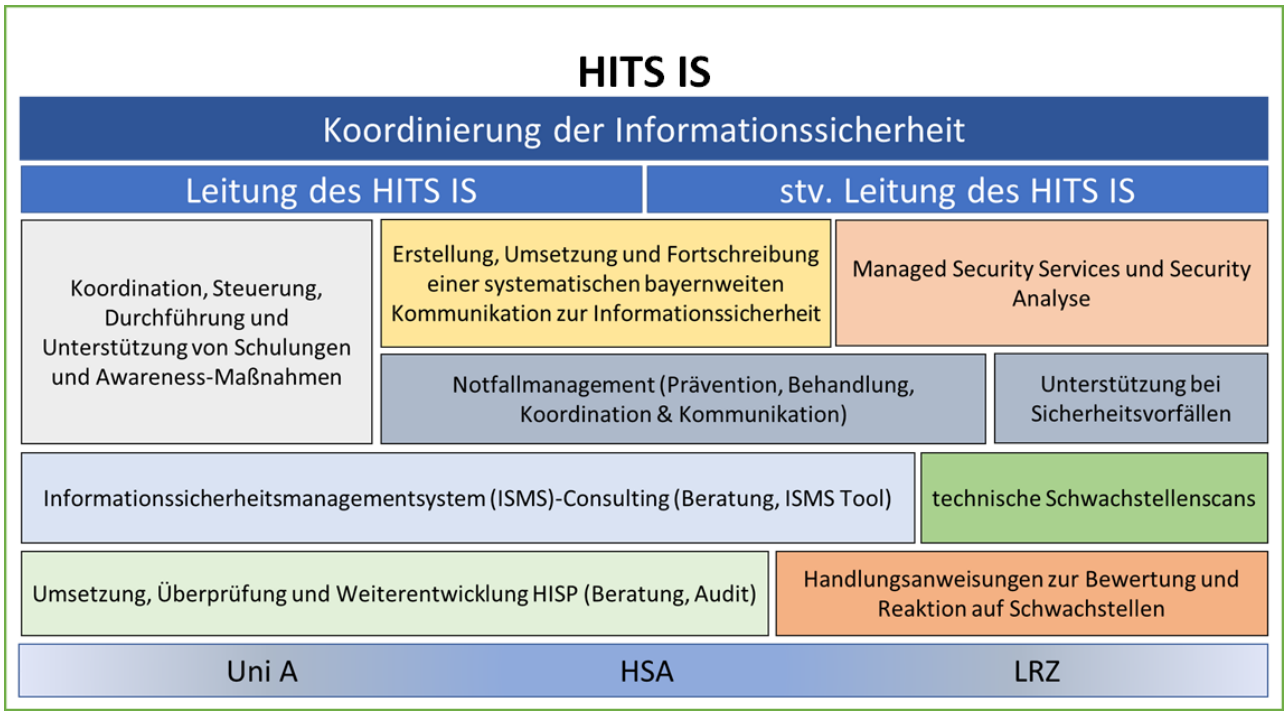

Abbildung 2: Aufgabenbereiche und Zusammenarbeit im HITS IS

2.2 Koordinierung der Informationssicherheit

Damit die technischen und organisatorischen Dienste des HITS IS dem Auftrag des leitenden Gremiums folgen, ist die zusammenhängende Planung, Organisation und Koordination beider Aufgabenbereiche des HITS IS unumgänglich. Eine enge Zusammenarbeit mit dem Service Delivery der einzelnen Aufgaben kann durch die kleinteilige Struktur des HITS IS gewährleistet werden, wenn die Steuerungsfunktionen zentral für technische und organisatorische Aufgabenbereiche erfolgt und die Arbeitsabläufe kontrolliert werden. So können bayernweit vergleichbare Ergebnisse aus den Aufgaben, die für einzelne Hochschulen erbracht werden an das leitende Gremium berichtet werden.

Die bereits an bayerischen Hochschulen angesiedelte Rolle des/der Informationssicherheitsbeauftragten (ISB) ist als qualifizierter lokaler Ansprechpartner von den teilnehmenden Einrichtungen festzulegen. Nur auf Basis dieser lokalen technischer Expertise und dem Verständnis der Gegebenheiten an den Hochschulen kann effektiv und zielführend unterstützt werden. So können zum Beispiel technische IT-Sicherheit Schwachstellenscans nur effektiv durchgeführt werden, wenn die lokale Struktur verstanden wurde. Gleichzeitig wird die technische hochschulübergreifende Expertise benötigt, um mögliche Schwachstellen nach der Identifikation zu bewerten und ggf. zu beheben. Im selben Sinne sind organisatorische, insbesondere ISMS und Notfallmanagement,

Aufgabenbereiche nur in Kooperation zwischen lokalen Verantwortlichen mit Prozesswissen und hochschulübergreifender Expertise bayernweit zu bewältigen.

Die Aufgaben und die strategische Zielrichtung des SOCs müssen der Informationssicherheits-strategie (siehe IT-Strategie der bayerischen Hochschulen) folgen und wie die anderen Dienste des HITS IS zentral gesteuert werden, um mit den organisatorischen Aufgaben zu korrelieren. So können aus den bayernweiten Erkenntnissen über Schwachstellen neuartiger Bedarf an das leitende Gremium kommuniziert und neue Aufgaben (z.B. Informationskampagnen, Verbesserungen der IT-Sicherheitsprozesse, Umsetzungsunterstützungsprojekte) durch das Gremium priorisiert werden.

Für einen bayernweiten Überblick und eine rasche Reaktion auf Sicherheitsereignisse, ist es wichtig, bei technischen Analysen oder Scans zielgerichtet alle Einrichtungen und Angriffspunkte einzubeziehen.

Über die kurzen Wege der internen Kommunikation des HITS IS mit dem leitenden Gremium (aus dem Digitalverbund) können bayernweite Aufträge zur aktuellen Verwundbarkeit angenommen, abgearbeitet und zeitnah kommuniziert werden (z.B. alle über das Internet erreichbaren Spoolerdienste der Hochschulen).

2.3 HITS IS: Aufgabenbereich SOC

Im Allgemeinen überwacht ein Security Operations Center (SOC) zentral IT-Ressourcen und -Infrastrukturen und analysiert die von den installierten Sicherheitsmechanismen gemeldeten Auffälligkeiten. Durch werkzeuggestützte, systematische Analyse und zeitliche Korrelation werden Ereignismeldungen zueinander in Beziehung gesetzt. Dies erhöht die Aussagekraft sowie die Reaktionsgeschwindigkeit bei gleichzeitiger Reduktion der Anzahl an Fehlalarmen. Unter Einsatz von Threat Intelligence Informationen können die korrelierten Ereignisse noch weiter mit Zusatz-information angereichert werden. Zudem können diese zentral gesammelten und korrelierten Ereignisse in Kombination mit den Ergebnissen regelmäßig oder anlassbezogen durchgeführter Schwachstellenscans der Erstellung eines organisations- bzw. infrastrukturweiten Sicherheitslagebilds dienen. Der Aufbau eines auf dem erstellten Lagebild basierenden Frühwarn-systems rundet das grundlegende Aufgabenspektrum eines SOC ab und kann eine Organisation, z.B. eine Hochschule frühzeitig(er) auf drohende Angriffswellen vorbereiten.

Das HITS IS SOC unterstützt lokal tätiges Sicherheitspersonal. Dort werden bereits Security-Monitoring und -analysesysteme betrieben und den von diesen erkannten Auffälligkeiten nach-gegangen. HITS IS SOC reichert diese Auffälligkeiten etwa durch Scanergebnisse von Schwach-stellenscans an und hilft Hochschulen beim Finden und der Umsetzung zugeschnittener Gegenmaßnahmen oder beim Behandeln eingetretener Sicherheitsvorfälle.

2.3.1 Unterstützung bei Sicherheitsvorfällen

Erfolgreiche Angriffe und Kompromittierung von IT-Systemen sind keine Ausnahme. Sie treffen IT-Systeme an bayerischen Hochschulen und das oft zu ungünstigen Zeitpunkten, wenn die Zeit drängt und für die Behandlung kaum Personal zur Verfügung steht. Resultierende Sicherheitsereignisse und -vorfälle sind, sofern sich daraus merkliche Auswirkungen in den Abläufen der Hochschulen ergeben, zeitnah, strukturiert, effektiv und unter Effizienzgesichtspunkten zu behandeln. Die Analyse und Bewertung von Sicherheitsereignissen und die Reaktion auf die sich daraus ergebenden Sicherheitsvorfälle, ist in vielen Fällen aufwändig und erfordert Expertenwissen, das an den Hochschulen oftmals nicht in ausreichendem Maße vorhanden ist. Dieses aufwändige Unterfangen bindet sehr rasch, sehr viele und in der wirksamen Behandlung von Sicherheitsvorfällen nicht notwendigerweise ausgebildete personelle Ressourcen vor Ort. Dies beeinträchtigt die direkt involvierten Hochschulangehörigen in ihrer täglichen Arbeit und indirekt unter Umständen viele weitere Hochschulangehörige.

Die Reaktion auf Sicherheitsvorfälle weitet sich zudem sehr schnell aus. Den Datenschutz betreffende Fragen sind hierbei genauso oft und schnell zu beantworten wie die, die von ermittelnden Strafverfolgungsbehörden gestellt werden. Aus Sicherheitsvorfällen resultierende Notfall- und Krisensituationen erfordern zusätzliche Maßnahmen aus dem Notfallmanagement und die prozessübergreifende Abstimmung mehrerer Personen und Teams und eine vorfallsbezogene

Kommunikationsstrategie. Wichtig ist zudem die Sicherung von Beweisen, insbesondere zur Unterstützung der Arbeit zuständiger Ermittlungsbehörden. Abschließend sollen aus der Behandlung Erkenntnisse gezogen werden, um zukünftig, vergleichbare Angriffe und Vorfälle zu vermeiden. Damit verbunden sind die (Neu-)Bewertung von Risiken und die Ableitung konkreter (Schulungs- und Awareness-) Maßnahmen, die die Eintrittswahrscheinlichkeit gleichartiger Vorfälle senken können. Dieses sehr breite Aufgabenspektrum benötigt zur Bewältigung geschultes und geübtes Personal. Die zentralisierte Dokumentation dezentraler, an betroffenen Einrichtungen gewonnenen Analyseergebnisse beschleunigt die Bereitstellung notwendiger Informationen.

Die zentrale Unterstützung und Koordination durch das HITS IS bei der Behandlung von Sicherheitsvorfällen schöpft Synergien, bietet schnelle, strukturierte Reaktion durch ausgebildete und erfahrene Sicherheitsvorfalls- und Notfallexperten. Es entlastet und unterstützt das lokal in die Vorfallsbearbeitung einbezogene Personal der betroffenen Hochschule. Zu den Aufgaben dieser zentralen Unterstützung gehören konkrete Handlungsanweisungen für die Reaktion auf einen Angriff, wirksame Maßnahmen zur Mitigation, insbesondere Isolation betroffener Systeme zum Schutz nicht kompromittierter Systeme und dort verarbeiteter Daten, die Verhinderung der Ausweitung der Angriffe, die Beseitigung von Schäden sowie Wiederanlaufpläne (in Kooperation mit dem Notfallmanagement aus dem ISMS), zur möglichst schnellen Wiederherstellung eines geregelten, gesicherten und geschützten IT-Betriebs.

Während der Analyse erlangte Informationen sollten als gesicherte Erkenntnis schnellstmöglich hochschulübergreifend geteilt werden, damit festgestellt werden kann, ob die Systeme anderer Hochschulen von dem Angriff betroffen sind. Generell strukturiert und beschleunigt ein zentral koordinierter Ansatz die Vorfallsbearbeitung.

Darauf aufbauend kann insbesondere bei sehr ernsten Sicherheitsvorfällen (Major Incidents) ein Krisen-Squad-Team die betroffene Einrichtung intensiv – ggf. vor Ort - unterstützen, Kräfte bündeln und aktiv an der Analyse, Mitigation und Wiederherstellung der Systeme mitwirken.

Eine mit anderen Hochschulen abgestimmte Kommunikation, ebenfalls in die Behandlung involvierter CERTs oder beteiligter Strafermittlungsbehörden, des LSI, BSI und CAZ, BayLfD und betroffenen Anwender:innen ergänzen den Aufgabenbereich.

2.3.2 Technische Schwachstellenscans

Die in den Hochschulen betriebenen IT-Systeme werden immer zahlreicher und insbesondere komplexer. Sie sind vielfältigen Bedrohungen ausgesetzt und die Anzahl der Verwundbarkeiten und Schwachstellen nimmt im Hinblick auf deren Kritikalität laufend zu. Aus dem Internet direkt erreichbare Systeme und dort betriebene IT-Dienste werden fortlaufend angegriffen.

Jedoch bieten am Perimeter eingesetzte Firewall-Systeme in Hochschulnetzen nicht alleine die erhoffte Sicherheit. Analysen des Netzverkehrs zeigen, dass unmittelbar nachdem neue Schwachstellen bekannt werden, Angreifer beginnen automatisiert großflächig, d.h. nicht erkennbar zielgerichtet, ganze Netzbereiche zu scannen, in der Hoffnung dadurch über die neu entdeckte Schwachstelle verwundbare Systeme zu finden. Gelingt das tatsächlich, versuchen sie diese zeitnah auszunutzen und das betreffende IT-System zu kompromittieren.

Die Komplexität der an Hochschulen betriebenen IT-Infrastruktur sowie die stetig wachsende Anzahl und zunehmende Komplexität technischer Schwachstellen erfordert kontinuierliche Aufmerksamkeit und Informationsgewinnung sowie die Analyse der an Hochschulen eingesetzten Systeme. Um die Angriffsfläche von Hochschul-IT-Infrastrukturen zu minimieren sind regelmäßig durchgeführte, anlasslose sowie punktuell, schwachstellenbezogene Sicherheitsüberprüfungen der IT-Systeme notwendig. Die regelmäßige Durchführung von technischen Schwachstellenscans erfordert eine durchdachte und strukturierte Herangehensweise. HITS IS bietet die technische Infrastruktur und unterstützt Hochschulen bei der Beantwortung der hier genannten Fragen, welches Systeme, wann und mit welcher Art von Tests überprüft werden sollten.

Ergänzt werden solche regelmäßig durchgeführten Scans durch selektiv durchgeführte und auf eine konkrete Schwachstelle bezogene Scans seitens des HITS IS, um aktuelle Schwachstellen hochschulübergreifend zu identifizieren und ein bayernweites Lagebild im Hinblick auf die Verwundbarkeit einzelner Einrichtungen zu erstellen.

Mitentscheidend ist neben der Durchführung von Schwachstellenscans, die Kommunikation der Scanergebnisse und deren Bewertung im Hinblick auf die damit verbundene Kritikalität durch das HITS IS. Ein zielgruppenorientiertes und aussagekräftiges Reporting hilft einerseits Entscheidungsträgern bei der Einschätzung der gefundenen Schwachstellen und andererseits technischem Personal der betroffenen Hochschule durch die Bereitstellung konkreter Handlungsanweisungen beim Ergreifen wirksamer Abhilfemaßnahmen.

Wiederholte Scans unterstützen das Audit bei der Kontrolle der vollständigen Umsetzung der Maßnahmen und stellen die erfolgreiche Behebung vorhandener Sicherheitsprobleme sicher.

2.3.3 Handlungsanweisungen zur Bewertung und Reaktion auf Schwachstellen

Aktuelle Schwachstellen werden über verschiedene Kanäle ungefiltert an die Hochschulen verteilt. Diese Informationen sind notwendig, um die jeweilige Bedrohungslage lokal einschätzen zu können und müssen zeitnah und umfassend analysiert werden. Derlei Quellen gibt es viele, z.B. Mailinglisten des LSI und CAZ, Lageberichte des BSI, Meldungen des DFN-CERT oder anderer CERTs (z.B. EGI CSIRT, ...), Meldungen in den Medien oder abonnierten Mailinglisten. Auch die Hersteller von Betriebssystem- und diverser Applikationssoftware bieten Hochschulen über von ihnen abgeschlossenen, dedizierten Subscription Services im Rahmen von Wartung- und Supportverträgen solche Informationen an. Festzustellen ist, dass von den gemeldeten Schwachstellen oftmals viele oder alle Hochschulen zu einem gewissen Maß betroffen sind.

Die Informationsgewinnung und -verdichtung, die Analyse dieser Informationen, sowie die Ermittlung des individuellen Risikos und die anschließende Auswahl angemessener, notwendiger sowie minimalinvasiver Reaktionen ist ein ausgesprochen aufwändiger Prozess. Hierfür sind Kenntnisse der lokalen Gegebenheiten der Hochschule und fachliche Expertise notwendig. Erschwerend kommt hinzu, dass von den verschiedenen Meldern unterschiedliche Meldungen zur selben Schwachstelle bei den Hochschulen verteilt eingehen. Die einfache Weiterleitung unter Umständen einer größeren Anzahl von Schwachstellenmeldungen an alle Hochschulen ohne vorherige Bewertung des damit verbundenen Risikos und Ableitung konkret umzusetzender Gegenmaßnahmen ist wenig zielführend. Uneinheitliche Prozesse, der (Zeit-)Druck, unterschiedliche Einstufung der Risiken und fehlende Koordination zwischen den Hochschulen verlangsamen den Prozess massiv. Zudem werden die gleichen oder sehr ähnliche Arbeiten vielfach und zur selben Zeit an den verschiedenen Hochschulen unkoordiniert durchgeführt.

Das HITS IS SOC wird als bayernweite Zentrale für Kooperation, Kommunikation und Koordination beim Schwachstellenmanagement und als Schnittstelle für die verschiedenen Informationsquellen und -melder dienen. Eine dort zentral durchgeführte Analyse und Konsolidierung verschiedener Meldungen und darin enthaltener Informationen zu Schwachstellen durch das SOC, insbesondere wenn diese eine Vielzahl an Hochschulen gleichermaßen betreffen, die Bewertung des Risikos und die kooperative Ableitung konkreter Handlungsanweisungen zur Beseitigung der Schwachstellen, erleichtern den Informationssicherheitsverantwortlichen und dem technischen Personal vor Ort die Arbeit deutlich. Das HITS IS ist in der Lage Synergien zu schöpfen und ermöglicht ein zeitnahes, abgestimmtes und effektives, bayernweit einheitliches Vorgehen. Durch die Abstimmung untereinander (vor allem mit den Ergebnissen der Schwachstellenscans) lässt sich sehr schnell sehen, wie der aktuell Behebungsstand ist und an welchen Stellen gegebenenfalls noch weiterer Unterstützungsbedarf besteht.

2.3.4 Managed Security Service und Security-Analyse

Neu einzuführende Systeme und Applikationen an Hochschulen bergen mitunter Sicherheits- und Datenschutzrisiken, die vor der Einführung erkannt werden müssen und mit wirksamen Maßnahmen zu begegnen sind. Um erfolgreiche Angriffe und daraus resultierende Sicherheitsvorfälle auf die eigene IT- Infrastruktur erkennen zu können, ist ein Monitoring und die Analyse des Kommunikationsverhaltens der in der Hochschul-IT-Infrastruktur betriebenen IT-Systeme essentiell.

Diese Analyse ist ein ressourcenintensiver Prozess, der umfassende Kenntnisse der als normal anzusehenden Kommunikationsbeziehungen, effiziente Mechanismen zur Auswertung und das

Vorhandensein aktueller Threat-Intelligence-Informationen voraussetzt. Die ausschließlich hochschullokale Analyse generiert diesen Aufwand vor Ort und schöpft keine Synergien und wird das erforderliche Know-How nicht in der notwendigen Breite sicherstellen können.

Managed Security-Service und -Analyse als vom HITS IS bereitgestellter Dienst bietet einerseits die Möglichkeit der automatisierten Auswertung und Korrelation von Ereignissen und Log-Daten aus den Hochschulen. Die dabei gewonnenen Daten können hochschulübergreifend korreliert und mit Threat Intelligence Informationen (Indicators of Compromise, IoCs) verknüpft werden. Durch die Anreicherung mit Zusatzinformation ist eine (Früh-)Warnung vor drohenden Angriffen sowie die Erstellung hochschulweiter und -übergreifender Sicherheitslagebilder für Bayern das Ziel. Weiterhin unterstützt der Managed Security Service Hochschulen bei der prototypischen Evaluation neuer Sicherheitsleistungen, Systeme und Applikationen sachverständig und bei der Ausschreibung von Rahmenvertragsausschreibungen.

2.4 Aufgabenbereiche HITS IS ISMS

2.4.1 Erstellung, Umsetzung und Fortschreibung einer systematischen bayernweiten Kommunikation zur Informationssicherheit

Die bayernweite Vernetzung zur Informationssicherheit, sowie die zentrale Sammlung und bayernweite Verteilung von Informationen sind wesentlicher Bestandteil einer umfassenden Kommunikationsstrategie. Erkenntnisse über Schwachstellen an einzelnen Einrichtungen müssen dem Informationsgewinn und Prävention anderer dienen. Technische Erkenntnisse sind nicht nur durch Scans zu erwarten, vielmehr können allgemein auftretende Bedrohungen (z.B. Ransomware) oder öffentlich bekanntgemachte Schwachstellen (z.B. Printer Nightmare) zu einem allgemein hohen Verwundbarkeitsgrad der bayerischen Hochschulen insgesamt führen.

Das HITS IS erarbeitet koordiniert Erkenntnisse über Schwachstellen und stellt allen in einem Portal diese Informationen zur Verfügung. Die aktuelle Struktur an lokalen Ansprechpartnern (CISO, ISB, …) soll weiter aktiv vernetzt und mit Informationen versorgt werden

Ein Erfolgsfaktor hierfür ist ein Hand-in-Hand-Zusammenwirken zwischen den lokalen Ansprechpartnern und dem HITS IS sowie HITS IS intern. Erkennen, Analyse, Kommunikation und Information werden auf einer Plattform zur Verfügung gestellt. Das Wissensmanagement ist gut strukturiert, allen zugänglich, kann selbstständig abonniert und durch Beiträge ergänzt werden. Die Kommunikationsplattform soll dazu beitragen informationssicherheitsrelevante Inhalte zu diskutieren und an wichtigen (Zukunfts-) Themen gemeinsam zu arbeiten. Spezialwissen der einzelnen Hochschulen wird präsentiert und kann von anderen abgerufen werden. Ein Beispiel hierzu wäre eine „gemanagte Firewall“, die gemeinsam definiert wird und dann als Vorzugsvariante zentral beschafft und administriert werden könnte.

Eine zu definierende Kommunikationsstrategie legt fest, welche Inhalte über welche Kanäle an welche Zielgruppen wie kommuniziert werden und in welchen zeitlichen Intervallen dies geschieht. Wichtige Ergebnisse und Neuerungen werden über das HITS Kommunikations- und Reaktionsteam über einen zyklischen Newsletter einem breiteren Publikum bayernweit kommuniziert.

Die Zusammenarbeit mit Einrichtungen des Freistaats, z.B. LSI, CAZ, Bayern-CERT, zur Unterstützung der Informationssicherheit wird in 2022 strukturiert und in 2023 ein einheitlicher Eskalationsrahmen für Störfälle und in der Krisenbewältigung geschaffen.

Mit dem oben Beschriebenen führt HITS IS ISMS die Kommunikationsaufgaben der aktuellen Stabsstelle Informationssicherheit zielgerichtet fort und entwickelt dies weiter. Bisherige Erkenntnisse fließen direkt in die neue Struktur ein.

2.4.2 Umsetzung, Überprüfung und Weiterentwicklung des Hochschulinformationssicherheitsprogramms (HISP)

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

unabhängig vom jeweiligen Standard (BSI, ISO 27k, CISIS12) alle Phasen, die bei der Etablierung eines ISMS zu durchlaufen sind.

Durch ein erfolgreiches HISP wird ein einheitliches ISMS an allen bayerischen Hochschulen und Universitäten eingeführt, aufrechterhalten, gepflegt und in kontinuierlichen Abständen überprüft und verbessert. Das HISP ist hierbei als Benchmark zu verstehen, der einen regelmäßigen Soll-IST Vergleich aufzeigt und somit den jeweiligen Reifegrad der Informationssicherheit darstellt.

Folgt eine 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 wird vermieden, das dies zwar zur kurzfristigen Verbesserung in Teilen beiträgt, aber keinen durchgängigen Prozess zur Gewährleistung der Informationssicherheit erzeugt.

Bisher wird eine beratende Unterstützung bei der Einführung und aktive Unterstützung in Form von Musterdokumenten und -prozessen über die zentrale Stabsstelle Informationssicherheit gewährleistet. Allerdings wird die Unterstützung als Hilfestellung gesehen und entbehrt nicht der lokalen Erstellung von Informationssicherheitskonzepten und Vor-Ort-Organisation der Informationssicherheit und die Integration des HISP in die Hochschulorganisation. Die Begleitung bei der Umsetzung der Teilschritte des HISP bedarf konsequenter Beratungsunterstützung durch das HITS IS. Durch die Langfristigkeit des Programms ist es unentbehrlich die Effektivität der einzelnen Schritte regelmäßig zu überprüfen, zu verbessern und die Schritte zu detaillieren.

Durch die zentrale Unterstützung werden einheitliche Prozesse zur Gewährleistung der Informationssicherheit z. B. Security Incident, IT-Notfallmanagement, Business Continuity Prozess, Risikomanagement etabliert. Daneben werden einheitliche zentrale informationssicherheits-relevante Konzepte z.B. IT-Sicherheitskonzept, erstellt und implementiert, um die Vertraulichkeit, Integrität und die Verfügbarkeit sensibler Daten zu gewährleisten.

Das HITS IS etabliert eine zentrale Koordinationsstelle für hochschulinterne Auditoren, um das ISMS jeder Hochschule und Universität gegenseitig in regelmäßigen Abständen auf Wirksamkeit zu überprüfen und zu verbessern. Dadurch wird der Reifegrad jeder einzelnen Hochschule und Universität ermittelt, weiterentwickelt und erhöht.

Zukünftige Audits werden dabei mit dem Reifegradmodell nach ISO/IEC 21827 bewertet und in den CIO Runden zur Verfügung gestellt.

Mit einer zentralen Koordinationsstelle für HISP ist es möglich mit internen und externen Arbeitskreisen zu kommunizieren und zu agieren. Dadurch werden unterschiedliche Anforderung aus den Hochschulen und Universitäten zusammengeführt und eine gemeinsame Lösung erarbeitet. Durch das HISP kann eine Informationssicherheitsgovernance in Verbindung mit der IT-Strategie zur effektiven Steuerung von Ressourcen etabliert werden (siehe ISO27014). Regelmäßiges Reporting mit vorher definierten Kennzahlen zur Messung des Umsetzungsgrades von HISP für die spezifische Hochschulumgebung soll bis Ende 2022 etabliert werden.

2.4.3 Informationssicherheitsmanagementsystem (ISMS)-Consulting

Die Einführung eines ISMS ist für eine Hochschule eine strategische Entscheidung und die Erstellung und Umsetzung richten sich nach den Bedürfnissen und Zielen, den Informationssicher-heitsanforderungen, den organisatorischen Abläufen sowie nach Größe und Struktur der einzelnen Hochschule.

Die Einführung eines ISMS erfordert lokalisiertes Personal an der jeweiligen Hochschule. Dieses Personal hat beim Aufbau eines ISMS einen hochschulspezifischen und unabhängig von den gegebenen Voraussetzungen einen allgemeinen Beratungsbedarf. Das Wissen um die hochschul-spezifische Anwendung der gewählten Standards bietet eine solide Grundlage, um effektive und effiziente Sicherheitsmaßnahmen einzuführen.

Dieses Wissen stellt das HITS IS zentral über technische und strategische Berater zur Verfügung. Dadurch wird gewährleistet, dass die bisherige Arbeit der Stabsstelle Informationssicherheit konsequent weitergeführt und die Hochschulen mit der generischen Entwicklung bzw. Pflege von Musterdokumenten und Sicherheitskonzepten weiterhin unterstützt und im Aufbau und Integration von ISMS Prozessen in den lokalen Hochschulalltag begleitet werden. Die enge Zusammenarbeit

mit den ISB der Hochschulen intern und externen Arbeitsgruppen (wie BHN, AG ITSI, LSI) zur Förderung des Umsetzungsprogramms HISP und die Weiterentwicklung desselben prägen das Aufgabengebiet im Consulting.

Um den Integrationsaufwand an den Hochschulen hin zu einem kontinuierlichen Verbesserungsprozess zu vereinfachen, wurde 2021 mit dem ‚HITS Beschaffung' die Ausschreibung einer zentralen Software zur lokalen Steuerung des ISMS, des Datenschutzes und des Notfallmanagements gestartet. Teilnehmende Einrichtungen werden vom HITS IS mit Mustervorlagen und Integrationsanweisungen unterstützt. Um vor Ort den Aufwand gering zu halten bietet das HITS IS eine zentrale Instanz der Software an und pflegt bedarfsorientiert die Vorlagen zu Organisation, Technik, Risiken und aktuellen Bedrohungen. Die Übernahmen dieser so zur Verfügung gestellten Aktualisierungen erfolgt lokal durch Ansprechpartner an den jeweiligen Hochschulen. Es ist davon auszugehen, dass bis 2022 die ersten Hochschulen mit diesem Tool unterstützt werden können, eine Datenbasis (IT-Assets) für den Aufbau eines Notfallmanagements und Vorlagen für die Anwendung gängiger Standards im Tool integriert sind. In der Folge werden weitere Muster für Forschungseinrichtungen (z.B. TISAX), unterschiedlicher Campusmanagementsysteme (HISinOne, PRIMUSS) bzw. bedarfsorientiert entwickelt. Bis Ende 2023 soll jede teilnehmende Hochschule die Möglichkeit zur Anwendung einzelner Module bekommen.

Da sich Einflussgrößen der lokalen ISMS' im Laufe der Zeit ändern, wird es langfristig notwendig sein, fehlende oder ineffektive Prozesse zu identifizieren (Audits) und gemeinsam mit der betroffenen Hochschule das lokale ISMS bzw. die Standards für Bayern kontinuierlich zu verbessern.

2.4.4 Koordination, Steuerung, Durchführung und Unterstützung von Schulungen und Awareness-Maßnahmen

Der „Faktor Mensch" – das Wirken aller beteiligten Personen - hat eine wichtige Stellung in der Informationssicherheit. Bei Angriffen spielt er oft die zentrale Rolle und entscheidet, ob ein Angriff erfolgreich abgewehrt werden kann.

Hochschulangehörige sind somit eine wertvolle Ressource zum Schutz sensibler Informationen und der IT-Infrastruktur. Sie sind bei vielen Maßnahmen zur Informationssicherheit aktiv involviert, z. B. Wahl eines sicheren Passworts, Wegschließen von Unterlagen, Klassifizieren von Informationen, Sperren des Bildschirms, Informationsweitergabe am Telefon, Beobachten verdächtiger Situationen. Information Security Awareness heißt, dass Hochschulangehörige sensibel auf mögliche Angriffe reagieren, diese erkennen, wissen, wie sie sich verantwortungsbewusst und informationssicher verhalten und dies dann auch tun.

Für die Informationssicherheit an Hochschulen ist also die Einbeziehung aller Hochschulangehörigen von zentraler Bedeutung. Hochschulen haben zwar verstanden, dass die Sensibilisierung der Hochschulangehörigen wichtig ist, verfügen jedoch über wenig Erfahrung, welche Maßnahmen wie am besten eingesetzt werden um die Information Security Awareness (ISA) zu erhöhen.

Die Auswahl von geeigneten Awareness-Maßnahmen aus einem zentral bereitgestellten Fundus kann hochschulübergreifend und trotzdem hochschulspezifisch effizient und effektiv zentral erbracht werden. Zentral verfügbare für die Hochschulen spezifisch zusammengestellte Awarenessmaßnahmen sind geeignet, die Awareness und damit das informationssicherheitskonforme Verhalten zu erhöhen.

Bestehende Instrumente (z.B. Lern-Management-System), vorhandenes Spezialwissen (z.B. der Hochschule Würzburg u.a.) und vorhandene Fähigkeiten (z.B. professionelle Medienlabore der Uni und Hochschule Augsburg; didaktische, pädagogische und psychologische Lehrstühle) werden integriert. Um passende Maßnahmen anbieten zu können, müssen der Status Quo der Information Security Awareness an den Hochschulen ermittelt werden und spezielle auf die organisatorischen und technischen Rahmenbedingungen sowie heterogenen Gruppen von Hochschulangehörigen zugeschnittene Sensibilisierungsmaßnahmen ausgewählt oder erstellt werden. Das HITS IS wird dafür in der Folge Methoden und Kennzahlen für das Messen des Erfolgs von Awareness-Maßnahmen bereitstellen und die Einbettung von Sensibilisierung und Kommunikation in das Informationssicherheitskonzept der Hochschulen methodisch unterstützen. Zudem fließen die

Erkenntnisse und Prognosen aus dem SOC und Consulting in die Weiterentwicklung bzw. der Erstellung der Inhalte mit ein.

2.5 Zeitlicher Horizont für die Verfügbarkeit von Diensten des HITS IS

Bereits während der Rekrutierungs- bzw. Ausbildungsphase in Q1 und Q2/2022 kann mit den Abstimmungen und Bestandsaufnahmen begonnen werden. Der Vorteil vor allem für internes Personal liegt im Wissenszuwachs der detaillierten Bedürfnisse bayerischer Hochschulen in den jeweiligen Aufgabengebieten. Im ISMS Bereich können bestehende Konzepte der Stabsstelle weitergeführt und durch den verstärken Personaleinsatz zeitgleich abgearbeitet werden. Auch die Aufgaben im SOC Bereich können auf Vorarbeiten beispielsweise im Münchner Wissenschaftsnetz aufbauen, die in weiten Teilen geeignet sind, auch bayernweit zu wirken. Die 2. Hälfte des Jahres 2022 ist geprägt von der Ausgestaltung der jeweiligen Dienste. Diese erfolgt in enger Zusammenarbeit mit dem leitenden Gremium und den Ansprechpartner an den bayerischen Hochschulen. Ein Teil der Anforderungen wird sich aus den laufenden Audits an den Hochschulen ergeben, die ab 2022 im 3 Jahres Rhythmus für jeweils 9 Hochschulen durchgeführt wird.

Die folgende Darstellung zeigt einen Überblick über die ersten Aufgaben zum Aufbau und Umsetzung eines geregelten Betriebs am HITS IS:

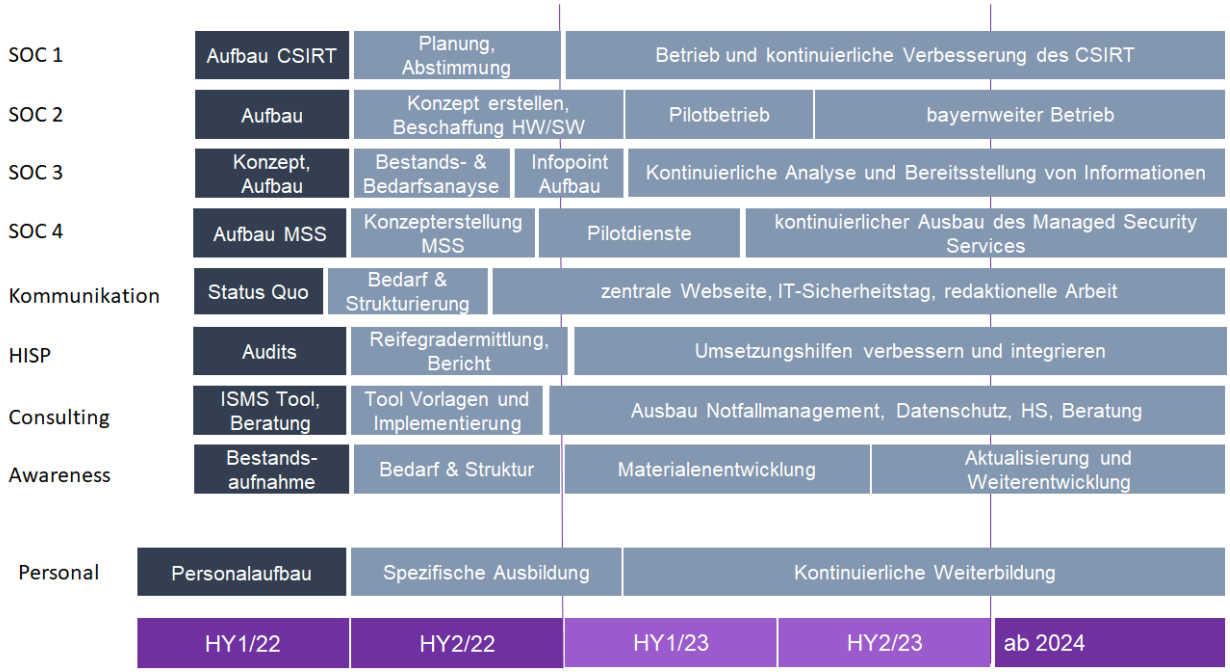

Abbildung 3: Aufgaben und Meilensteine für den Aufbau und die Dienste des HITS IS

3 Governance

Die Steuerung des HITS IS erfolgt gemäß der zukünftigen Governancestruktur der IT-Strategie der bayerischen Hochschulen und ist gesetzt. Der leitende Ausschuss des Digitalverbunds (LADV) bestimmt die Mitglieder eines Steuerungsgremiums zur Priorisierung der Aufgaben und Organisation des HITS IS. Das HITS IS selbst berichtet an den LADV und steht mit den ISB oder CISO der Hochschulen in Kontakt, um die Gesamtsituation der bayerischen Hochschulen zu erfassen. Beauftragung, Steuerung und Entlastung des HITS IS erfolgt durch das Leitungsgremium. Die fachlichen Leitlinien und die strategische Priorisierung der Aufgaben werden durch das Leitungsgremium festgelegt und fortgeschrieben.

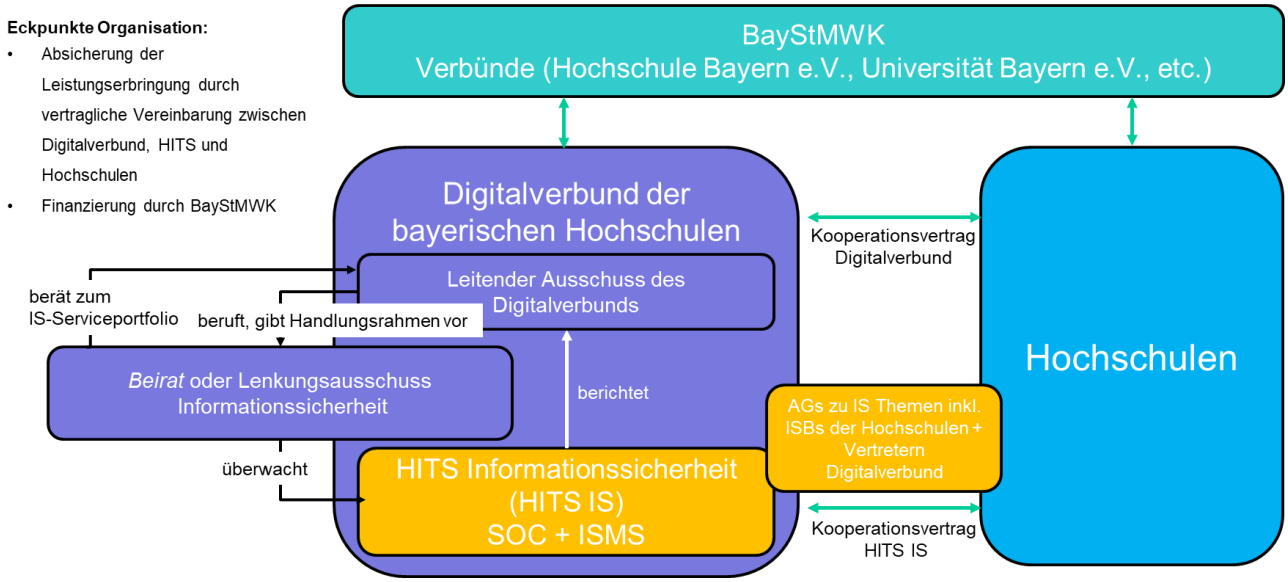

Abbildung 4: Eingliederung des HITS IS in den Digitalverbund

4 Personalkonzept, Sachkosten und Investitionen

4.1 Personalkonzept

LRZ, HSA und UniA werden die Stellen entsprechend des dargestellten Anforderungsprofils nachhaltig besetzen. Hierbei wird auf einen guten Mix der Fähigkeiten geachtet und ein mehrstufiger Entwicklungsplan realisiert. Im ersten Jahr werden von den Beschäftigten des HITS IS Basisdienste aufgebaut und deren Betrieb gestartet. Diese werden in den Folgejahren bedarfsorientiert weiter ausgebaut, verändert oder ggfs. eingestellt. Dies erfolgt mit einem gemanagten Lifecycle. Die nötigen Mitarbeiter können teilweise aus den an HSA, UniA, LMU oder TUM angebotenen Studiengängen und Forschungsabteilungen (HSA Innos) oder Abteilungen (LRZ) gewonnen werden.

Das Personalkonzept wird von allen drei Institutionen (HSA, LRZ und UniA) in enger Abstimmung mit dem Betriebskonzept organisiert. Ziel ist dabei ein Vertretungskonzept, welches (institutionsübergreifend) sicherstellt, dass im Falle von z. B. Krankheit, Urlaub, Lastspitzen und dem Weggang von Ressourcen, soweit kontinuierlich umsetzbar, kompetente Ansprechpartner verfügbar sind. Alle Mitarbeiter werden kontinuierlich gefördert, um sich im Bereich Informationssicherheit weiterzubilden.

Im aktuellen Konzept sind insgesamt 8 Personalstellen vorgesehen, jeweils 4 für die Themenbereiche ISMS und SOC. Die Antragsteller sind sich einig, dass ein effektives und effizientes HITS mit diesen limitierten zentralen Ressourcen nur dann schlagkräftig alle Hochschulen in Bayern unterstützen kann, wenn es auf die tatkräftige Unterstützung von lokalen Spezialisten in den jeweiligen Hochschulen sowohl im kontinuierlichen Auf-/Ausbau von ISMS Maßnahmen, der Umsetzung von Empfehlungen auf Basis von SOC Analysen und der Behandlung von Vorfällen bauen kann.

Je nach Nachfrage, zukünftigen weiteren Anforderungen an das Service-Portfolio des HITS IS und der Intensität der Unterstützung durch lokale Experten an den Hochschulen kann sich Bedarf an einer Verstärkung der Personalressourcen ergeben. Dieser sollte regelmäßig gemeinsam mit dem leitenden Ausschuss des Digitalverbunds (LADV) geprüft werden.

Um die beschriebene Vertretungsregelung nachhaltig umzusetzen, wird das HITS Informationssicherheit für Anfragen von Seiten der Hochschulen mit einem Ticketsystem arbeiten. Damit soll verhindert werden, dass aufgrund von Urlaubssituationen, Krankheiten etc. Ansprechpartner nicht erreichbar und damit womöglich zeitkritische Anfragen nicht rechtzeitig adressiert werden können. HITS-intern werden unabhängig davon Schwerpunktthemen und Projekte von dafür vorgesehenen Mitarbeitern fachspezifisch getrieben und begleitet werden. Ziel ist dabei eine möglichst gleichmäßige Auslastung der Ressourcen und schnelle Reaktion und Bearbeitung von Anfragen.

Die Aufteilung der insgesamt 8 Personalstellen erfolgt paritätisch zwischen den Aufgabenschwerpunkten und den beteiligten Institutionen.

Die Leitung des HITS Informationssicherheit soll durch den bereits erfahrenen und bewährten Kollegen Christian Fötinger (Stabsstelle Informationssicherheit) besetzt werden. Die stellvertretende Leitung wird in der Aufbauphase der erfahrene Experte für Informationssicherheit Stefan Metzger von Seiten des LRZ übernehmen. Mittelfristig ist geplant, dass diese Position von einem der beiden neu eingestellten LRZ Mitarbeiter Niveau übernommen wird.

Um eine enge Zusammenarbeit der HITS Mitarbeiter zu fördern ist beabsichtigt, sowohl im LRZ in München als auch am Standort Augsburg gemeinsam genutzte Büroflächen für die lokalen Viererteams einzurichten. Durch die geringe Distanz zwischen Augsburg und München sind regelmäßige gemeinsame Teammeetings aller HITS-Mitarbeiter möglich und geplant.

Die standortspezifischen Schwerpunkte des HITS IS sind nachfolgend dargestellt:

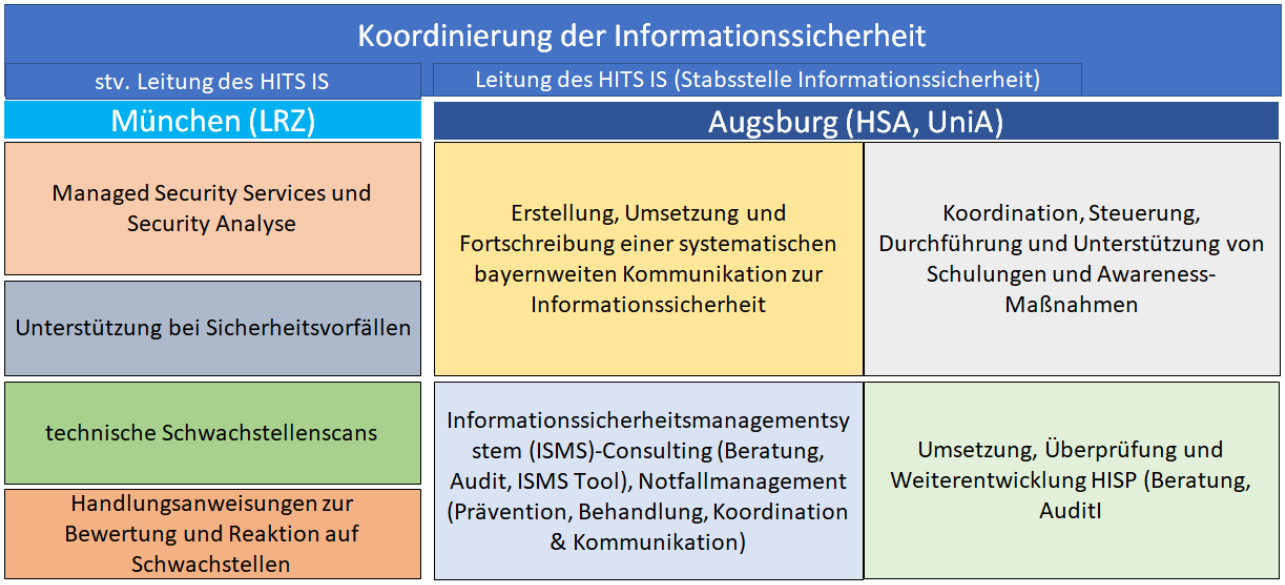

Abbildung 5: standortspezifische Schwerpunkte des HITS IS

4.1.1 Erwartete und zu erlangende Kenntnisse und Erfahrungen

Hierbei wurde darauf geachtet, dass die vorhandenen Fähigkeiten und Dienste von LRZ, HSA und UniA gut eingesetzt werden können. Die HSA beherbergt die aktuelle Stabsstelle Informationssicherheit. Hierbei sind in den vergangenen Jahren HISP als Standardvorgehensmodell entstanden, dass sukzessive weiterentwickelt und umgesetzt werden soll. Die aktuelle Vernetzung der Stabsstelle soll künftig fortgesetzt und verstärkt werden. Zudem besitzt die HSA mit dem Institut für innovative Sicherheit (HSA_innos) für Bereiche des ISMS Consulting sowie ISO27001 zertifizierte Ressourcen zur Gestaltung eines adäquaten gegenseitigen Auditierungsprogramms.

Die Universität Augsburg ergänzt dies mit ISO27001 zertifizierten Mitarbeitern, einem mittelgroßen Rechenzentrum mit ausgeprägter Netzwerkanbindung, zahlreichen Instituten, z.T. als abgesetzte Außenstandorte, und neben Sicherheitsfachwissen mit profunden pädagogischen und didaktischen

Fähigkeiten bei der Erstellung von Security-Awareness-Materialien. Fragestellungen aus dem Kontext des Neuaufbaus einer Universitätsmedizin sowie eines Rechenzentrumsneubaus können in die Arbeit des HITS IS einbezogen und schließlich verallgemeinerten Empfehlungen zugeführt werden.

Das breite Feld „ISMS Consulting“, remote und vor Ort wird gemeinsam verantwortet.

Das LRZ bringt sich als IT-Dienstleister und Betreiber des Münchner Wissenschaftsnetzes mit Fachexpertise in verschiedensten technischen Bereichen ein, zu denen das Security-Monitoring oder der Aufbau eines Schwachstellenmanagement- oder Penetrationtesting-Service zählen. Die Dienstbereitstellung erfolgt im Rahmen eines nach ISO/IEC 27001 und ISO/IEC 20000-1 zertifizierten Managementsystems. Entsprechend verfügen alle Beschäftigten über Grundkenntnisse in beiden Normen, während die am Aufbau des Managementsystems beteiligten Personen darüber hinaus über sehr weitreichende Fachkenntnisse hier bis zum Auditorenlevel zu bieten haben.