Veröffentlicht in den Amtlichen Bekanntmachungen der Universität Ulm Nr. 22 vom 05.10.2020, Seite 146 - 149

Leitlinie zur Informationssicherheit der Universität Ulm

vom 29.09.2020

Das Präsidium hat in seiner Sitzung am 16.09.2020 aufgrund von § 16 Abs. 3 Satz 1 LHG nachfolgende Leitlinie beschlossen.

Präambel

Die Digitalisierung durchdringt zunehmend alle Lebensbereiche von Wirtschaft und Gesellschaft. Als Teil der Gesellschaft unterstützt und nutzt die Universität Ulm diese Entwicklung, muss aber auch dafür Sorge tragen, dass die damit einhergehenden Gefahren und Risiken beherrscht werden. Die Funktionsfähigkeit der Universität Ulm bei der Wahrnehmung ihrer Aufgaben in Forschung, Lehre, Studium und Weiterbildung hängt mittlerweile ganz wesentlich von der Verfügbarkeit und Integrität ihrer IT-Infrastruktur ab. Gleichzeitig sind die IT-Systeme immer größeren Bedrohungen durch eine Vielzahl von Angriffsvektoren, aber auch durch technische und organisatorische Schwachstellen ausgesetzt.

Um allen Mitgliedern der Universität eine angemessen sichere und verlässliche Arbeitsumgebung zur Verfügung stellen zu können, sind das Ergreifen geeigneter Schutzmaßnahmen für sensible Daten sowie ein die ganze Universität einschließendes Informationssicherheitsmanagement von höchster Priorität.

In Wahrnehmung seiner Verantwortung für die Informationssicherheit legt das Präsidium auf Grundlage der VwV Informationssicherheit vom 07.04.2017 in dieser Leitlinie die Ziele, Grundsätze und Organisation für den Informationssicherheitsprozess an der Universität Ulm fest. Die Leitlinie ist Grundlage für das Informationssicherheitskonzept der Universität und die Ableitung konkreter Sicherheitsrichtlinien.

§ 1 Geltungsbereich

Die Leitlinie für Informationssicherheit gilt für alle Einrichtungen der Universität Ulm inklusive der vorklinischen Einrichtungen, für alle ihre IT-Systeme und alle Tätigkeiten, bei denen schutzbedürftige Informationen verarbeitet werden, sowie für die Gesamtheit der Nutzerinnen und Nutzer dieser Systeme.

§ 2 Sicherheitsniveau

(1) Ziel ist es, unter Einhaltung der einschlägigen rechtlichen Vorgaben ein angemessen hohes Schutzniveau für sämtliche IT-Systeme der Universität Ulm sicherzustellen.

(2) Die Schutzziele sind:

a) Vertraulichkeit: Nur Befugte haben Kenntnis oder Zugriff auf Informationen[1]. Die sachgemäße Handhabung vertraulicher Informationen ist, unabhängig von der Art ihrer Aufzeichnung, sicherzustellen.

b) Integrität: Unbefugte oder unbemerkte Veränderungen von Informationen, sei es durch Personen oder technische Fehler, müssen ausgeschlossen sein. Informationen dürfen weder irrtümlich noch mutwillig manipuliert werden.

[1] Informationen können Daten (z. B. Dokumente), Infrastruktur (z. B. Server) und Übertragungswege (z. B. E-Mail-Kommunikation) sein.

c) Verfügbarkeit: Die Informationen müssen zu jeder Zeit einer autorisierten Person zugänglich und für diese verfügbar sein. Daraus folgt, dass die Funktionsfähigkeit der IT-Infrastruktur zum einen vor regulären Ausfällen und zum anderen vor gezielten Angriffen zu schützen ist.

(3) Die Universität Ulm strebt ein angemessen hohes und auf den jeweiligen Schutzbedarf abgestimmtes Informationssicherheitsniveau an, das sich an den jeweils geltenden BSI-Standards orientiert. Dieses Ziel wird schrittweise durch eine Kernabsicherung[2] aller betriebskritischen zentralen Systeme, mit denen die essenziell wichtigen Geschäftsprozesse und Ressourcen abgedeckt werden, und eine Basisabsicherung weiterer Systeme erreicht.

(4) Um die genannten Schutzziele zu erreichen, müssen geeignete technische, organisatorische und personelle Maßnahmen in den Anwendungen, dem IT-Netz, den (ggf. mobilen) Endgeräten und auf den Übertragungswegen ergriffen werden.

§ 3 Träger von Pflichten

Alle Einrichtungen der Universität Ulm sind verpflichtet sicherzustellen, dass bei ihnen die Grundsätze der Informationssicherheit und weiterer Sicherheitsziele eingehalten werden. Dazu gehören,

a) die Gewährleistung der Verfügbarkeit und Funktionsfähigkeit aller die Geschäftsprozesse der Universität unterstützenden IT-Systeme, Anwendungen und Daten sowie die Verhinderung einer missbräuchlichen Verwendung,

b) die Einhaltung von gesetzlichen Vorgaben und sonstigen relevanten rechtlichen Bestimmungen,

c) die Umsetzung der hochschulintern geltenden Sicherheitsrichtlinien und weiterer Maßnahmen zur Gewährleistung der Informationssicherheit,

d) die Wahrung der Persönlichkeitsrechte der Mitglieder und Angehörigen der Universität, sowie anderer Nutzerinnen und Nutzer.

§ 4 Informationssicherheitsprozess

(1) Um das in § 2 beschriebene Sicherheitsniveau zu erreichen, wird ein ganzheitlicher und die gesamte Universität umfassender Informationssicherheitsprozess eingeleitet. Das mit diesem Prozess etablierte Informationssicherheits-Managementsystem (ISMS) folgt einem PDCA-Zyklus, um die Wirksamkeit der ergriffenen Maßnahmen und organisatorischen Strukturen kontinuierlich zu überprüfen und an neue Bedrohungsszenarien sowie technische Gegebenheiten anzupassen:

   a) Plan – Planung von Sicherheitsmaßnahmen,

   b) Do – Umsetzung der Maßnahmen,

   c) Check – Erfolgskontrolle, Überwachung der Zielerreichung,

   d) Act – Beseitigung von Defiziten, Verbesserung.

(2) Ein ergänzend erstelltes Informationssicherheitskonzept dient der Umsetzung der Informationssicherheitsleitlinie und beschreibt die geplante technische und organisatorische Vorgehensweise, um die angestrebten IT-Sicherheitsziele an der Universität Ulm zu erreichen.

(3) Aus dem Informationssicherheitskonzept werden Informationssicherheitsrichtlinien entwickelt. Sie werden anhand der im Informationssicherheitskonzept definierten Sicherheitsstandards formuliert und realisiert und sind somit operative Elemente des Informationssicherheitskonzepts.

§ 5 Organisationsstruktur

(1) Die erfolgreiche Umsetzung des Informationssicherheitsprozesses setzt klar geregelte Verantwortlichkeiten und die daraus resultierende Erfüllung von Aufgaben voraus. Dabei sind folgende Personen und Stellen beteiligt:

   a) Präsidium

[2] Der BSI IT-Grundschutz unterscheidet drei Schutzniveaus: Basis-, Standard- und Kernabsicherung (Fassung 200-1 bis 200-3).

Das Präsidium trägt die Gesamtverantwortung für die IT-Strategie sowie die Informationssicherheit an der Universität Ulm.

b) Chief Information Security Officer (CISO)

Die oder der CISO wird vom Präsidium der Universität Ulm bestellt und ist der obersten Leitungsebene als unabhängige Stabsstelle zugeordnet.[3] Sie/er unterliegt insoweit keinen fachlichen Weisungen und ist in der Ausübung ihres/seines Amtes frei. Sie/er kann sich im Rahmen ihrer/seiner Aufgaben unmittelbar an die Hochschulleitung wenden[4]; ihr oder ihm können zur Unterstützung weitere Mitarbeiterinnen und Mitarbeiter zugeordnet werden.

Die oder der CISO ist Hauptansprechperson für sämtliche Themen rund um die Informationssicherheit und unterstützt die Hochschulleitung bei der Umsetzung der festgesetzten Maßnahmen. Sie oder er fördert und koordiniert alle erforderlichen Belange der Informationssicherheit für die Universität. Sie oder er koordiniert federführend die Erstellung des Informationssicherheitskonzepts und dessen Fortschreibung; das gleiche gilt für Teilkonzepte und Richtlinien. Im Fall einer akuten Bedrohungslage oder eines konkreten Sicherheitsvorfalls ist die oder der CISO berechtigt, zur Gefahrenabwehr oder Schadensbegrenzung erforderliche und geeignete Maßnahmen bis hin zur sofortigen vorübergehenden Stilllegung des entsprechenden IT-Systems anzuordnen.

c) Chief Information Officer (CIO)

Die oder der CIO wird vom Präsidium der Universität Ulm bestellt. Ihre/seine Aufgabe entspricht den Aufgaben aus Ziffer 5 der VwV IT-Organisation[5] und umfasst insbesondere die strategische Weiterentwicklung und die operative Ausgestaltung der universitären Informationstechnologie. Sie oder er berücksichtigt dabei die Grundsätze der Informationssicherheit und ergreift entsprechende Sicherheitsmaßnahmen. In dieser Funktion arbeitet sie oder er eng mit dem CISO zusammen.

d) Information Security Officers (ISO)

Je nach Bedarf und Größe der Organisationseinheiten werden zusätzlich fachkundige Informationssicherheitsbeauftragte (ISO) auf Ebene zentraler Einrichtungen, Fakultäten oder Departments bestellt. Die ISOs arbeiten mit der oder dem CISO zusammen. Sie unterstützen die jeweilige Leitung der Organisationseinrichtung bei der Umsetzung des Sicherheitskonzepts und der Einhaltung von Sicherheitsrichtlinien und berichten der oder dem CISO dazu auf Anfrage.

e) Information Security Management Team (ISMT)

Dem ISMT gehören an

- der oder die CISO,
- ihre oder seine Stellvertretung,
- die ISOs der Organisationseinheiten,
- Ansprechpersonen ausgewählter Fachverfahren und sonstigen IT-Verantwortliche.

Bei der Zusammensetzung des ISMT sollen alle für die Informationssicherheit der Geschäftsprozesse der Universität relevanten Fachbereiche berücksichtigt werden. Es tritt auf Einladung des CISO in der Regel mindestens einmal im Semester zusammen.

Das ISMT hat die Aufgabe, die oder den CISO bei der Erstellung des Informationssicherheitskonzepts und der Umsetzung des Informationssicherheitsprozesses zu beraten und zu unterstützen.

f) Kommunikations- und Informationszentrum (kiz)

Das kiz ist an der Universität Ulm der Betreiber aller zentralen IT-Dienstleistungen. Es ist bei den von ihm betriebenen Systemen für die Sicherstellung eines angemessenen IT-Schutzes verantwortlich. Dazu führt es das in Zusammenarbeit mit dem CISO und dem ISMT entwickelte Informationssicherheitskonzept als wesentlichen Teil seines Servicemanagements ein und setzt dieses um. Darüber hinaus erarbeitet das kiz zusammen mit dem CISO Leitfäden und Dokumentationen für die Nutzung seiner Dienste.

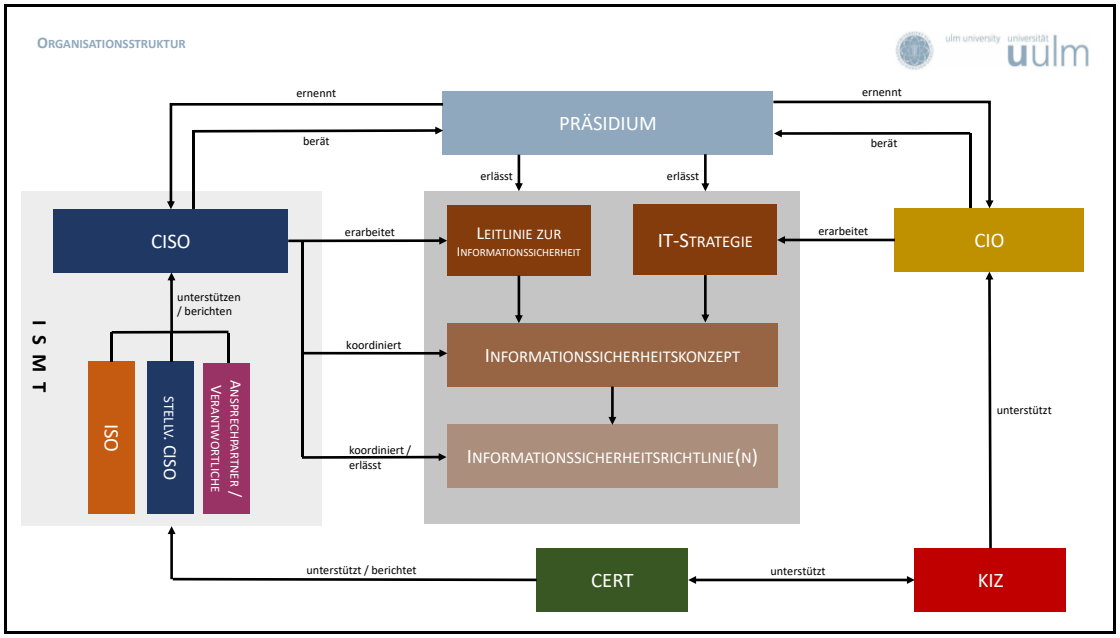
[3] Gemäß Empfehlung des BSI-Standards 200-2
[4] VwV Informationssicherheit vom 07.04.2017, Ziffer 5.2.3.
[5] VwV IT-Organisation vom 07.06.2016

g) Computer Emergency Response Team (CERT)

Das CERT ist die zentrale Anlaufstelle bei Informationssicherheitsvorfällen an der Universität Ulm. Es ist organisatorisch und disziplinarisch dem CISO zugeordnet und sollte aus mindestens zwei IT-Sicherheitsspezialisten bestehen.

Das CERT unterstützt die Einrichtungen bei deren Analyse und Behebung und koordiniert den ggf. erforderlichen Meldeprozess. Es bildet außerdem die Schnittstelle zu den operativen Ansprechpersonen der betriebskritischen Infrastrukturen und Fachverfahren, um bei Sicherheitsvorfällen zügig handeln und umfassende forensische Analysen durchführen zu können (Mehrstufigkeit). Zudem wirkt es bei der Entwicklung des Informationssicherheitskonzepts und den Informationssicherheitsrichtlinien mit.

(2) Die gesamte Struktur und Organisation des Informationssicherheitsprozesses der Universität Ulm fasst das folgende Schaubild zusammen:



§ 6 Inkrafttreten

Diese Leitlinie tritt am Tage nach ihrer Veröffentlichung in den Amtlichen Bekanntmachungen der Universität in Kraft.

Ulm, den 29.09.2020

gez.

Prof. Dr.-Ing. Michael Weber

- Präsident -