Ergebnisse der ZKI Top Trends-Umfrage des ZKI-Arbeitskreises Strategie und Organisation für das Jahr 2024

Malte Dreyer, Humboldt-Universität zu Berlin, https://orcid.org/0000-0002-1775-8622

malte.dreyer@hu-berlin.de

https://doi.org/10.5281/zenodo.10640084

Einführung

Der Arbeitskreis Strategie und Organisation des ZKI-Vereins[1] führt eine jährliche Umfrage zu den wichtigsten Themen und Trends von IT-Einrichtungen aus Hochschulen und Forschungseinrichtungen durch. Die Umfrageergebnisse sollen dabei helfen, wichtige Entwicklungen, Themen und Best Practices im Blick zu behalten und bei den umfangreichen Themenfeldern der Digitalisierung und der rasanten Erneuerung von Technologien Schritt zu halten bzw. auch Anregungen für die weitere Ausgestaltung an der eigenen Einrichtung zu gewinnen.

Die Kernumfrage adressiert die wichtigsten Themen und Veränderungen im Umfragejahr in standardisierter Form. Darüber hinaus werden in jedem Jahr individuelle Schwerpunkte abgefragt, die viele Einrichtungen beschäftigen. Für das Jahr 2024 lagen die Schwerpunktfragen im Bereich **Digitaler Souveränität:**

- Fragen zu den Dimensionen Digitaler Souveränität sowie der Rolle von Open-Source-Software, Cloud-Diensten und Partnerschaften.
- Fragen im Umfeld der IT-Sicherheit und von Cyber-Angriffen.

Weiterhin wird nach Modellen zur IT-Governance sowie zu den Positionen CDO und CISO gefragt.

Die Umfrage wird von CIOs, Leiterinnen und Leitern von Rechenzentren, IT-Direktorinnen und Direktoren sowie Personen in vergleichbaren Rollen ausgefüllt. Die Beantwortung ist bei allen Fragen optional. In diesem Artikel werden die Ergebnisse der Top-Trends-Umfrage 2024 dargestellt[2].

Im Jahr 2024 haben 180 Einrichtungen aus Deutschland, Österreich und der Schweiz an der Umfrage teilgenommen. Die meisten Umfrageteilnehmenden haben die Umfrage in weniger als 9 Minuten beantwortet, 75% in weniger als 20 Minuten.

Die Umfrageergebnisse aus dem Vorjahr 2023 sind unter https://zenodo.org/doi/10.5281/zenodo.7599852 aufbereitet.

[1] https://www.zki.de/

[2] Ich bedanke mich bei Maik Bierwirth für das kritische Lektorat.

Inhalte

Zusammenfassung

Die Umfrage hat in diesem Jahr mit 180 Teilnehmenden eine weit größere Resonanz gefunden, als in den Vorjahren. Dies liegt zum einen an der Beteiligung von Hochschulen aus Österreich und der Schweiz, zum anderen auch an einer stärkeren Beteiligung aus deutschen Hochschulen.

Cybersecurity und IT-Sicherheit werden sowohl im Kontext der Sicherheitstechnologien als auch in Bezug auf Datenschutz und Compliance bei fast allen Fragen genannt. In diesem Jahr liegt ein Schwerpunkt der Antworten auf den Herausforderungen zum Aufbau eines Notfallmanagements bzw. dem Einsatz zusätzlicher Komponenten in diesem Zusammenhang. Über 80% der Hochschulen haben bereits die Position eines CISO[3] eingerichtet. Die Rolle eines CDO ist derzeit lediglich an ca. 18% der Hochschulen etabliert. Die überwiegende Anzahl der teilnehmenden Hochschulen folgt in der Entwicklung des ISMS den Vorgaben des BSI-Grundschutz. Wobei es als ein großer Erfolg für den ZKI Arbeitskreis Informationssicherheit zu werten ist, dass ungefähr die Hälfte der BSI-Nennungen auf die spezifischen Empfehlungen für Hochschulen – dem BSI-ZKI IT-Grundschutzprofil für Hochschulen – entfallen. Mit ca. 14% fallen die Nennungen bzgl. des Einsatzes der ISO27K-Reihe geringer aus. Fast die Hälfte der teilnehmenden Hochschulen haben bereits einen Dienstleister für die Reaktion auf Cybervorfälle eingebunden. Die Bedrohungslage für Cyberangriffe auf die eigene Einrichtung wird auf einer Skala von 1 – sehr gering – bis 10 – sehr hoch – durchschnittlich mit ca. 8 als hoch bewertet. In Österreich liegt dieser Wert noch geringfügig höher. Die Herausforderungen, qualifizierte IT-Fachkräfte zu finden und zu halten, nehmen in den Antworten einen noch größeren Anteil ein als in den Vorjahren. Dies zeigt sich auch an Antworten zur Neugestaltung der IT-Organisation, der Beschäftigung mit modernen Arbeitsformen und neuen Organisationsstrukturen. Das Thema Digitale Transformation durchdringt die Antworten auf die meisten Fragen. Hierunter fallen allgemein die Umstellung auf digitale Prozesse, aber auch sehr konkrete Antworten zur Umstellung von Verwaltungsabläufen. Der Einsatz von internen oder externen Clouds und Cloud-Technologien sowie vielfältige Kooperationen zeigen eine große Dynamik in dem Bestreben der IT-Zentren, dem Bedarf an neuen Diensten und Technologien gerecht zu werden. „Automatisierung“ ist in diesem Jahr eine Antwort, die erstmalig sehr häufig im Zusammenhang mit „Digitalisierung“ erwähnt wird. Gleichzeitig wird Automatisierung auch im Umfeld von neuen Technologien und KI als ermöglichende Technologiegrundlage für die Digitalisierung genannt. In diesem Zusammenhang ist auch die wesentlich verstärkte Nennung von Containertechnologien zu sehen.

Die Themenkomplexe Governance und Compliance erfahren im Vergleich zu den Vorjahren eine weit stärkere Erwähnung in den Antworten. Bei der Frage „Welche gesetzgeberischen Regelungen sehen Sie im nächsten Jahr als besonders relevant?“ wird dies besonders deutlich. Im Vergleich zu den Vorjahren werden dort sehr umfangreiche Antworten zu Standards und Gesetzen gegeben, die für den Betrieb angestrebt werden, und eine weit stärkere Nennung von Policies als Grundlage für strukturierte Abwägungsprozesse und Entscheidungen. Da eine stärkere Aussagefähigkeit hinsichtlich Compliance auch übergreifend mit einer klareren und expliziteren Governance für die Führung der IT-Zentren einhergehen, nehmen auch Antworten zur Umgestaltung von IT-Zentren, zu Neustrukturierungen, Maßnahmen zur Qualitätssicherung und zu Methoden zur Projektsteuerung zu.

[3] Chief Information Security Officer – oft auch „IT-Sicherheitsbeauftragte“

Die relevanten Top-Trends im Jahr 2024 für die ZKI-Community sind die Themen:

Tabelle 1: Relevante Top-Trends –194 Nennungen von 91 Einrichtungen

Die Umfrage fragt zum einen nach allgemeinen IT-Trends und zum anderen nach Trends, die für die eigene Einrichtung besonders relevant sind (vgl. Kernumfrage). Dargestellt sind hier die Trends mit der höchsten Relevanz für die Einrichtungen. Gab es in der Vergangenheit jeweils eine größere Differenz zwischen den allgemeinen und den relevanten Themen, so hat sich dieser Unterschied in den letzten Jahren immer weiter aufgelöst. In diesem Jahr unterscheiden sich die Antworten lediglich in einer konkreteren Beschreibung der relevanten Themen und sind von den Themen her überwiegend identisch. Im Vorjahr wurde das Thema „KI“ sehr häufig in den allgemeinen Trends genannt, jedoch noch nicht als relevant für die eigene Einrichtung gesehen. Dies hat sich für 2024 verändert und das Thema hat den zweiten Platz der Nennungen erreicht.

Schwerpunktfragen 2024 – Digitale Souveränität

Das Thema „Digitale Souveränität“ (DS) nimmt für Hochschulen und Forschungseinrichtungen entlang der Konzentration von Dienstleisterstrukturen, steigenden Lizenzkosten, Datenschutz- und IT-Sicherheitserwägungen, wechselnden und unvorhersehbaren Rahmenbedingungen sowie Nachhaltigkeitsaspekten einen zunehmenden Stellenwert ein. Das Thema kreist dabei um die Frage, in welchem Ausmaß Einrichtungen über den Einsatz digitaler Ressourcen, Daten und Infrastrukturen selbst entscheiden können oder Veränderungen durch den Markt hinnehmen müssen. Für Hochschulen bedeutet digitale Souveränität konkreter, in welchem Umfang sie die Selbstbestimmtheit über ihre digitalen Technologien, Systeme und Daten behalten und dadurch ihre Lehr- und Forschungsfreiheit erhalten können.

Auch der Wissenschaftsrat hat sich mit seiner Veröffentlichung „Empfehlungen zur Souveränität und Sicherheit der Wissenschaft im digitalen Raum“ zum Thema positioniert[4]. In den Empfehlungen weist der WR dem Wissenschaftssystem eine besondere Bedeutung hinsichtlich der Förderung von Digitaler Souveränität zu und empfiehlt die bestehenden Kompetenzen und Kooperationsstrukturen gezielt zur Erhöhung der Digitalen Souveränität einzusetzen.

IT-Zentren sind dabei gefordert, das Thema Digitale Souveränität für sich zu interpretieren und konkrete Maßnahmen abzuleiten bzw. Strategien zu entwickeln, um eine nachhaltige Aufstellung ihres Service-Portfolios zu fördern. Im ZKI-Arbeitskreis wurde das Thema im Jahr 2023 diskutiert und dabei wurden unterschiedliche Dimensionen identifiziert, wie die Fragestellungen rund um Digitale Souveränität die Strategie und das Handeln von IT-Zentren beeinflussen[5]. Hieraus entwickelte sich die Idee, das Thema „Digitale Souveränität“ als Schwerpunktthema für die kommende Top-Trends-Umfrage auswählen, um einen breiteren Überblick zu gewinnen, wie Digitale Souveränität an den Hochschulen bereits gefördert wird und mit welchen Handlungsfeldern das Thema assoziiert wird.

Die Schwerpunktfragen zum Thema Digitale Souveränität in der Umfrage waren:

- Was sind aus Ihrer Sicht die wichtigsten Dimensionen oder Aufgabenbereiche, die „Digitale Souveränität“ Ihrer Hochschule ausmachen?
- Welche Rolle spielen Open-Source-Technologien in Ihren Bemühungen um digitale Souveränität?
- Welche Rolle spielen Cloud-Dienste und -Infrastrukturen außerhalb Ihrer Einrichtung bei der Umsetzung Ihrer digitalen Souveränitätsstrategie, und wie sichern Sie diese ab?
- Welche Partnerschaften und Kooperationen mit anderen Hochschulen oder Forschungseinrichtungen unterhält Ihre Einrichtung, um die digitale Souveränität zu stärken?
- Welche Maßnahmen hat Ihre Einrichtung ergriffen, um die Sicherheit und Integrität ihrer IT-Infrastruktur zu gewährleisten?
- Nach welchem Standard wird das Informationssicherheitsmanagementsystem ISMS an Ihrer Einrichtung entwickelt?
- Haben Sie einen Dienstleister für „Incident Response“ eingebunden?
- Wie schätzen Sie das Risiko von Cyberangriffen auf Ihre Einrichtung ein?

[4] Wissenschaftsrat (2023): Empfehlungen zur Souveränität und Sicherheit der Wissenschaft im digitalen Raum; Köln. https://doi.org/10.57674/m6pk-dt95

[5] Beispiele für Aspekte von DS, die oft nicht direkt dem Thema zugeordnet werden, sind Mietlizenzen für Access Points oder Speicherlösungen sowie Fragen zu standardisierten Schnittstellen im Bereich der Medientechnik.

Zusammenfassung der Antworten

Die Antworten zeigen, wie vielschichtig das Thema Digitale Souveränität ist und sie verdeutlichen, dass bereits umfangreiche Aktivitäten der Hochschulen bestehen. Hervorzuheben sind hier insbesondere die weitreichenden Kooperationen auf allen Ebenen, nicht nur auf der Ebene der Erbringung von Diensten, sondern auch in der Zusammenarbeit zur Erarbeitung von Themen, für Unterstützungsleistungen und zu Plattformen für den direkten Austausch. Neben Antworten zu konkreten Betriebsmodellen, wie On-Premises, Hochschul-Clouds, externen Clouds oder SaaS wird der Standort des Betriebs innerhalb von Deutschland oder innerhalb Europas, in Zusammenhang mit Herausforderungen beim Datenschutz, als Kernkriterium aufgeführt. Auch ein Fokus auf die Vertragsgestaltung mit externen Dienstleistern, Exit-Strategien, Multi-Vendor-Ansätze und der Bedarf für offene Schnittstellen werden häufig genannt.

Die Ergebnisse zeigen, dass eine sehr differenzierte und reflektierte Haltung zum Einsatz von Cloud-Diensten besteht. Dieser Themenkomplex geht einher mit einer klareren Steuerung der Entscheidungsfindung zum Einsatz von Software und dem Bezug von Lizenzen entlang von Policies. Häufig wird dabei auch ein enger Zusammenhang mit der Zugänglichkeit und Einführung von innovativen Technologien erwähnt, die ggf. aufgrund des Personal- und Fachkräftemangels sonst für viele Hochschulen nicht leistbar wäre. Hier besteht ein deutliches Desiderat für zusätzliche kollaborative Ansätze, um zumindest im Zusammenspiel von Hochschulen, im Rahmen von Verbünden oder in Arbeitsgemeinschaften, solche innovativen Themen für mehr Hochschulen nutzbar zu machen.

Neben den Betriebs- und Kontrahierungsformen gibt es viele Nennungen, die auf die Etablierung von Alternativen für bestehende Produkte abzielen. Open-Source-Policies sind dabei ein häufig beschriebener Ansatz, um Vendor-Lock-ins aufzulösen oder für die Zukunft zu vermeiden. Die überwiegende Anzahl der Antworten räumt Open-Source-Software (OSS) dabei eine große Rolle ein oder hat eine Open-Source-First-Policy etabliert. Neben der technologischen Unabhängigkeit werden auch die größere Flexibilität und Anpassbarkeit bei Open-Source-Ansätzen betont. Im Gegensatz dazu werden auch Akzeptanzprobleme beim Einsatz von OSS genannt.

Nicht zuletzt betrifft die Forderung nach Datensouveränität auch die Datensicherheit der eigenen Infrastruktur und so sind Fragen der IT-Sicherheit eine notwendige Vorbedingung für die Digitale Souveränität der Einrichtungen. Die meisten Antworten beschreiben in diesem Zusammenhang verstärkte Aktivitäten für den Aufbau eines ISMS (Information Security Management System) und von BCM (Business Continuity Management) bzw. den Aufbau von eigenen Personalkapazitäten und die Einbeziehung von externen Dienstleistungen für diese Zwecke. Begleitet werden diese Veränderungsprozesse durch umfangreiche technische Maßnahmen wie z.B. in den Bereichen Identity- und Access-Management, Netzwerksicherheit und der Absicherung der Basisinfrastrukturen zur Virtualisierung.

In diesem Themenfeld werden ebenso vermehrt Kostenabwägungen vor dem Hintergrund von ausbleibenden Budgeterhöhungen oder sogar Budgetkürzungen als Motivation für die Zuwendung zum Thema Digitaler Souveränität erwähnt. Dies bedeutet im Umkehrschluss, dass viele Hochschulen von einem stärkeren Einsatz für Digitale Souveränität auch konkrete Kostenvorteile erwarten.

Was sind aus Ihrer Sicht die wichtigsten Dimensionen oder Aufgabenbereiche, die „Digitale Souveränität“ Ihrer Hochschule ausmachen?

Die Frage erhielt 233 Antworten von 97 Hochschulen. Die Antworten verteilen sich dabei wie folgt.

Kategorie	Anzahl Nennungen
On-Premises-Betrieb	34
Open-Source-Software	31
Etablierung von Alternativen	18
Exit-Verträge für Cloud-Anbieter	11
Technologische Unabhängigkeit	10
Datenhoheit und Datenschutz	9
Implementierung von Standards	9
Zusammenarbeit/Kooperation	8
Betriebsmodelle und Datenkontrolle	7
Cloud-Strategie	6
Softwarestrategie	5
Eigenentwicklung und Innovation	5
Herausforderungen bei der Umsetzung	5
Digitale Fähigkeiten und Ressourcen	4

In den Antworten zu den thematischen Bereichen der Digitalen Souveränität konnten die folgenden teilweisen überlappenden oder auch gegensätzlichen Dimensionen identifiziert werden.

Betriebsmodelle und Datenkontrolle: Diese Kategorie befasst sich mit der Vermeidung von Vendor-Lock-Ins, dem On-Premise-Betrieb, der EU/DE-Auftragsdatenverarbeitung, der Hoheit über Daten und Datenschutz, der Einführung von Standards zur Souveränität von einzelnen Anbietern, den Exit-Strategien und -Verträgen für Cloud-Anbieter.

Softwarestrategie: Der Schwerpunkt liegt hier auf der Nutzung von Open-Source-Software, der Etablierung alternativer Ansätze, dem Multi-Vendor-Ansatz und der Stärkung von Open-Source-Communities.

Technologische Unabhängigkeit: Hier geht es darum, nicht zu stark von externen Anbietern abhängig zu sein, einen Vendor-Lock-In zu vermeiden und Standards für technologische Unabhängigkeit umzusetzen.

Cloud-Strategie: Diese Kategorie umfasst strategische Abwägungen zwischen Cloud- und lokalem Betrieb, offene Schnittstellen für anzubindende Systeme, hochschulübergreifende Private-Clouds und Exit-Strategien für Cloud-Anbieter.

Digitale Fähigkeiten und Ressourcen: Es geht darum, die Stärkung digitaler Fähigkeiten bei Studierenden und Beschäftigten zu fördern, alternative Ansätze für Unabhängigkeit und Fachwissen abzuwägen, Standardisierungsmaßnahmen anzuwenden und interne Schulungen durchzuführen.

Herausforderungen bei der Umsetzung: Aufgezeigt werden die Herausforderungen bei der Umsetzung von On-Premises-Betrieb und Herausforderungen für einen Wechsel aufgrund von Personalmangel oder auch aufgrund eines Mangels an einsatzfähigen Alternativen.

Zusammenarbeit/Kooperation: Diese Kategorie behandelt Kooperationen mit anderen Hochschulen, die Schaffung von Kooperationsökosystemen und die Beteiligung anderer Organisationen bei Softwareauswahl und Verhandlungen mit Anbietern.

Datensicherheit und Datenschutz: Thematisiert wird das Sicherheitsbewusstsein bei IT-Führungskräften, die mangelnden Ressourcen für Sicherheit und der Fokus auf Datenschutz.

Eigenentwicklung und Innovation: Dies betrifft den Aufbau von Entwicklungskompetenzen im eigenen Haus, detaillierte Abwägungen bezüglich Software-Nutzung und die Berücksichtigung von Inhouse-Entwicklungen.

Welche Rolle spielen Open-Source-Technologien in Ihren Bemühungen um digitale Souveränität?

Auf diese Frage gab es 116 Antworten von 98 Hochschulen, die sich wie folgt auf die Kategorien verteilen lassen.

Kategorie	Anzahl
Begrenzte oder untergeordnete Rolle	16
Abwägung von Vor- und Nachteilen	15
Open-Source First	14
Flexibilität und Anpassbarkeit	14
Kostenmanagement und Budgetbeschränkungen	12
Unabhängigkeit und Vermeidung von Vendor-Lock-in	8
Professionalisierung und Support	8
Hohe Priorität und aktive Nutzung	6
Fehlende Nutzung oder Akzeptanz	4
Sicherheits- und Compliance-Überlegungen	4
Spezifische Anwendungsbereiche	3
Komplementärer Einsatz zu kommerzieller Software	3

Die Antworten lassen sich in die folgenden Kategorien einteilen.

Begrenzte oder untergeordnete Rolle: Antworten, die darauf hindeuten, dass Open-Source-Technologien eine begrenzte oder untergeordnete Rolle spielen. Häufig werden als Gründe hierfür Ressourcenbeschränkungen oder fehlende Expertise genannt.

Abwägung von Vor- und Nachteilen: Antworten, die eine differenzierte Sichtweise zeigen, indem sie Vor- und Nachteile von Open-Source gegenüber proprietärer Software für jeden einzelnen Einsatzzweck abwägen.

Open-Source First: Antworten, die auf die strategische Entscheidung hinweisen, Open-Source-Technologien zu integrieren, oft im Rahmen einer Open-Source-First-Strategie.

Flexibilität und Anpassbarkeit: Antworten, die die Flexibilität und Anpassbarkeit von Open-Source-Software betonen, um spezifische Bedürfnisse zu erfüllen.

Kostenmanagement und Budgetbeschränkungen: Antworten, die den Einsatz von Open-Source als kosteneffiziente Lösung hervorheben, insbesondere bei Budgetbeschränkungen.

Unabhängigkeit und Vermeidung von Vendor-Lock-in: Antworten, die auf die Bedeutung von Open-Source für die Unabhängigkeit von einzelnen Softwareanbietern und die Vermeidung von Vendor-Lock-ins hinweisen.

Professionalisierung und Support: Antworten, die die Bedeutung von professionellem Support für Open-Source-Technologien hervorheben.

Hohe Priorität und aktive Nutzung: Antworten, die betonen, dass Open-Source-Technologien eine zentrale Rolle spielen und aktiv genutzt werden.

Fehlende Nutzung oder Akzeptanz: Antworten, die angeben, dass Open-Source-Technologien nicht genutzt werden oder auf Widerstand stoßen, oft aufgrund von Personal- oder Kompetenzmangel.

Sicherheits- und Compliance-Überlegungen: Antworten, die auf Sicherheitsaspekte und Compliance-Anforderungen im Zusammenhang mit Open-Source-Technologien eingehen.

Spezifische Anwendungsbereiche: Antworten, die auf spezifische Bereiche hinweisen, in denen Open-Source-Technologien bevorzugt eingesetzt werden, wie Webdienste oder Lernmanagementsysteme.

Komplementärer Einsatz zu kommerzieller Software: Antworten, die den Einsatz von Open-Source als Ergänzung zu kommerzieller Software beschreiben.

Die Antworten zu dieser Frage weisen eine besonders hohe Heterogenität auf. Deshalb wurde zusätzlich untersucht, wie sich die Antworten bei eher großen und eher kleinen Hochschulen unterscheiden.

Eher große Hochschulen betonen eine große Rolle von Open Source, Open-Source-First-Strategien, Serverbetrieb auf Linux, die historische Bedeutung von OSS für Hochschulen und gesteigerte Support-Aufwendungen für OSS. Eher kleinere Hochschulen betonen die Kostenaspekte beim Einsatz von OSS, die Forderung, dass OSS auch sicherheitstechnisch erprobt sein muss, eine Abwägung von Funktionalitäten zum Wartungsaufwand und einen Schwerpunkt für die Bereiche Forschung und Lehre.

Weiterhin wurden bei dieser Frage spezifische Projekte bzw. Produkte benannt:

- BigBlueButton
- Bitwarden
- BookStack
- Docker
- Linux
- Nextcloud
- OpenProject
- OpenStack
- Suricata
- Znuny/OTRS

Welche Rolle spielen Cloud-Dienste und -Infrastrukturen außerhalb Ihrer Einrichtung bei der Umsetzung Ihrer digitalen Souveränitätsstrategie, und wie sichern Sie diese ab?

Für diese Frage gab es 106 Antworten von 88 Hochschulen mit der folgenden Verteilung.

Kategorie	Anzahl
Herausforderungen Sicherheit & Datenschutz	13
Große Rolle	12
Irrelevant	8
Kleine Rolle	8
Zunehmend wichtig	7
Im Rahmen von Kooperationen	7
Herausforderungen Vertragsmanagement	7
Ermöglichung Technologiezugang	6
Im Rahmen einer Multi-Cloud-Strategie	5
Lösungsansatz für Personal- & Fachkräftemangel	5
Fehlendes Problembewusstsein	4
Schulung & Bewusstsein	3
Ermöglichung besserer Service-Levels	2
Nur bei bestehender Anbieterflexibilität	2

Die Antworten auf diese Frage lassen sich wie folgt in Kategorien einordnen.

Herausforderungen Sicherheit & Datenschutz: Es bestehen große Herausforderungen zur Abstimmung der notwendigen Maßnahmen im Bereich Sicherheit und Datenschutz für die Nutzung von Cloud-Diensten.

Große Rolle: Cloud-Dienste sind ein zentraler Bestandteil der digitalen Infrastruktur und Strategie.

Irrelevant: Cloud-Dienste haben keinen Einfluss auf die digitale Strategie der Einrichtung.

Kleine Rolle: Cloud-Dienste werden nur begrenzt oder für spezifische Zwecke genutzt.

Zunehmend wichtig: Die Bedeutung von Cloud-Diensten nimmt zu.

Im Rahmen von Kooperationen: Nutzung von Cloud-Diensten im Rahmen von Partnerschaften mit anderen Hochschulen.

Herausforderungen im Vertragsmanagement: Schwierigkeiten und Komplexität im Management von Cloud-Verträgen.

Ermöglichung Technologiezugang: Cloud-Dienste ermöglichen Zugang zu fortschrittlichen Technologien.

Multi-Cloud-Strategie: Verfolgung eines Ansatzes, der mehrere Cloud-Anbieter einbezieht.

Personal- & Fachkräftemangel: Cloud-Dienste als Lösung für Mangel an Personal und Fachkräften.

Fehlendes Problembewusstsein: Geringes Bewusstsein für Probleme und Risiken im Zusammenhang mit Cloud-Diensten.

Schulung & Bewusstsein: Notwendigkeit von Ausbildung und Bewusstseinsbildung im Umgang mit Cloud-Diensten.

Service-Levels: Cloud-Dienste ermöglichen verbesserte Servicequalität.

Anbieterflexibilität: Präferenz für Cloud-Dienste, bei denen ein Anbieterwechsel einfach ist.

Aufgrund der großen Heterogenität der Antworten wurde auch untersucht, wie sich die Antworten bei eher großen Hochschulen und eher kleinen Hochschulen unterscheiden. Eher große Hochschulen betonen bei den Aspekten den Einsatz von Community-Cloud-Lösungen im Bereich der Zusammenarbeit, die Verwendung von AWS, Azure und Google, die Nutzung der Dienste des DFN und Dienste anderer Hochschulen. Eher kleinere Hochschulen betonen die Aspekte der Skalierbarkeit und Verfügbarkeit, den Bedarf für Sensibilisierung und Awareness, Fragen des Datenschutzes sowie die Herausforderungen im Zusammenhang mit dem Vertrags-, Kosten-, und Supportmanagement bei Cloud-Diensten. Es wird häufiger betont, dass eher nur wenige Verträge für Cloud-Dienste abgeschlossen werden, die aber jeweils eine hohe Relevanz für die Hochschule haben.

Die folgenden Produkte oder Organisationen wurden im Umfeld dieser Frage erwähnt.

- BBB (BigBlueButton)
- COSINEX Vergabeportal
- DFN (Deutsches Forschungsnetz)
- FAUbox (Bayerische PowerFolder-Instanz)
- iCAS
- Jitsi
- M365 (Microsoft 365)/ Microsoft Office
- MATLAB
- Microsoft Azure
- Microsoft Exchange
- Microsoft Sharepoint
- Microsoft Teams
- Overleaf
- SAP
- SWITCHcloud
- VEEAM
- Zoom/Zoom X

Welche Partnerschaften und Kooperationen mit anderen Hochschulen oder Forschungseinrichtungen unterhält Ihre Einrichtung, um die digitale Souveränität zu stärken?

Diese Frage wurde von 89 Hochschulen mit 111 Nennungen beantwortet. Die Antworten lassen sich wie folgt einordnen.

Kategorie	Anzahl
Regionale und Bundesweite Kooperationen	16
Beteiligung an spezialisierten Allianzen und Projekten	13
Kooperationen in speziellen Bereichen	11
Mitgliedschaft in IT-Netzwerken und Verbänden	10
Spezifische Hochschulpartnerschaften	10
Regelmäßiger Austausch und Abstimmungen	10
Kooperative Software- und Infrastrukturprojekte	10
Keine Partnerschaften oder Kooperationen	9
Informeller Erfahrungsaustausch und persönliche Kontakte	9
Bildung und Nutzung von Genossenschaften und Verbünden	7
Nutzung gemeinsamer Ressourcen	6
Internationale und nationale Fachverbände und Initiativen	6
Initiativen zur digitalen Forschungsinfrastruktur	6
Austausch von Cloud- und IT-Dienstleistungen	5
Kooperationen im Bereich Hochleistungsrechnen	4
Kooperationen für Notfall- und Krisensituationen	4

Die Antworten auf diese Frage lassen sich in die folgenden Kategorien einordnen.

Regionale und Bundesweite Kooperationen: Diese Kategorie deckt Partnerschaften ab, die sich auf eine bestimmte geografische Region konzentrieren.

Beteiligung an spezialisierten Allianzen und Projekten: Diese Kategorie umfasst die Beteiligung an spezialisierten Projekten und Allianzen mit einem fokussierten Ziel.

Kooperationen in speziellen Bereichen: Beispiele sind „Kooperation im Bereich Current Research Information System (CRIS)“, „Kooperationen im Bereich IT-Sicherheit“. Diese Kategorie umfasst Kooperationen, die sich auf spezielle Bereiche oder Themen konzentrieren.

Mitgliedschaften in IT-Netzwerken und Verbänden: Beinhaltet Antworten wie ZKI-Mitgliedschaft, DFN-Mitgliedschaft, OSBA-Mitgliedschaft. Diese Kategorie umfasst die Teilnahme an Netzwerken und Verbänden, die auf IT- und digitale Infrastruktur spezialisiert sind.

Spezifische Hochschulpartnerschaften: Hier werden konkrete Hochschulnamen genannt, die auf spezifische bilaterale Kooperationen hinweisen.

Regelmäßiger Austausch und Abstimmungen: Diese Kategorie bezieht sich auf regelmäßige Treffen und Koordinationen zwischen verschiedenen Einrichtungen.

Kooperative Software- und Infrastrukturprojekte: Diese Kategorie beinhaltet kooperative Projekte im Bereich Software und Infrastruktur.

Keine Partnerschaften oder Kooperationen: Diese Kategorie beinhaltet Hochschulen, die angeben, keine relevanten Partnerschaften zu haben.

Informeller Erfahrungsaustausch und persönliche Kontakte: Diese Kategorie bezieht sich auf weniger formelle Formen des Austauschs und der Zusammenarbeit.

Bildung und Nutzung von Genossenschaften und Verbünden: Diese Kategorie umfasst die Bildung von Genossenschaften oder Verbünden zur Stärkung der digitalen Souveränität.

Nutzung gemeinsamer Ressourcen: Beispiele sind „Nutzung hochschulübergreifender Angebote für Backup und Cloudspeicher", „Gemeinsames Rechenzentrum". Diese Kategorie fokussiert sich auf die gemeinsame Nutzung von Ressourcen und Infrastrukturen.

Internationale und nationale Fachverbände und Initiativen: Antworten wie „Engagement in AcoNet", „Beteiligung an europäischen Initiativen wie Gaia-X". Hier werden überregionale und internationale Fachverbände und Initiativen erwähnt.

Initiativen zur digitalen Forschungsinfrastruktur: Diese Kategorie betrifft Initiativen, die speziell auf die Verbesserung der digitalen Forschungsinfrastruktur abzielen.

Austausch von Cloud- und IT-Dienstleistungen: Antworten wie „Nutzung der DFN-Cloud", „Community Cloudlösungen". Diese Kategorie betrifft spezifische Dienstleistungen im IT-Bereich, die von den Hochschulen genutzt oder angeboten werden.

Kooperationen im Bereich Hochleistungsrechnen: umfasst die Zusammenarbeit zwischen Hochschulen bei der Nutzung von Hochleistungsrechnern und -systemen. Dies kann die gemeinsame Nutzung von Rechenressourcen, die Entwicklung neuer Technologien und die Förderung von Forschungsprojekten in diesem Bereich beinhalten.

Kooperationen für Notfall- und Krisensituationen: bezieht sich auf die Zusammenarbeit zwischen Hochschulen bei der Vorbereitung und Bewältigung von Notfällen und Krisen. Dies kann die Entwicklung von Notfallplänen, die Ausbildung von Beschäftigten und die Bereitstellung von Ressourcen für Notfälle umfassen.

Die folgenden Produkte oder Organisationen wurden in den Antworten benannt.

- ACOmarket (Austrian Academic Computer Network Marketplace)
- AcoNet (Austrian Academic Computer Network)
- Bayerische Digitalverbund
- BMBWF (Bundesministerium für Bildung, Wissenschaft und Forschung)
- CAMPUSonline (Österreichisches Campusmanagementsystem)
- CRIS NRW Forschungsdatenmanagement
- DFN-Cloud
- DFN-Mitgliedschaft (Deutsches Forschungsnetz)
- DH-NRW (Digital Humanities Nordrhein-Westfalen)
- ELAN (Elearning Academic Network Niedersachsen)
- European University Alliances (Europäische Hochschulverbünde)
- Gaia-X (Dateninfrastruktur für Europa)
- GIT (Gesellschaft für Informatik in Thüringen)
- GWDG (Gesellschaft für wissenschaftliche Datenverarbeitung Göttingen)
- HDN (Hochschule Digital Niedersachsen)

- HIS-Genossenschaftsmitglied (Hochschul-Informations-Systeme)
- LANIT (Landesweite Netzwerke für IT in Niedersachsen)
- LRZ (Leibniz-Rechenzentrum)
- NFDI (Nationale Forschungsdateninfrastruktur)
- NHR (Nationales Hochleistungsrechnen)
- NREN (National Research and Education Network) (SWITCH)
- NRW-Partnerschaften (Partnerschaften in Nordrhein-Westfalen)
- OSBA-Mitgliedschaft (Open Source Business Alliance)
- Rechenzentrumsallianz Rheinland-Pfalz
- Uniko (Österreichische Universitätenkonferenz)
- ZKI-Mitgliedschaft (Zentren für Kommunikation und Informationsverarbeitung)

Welche Maßnahmen hat Ihre Einrichtung ergriffen, um die Sicherheit und Integrität ihrer IT-Infrastruktur zu gewährleisten?

Die Frage wurde von 86 Hochschulen mit 133 Angaben beantwortet.

Kategorie	Anzahl
IT-Management und Governance	14
Personal und Ressourcen	14
Firewall und Netzwerksicherheit	11
Notfallplanung und Reaktionsfähigkeit	8
Awareness und Schulungen	7
Externe Dienstleistungen und Partnerschaften	7
Sicherheitsmaßnahmen und Audits	6
Authentifizierung und Zugangskontrolle	5
Compliance und Standards	4
Virtualisierung und Infrastrukturmanagement	2

Die folgenden Kategorien wurden aus den Antworten gebildet.

IT-Management und Governance: Der Aufbau eines ISMS (Information Security Management System) und BCM (Business Continuity Management) ist für ein strukturiertes Vorgehen im IT-Sicherheitsmanagement erforderlich. Die Einhaltung von Governance-Maßnahmen trägt zur Gesamtstabilität und Resilienz der IT-Systeme bei.

Personal und Ressourcen: Der Aufbau von spezialisierten Kapazitäten für den Bereich IT-Sicherheit und die Förderung der Kompetenzen zu IT-Sicherheit auf allen Ebenen sind wesentlich, um den wachsenden Sicherheitsherausforderungen gerecht zu werden.

Firewall und Netzwerksicherheit: Die Implementierung von Next-Generation-Firewalls und fortschrittlichen Antivirus-Lösungen, zusammen mit Techniken wie Geoblocking und der Einsatz einer WebApplicationFirewall (WAF), stärken die Abwehr von Netzwerkangriffen.

Notfallplanung und Reaktionsfähigkeit: Die Entwicklung von Notfallplänen und die Vorbereitung auf Incident Response sind entscheidend, um auf Sicherheitsvorfälle schnell und effizient reagieren zu können.

Awareness und Schulungen: Bewusstseinsbildung und Schulungen sind wichtig, um die menschliche Komponente der Cybersicherheit zu stärken. Phishing-Simulationen und regelmäßige Trainings können das Bewusstsein für Cyberbedrohungen erhöhen und helfen, sicherheitsrelevante Vorfälle zu reduzieren.

Externe Dienstleistungen und Partnerschaften: Die Zusammenarbeit mit externen Sicherheitsexperten und Dienstleistern, wie einem SOC (Security Operations Center), kann die Fähigkeit zur Erkennung und Reaktion bei Sicherheitsvorfällen erheblich verbessern.

Sicherheitsmaßnahmen und Audits: Regelmäßige Sicherheitsaudits, Penetrationstests und Schwachstellenscans sind wesentliche Elemente zur Identifizierung und Behebung von Sicherheitslücken.

Authentifizierung und Zugangskontrolle: MFA (Multi-Faktor-Authentifizierung) und 2FA (Zwei-Faktor-Authentifizierung) sind effektive Methoden, um unbefugten Zugriff zu verhindern. Die

Durchsetzung starker Passwortregeln und die Sensibilisierung für externe E-Mails erhöhen zusätzlich die Sicherheit.

Compliance und Standards: Die Einhaltung von Standards wie ISO 27001 und BSI sowie die Compliance mit DSGVO-Vorgaben sind nicht nur rechtlich notwendig, sondern auch ein Zeichen für Best Practices im Bereich Sicherheit.

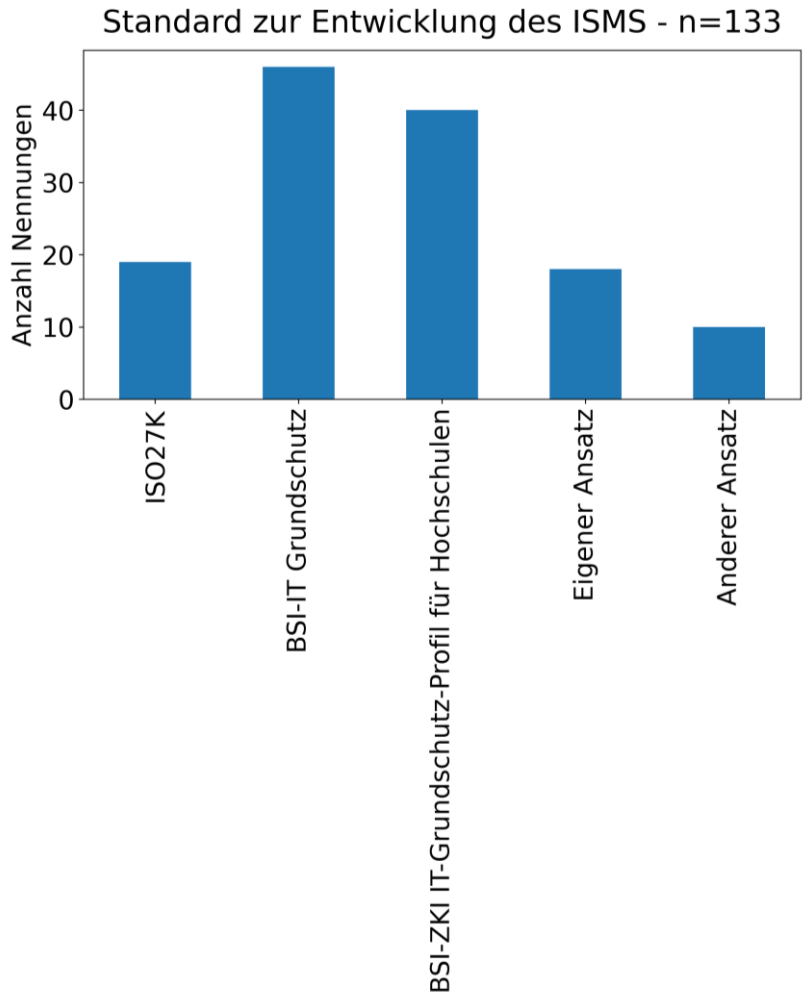
Virtualisierung und Infrastrukturmanagement: Der Wechsel von VMWare zu OpenStack/Proxmox/ Ceph könnte Kostenvorteile bieten und mehr Flexibilität in der Verwaltung der virtuellen Infrastruktur ermöglichen. Die Herausforderung liegt in der Migration und im Umgang mit möglichen Kompatibilitätsproblemen. Das Härten der virtuellen Infrastruktur und der redundante Aufbau aller zentralen IT-Ressourcen sind entscheidend für die Betriebssicherheit.

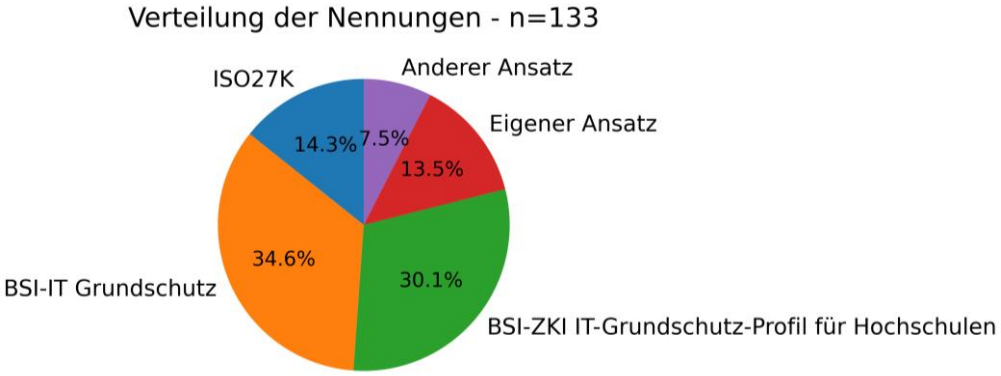
In den Antworten wurden die folgenden Produkte und Organisationen benannt.

- **DFN-Cert:** Ein Sicherheitsdienstleister für Forschungs- und Bildungseinrichtungen.
- **eduroam:** Ein sicherer WLAN-Zugangsdienst für Bildungseinrichtungen.
- **eduVPN:** Ein Virtual Private Network (VPN) für Bildungseinrichtungen.
- **GrayLog Enterprise Security:** Eine Logfile-Analyseplattform.
- **Greenbone:** Ein Schwachstellenscanner, der zur Identifizierung von Sicherheitslücken und zur Stärkung der IT-Sicherheit eingesetzt wird.
- **ISO 27001 und NIST:** Diese sind Sicherheitsstandards, die erwähnt werden, um die Einhaltung von Best Practices zu betonen.
- **Multi-Faktor-Authentifizierung (MFA) und 2-Faktor-Authentifizierung (2FA):** Diese werden als Methoden zur Zugangskontrolle und zur Erhöhung der Sicherheit genannt.
- **Next-Generation-Firewalls:** Diese werden als Teil der Netzwerksicherheit erwähnt.
- **Palo Alto Next-Generation Firewalls:** Eine spezifische Marke von Next-Generation-Firewalls.
- **Proofpoint ET Pro Rule Set:** Ein Regelset für die Sicherheit.
- **Proxmox/Ceph:** Ein Wechsel zu Proxmox und Ceph wird als mögliche Alternative zu VMWare diskutiert.
- **Semperis Purple Knight:** Eine Lösung zur Absicherung von Active Directory.
- **Sentinel One:** Ein Endpoint-Sicherheitsprodukt wird erwähnt.
- **Sophos:** Ein Unternehmen, das Sicherheitslösungen anbietet, wird in Bezug auf Client-Absicherung genannt.
- **Suricata:** Ein Intrusion Detection System (IDS).
- **VMWare:** Dieses Produkt wird in Zusammenhang mit Virtualisierung und Infrastrukturmanagement genannt.
- **WebApplicationFirewall (WAF):** Eine spezielle Firewall für Webanwendungen zur Stärkung der Sicherheit gegenüber Webangriffen.

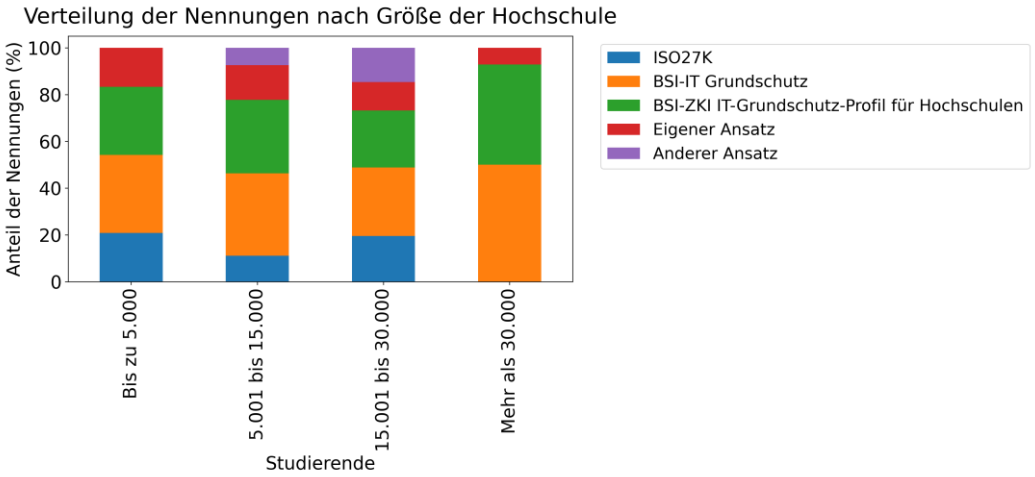
Nach welchem Standard wird das Informationssicherheitsmanagementsystem ISMS an Ihrer Einrichtung entwickelt?

Die folgende Verteilung der Antworten hat sich für diese Frage ergeben.

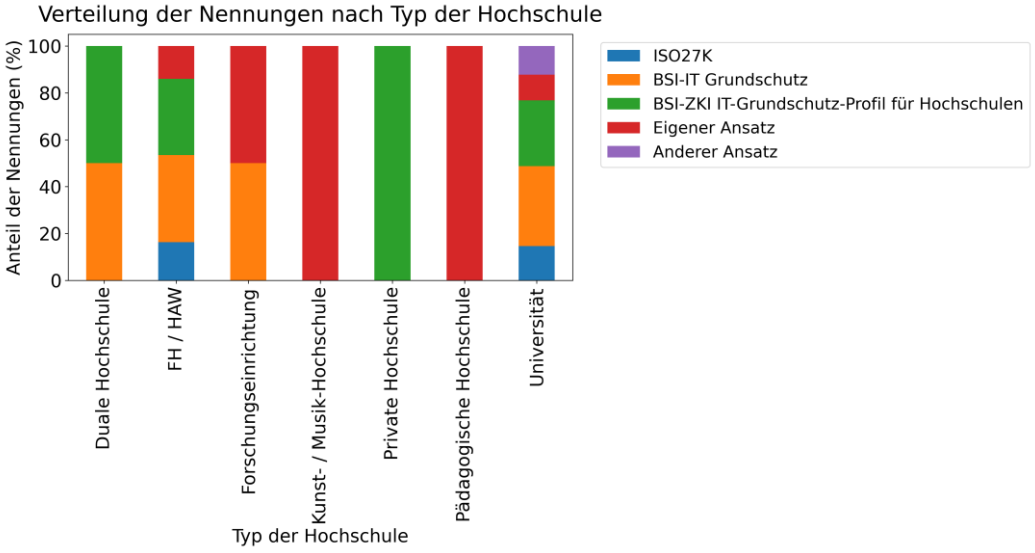




Dargestellt nach der Größe der Hochschule, ergibt sich die folgende Darstellung.



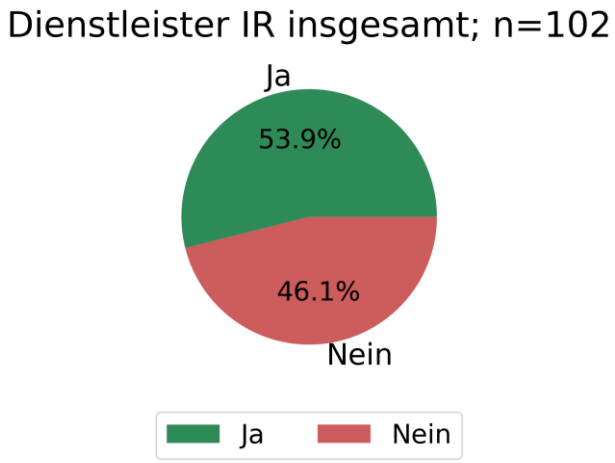
Nach dem Typ der Hochschule unterschieden, ergibt sich die folgende Grafik.



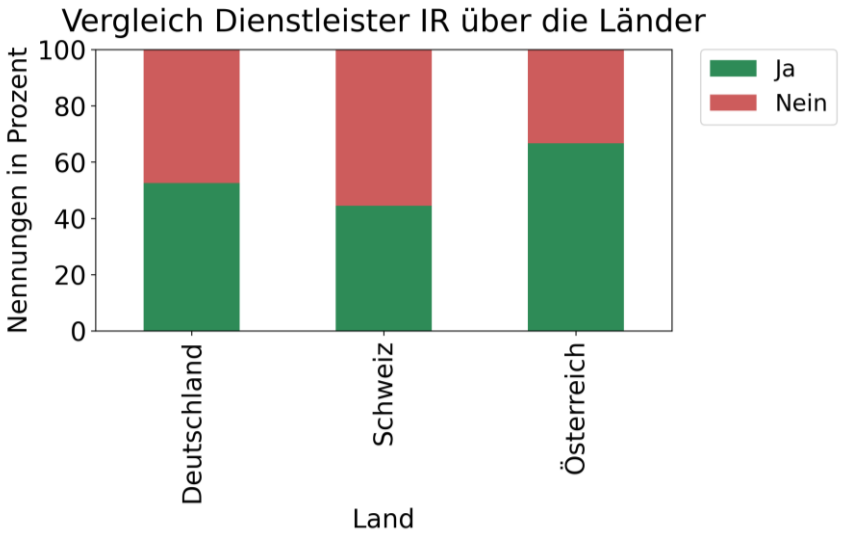
Haben Sie einen Dienstleister für „Incident Response“ eingebunden?

Andere Benennungen für ähnliche Dienstleistungen sind z.B. „APT-Dienstleister“, „Response Retainer“ oder „Cyber Incident Response Retainer“.

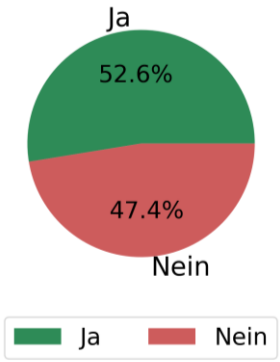
55 Hochschulen haben bereits einen Dienstleister eingebunden, 47 haben dies noch nicht umgesetzt. Die folgende Darstellung illustriert diese Verteilung.



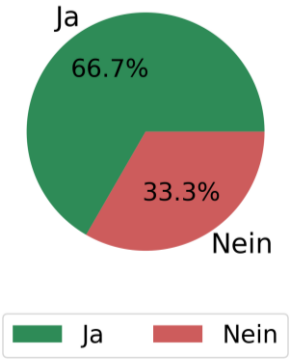
Die Verteilung auf die teilnehmenden Länder für diese Umfrage wird in den folgenden Darstellungen abgebildet.



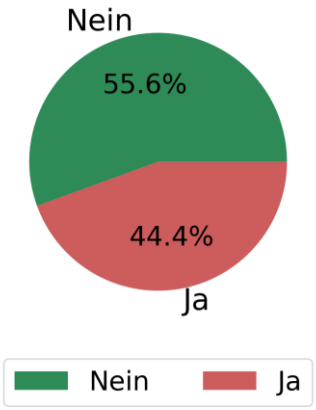
Dienstleister IR - Deutschland; n=78



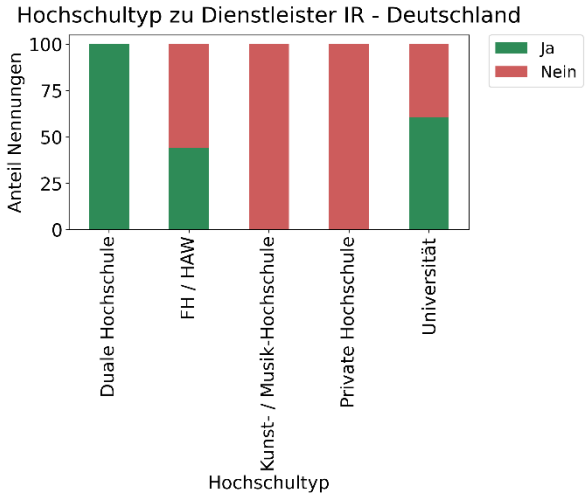
Dienstleister IR - Österreich; n=15

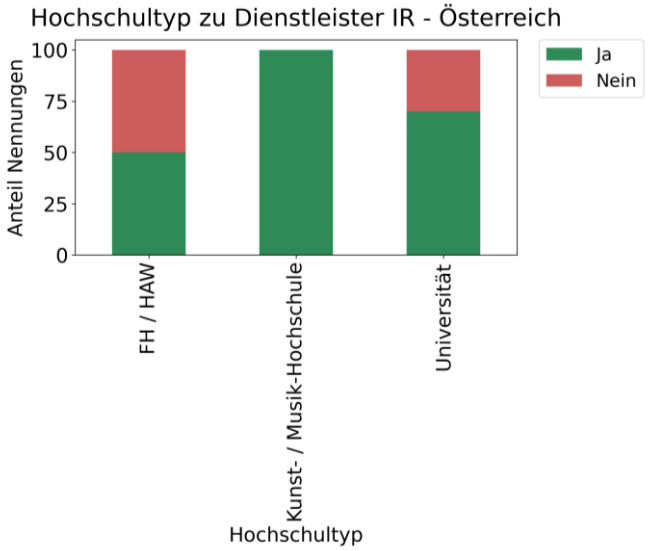


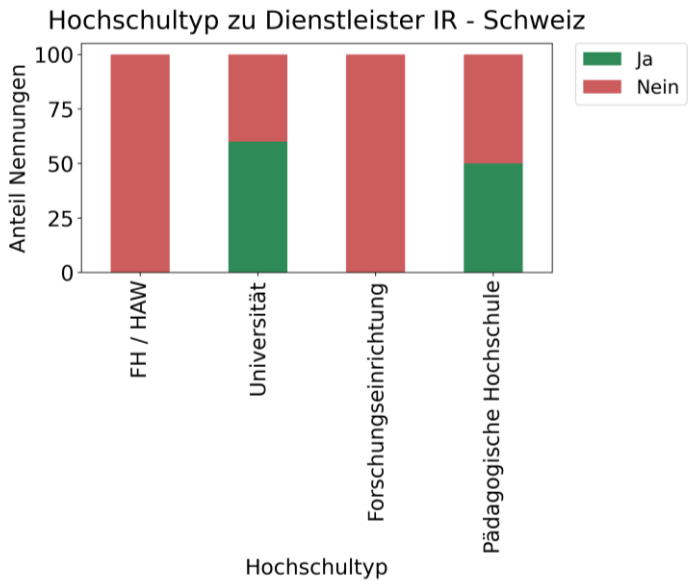
Dienstleister IR - Schweiz; n=9



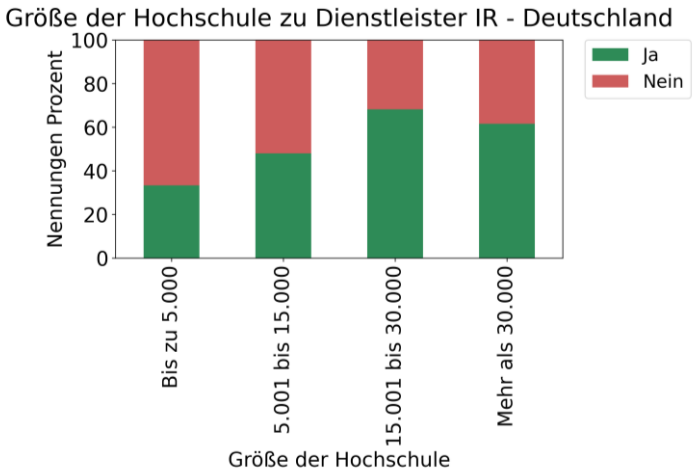
Die folgenden Darstellungen zeigen die Verteilung zur Einrichtung eines IR-Dienstleisters in Bezug auf den Typ der Hochschule.

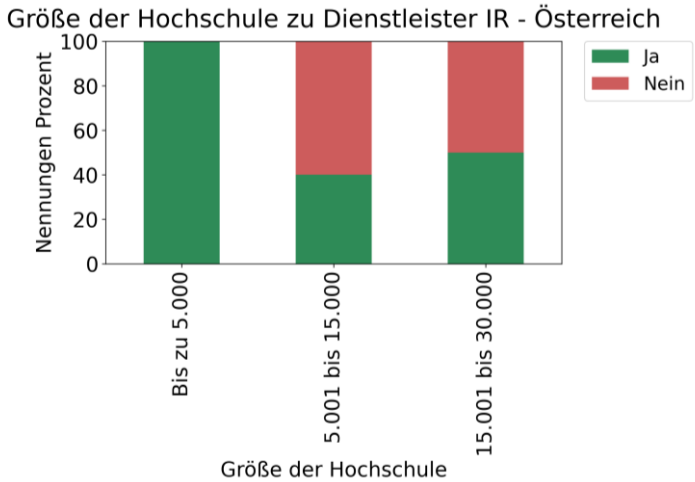


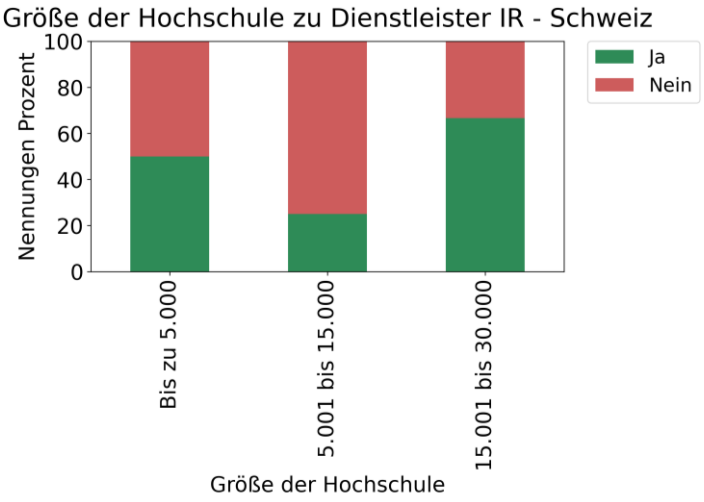




Im Folgenden ist die Verteilung in Abhängigkeit der Größe der Hochschule angegeben.

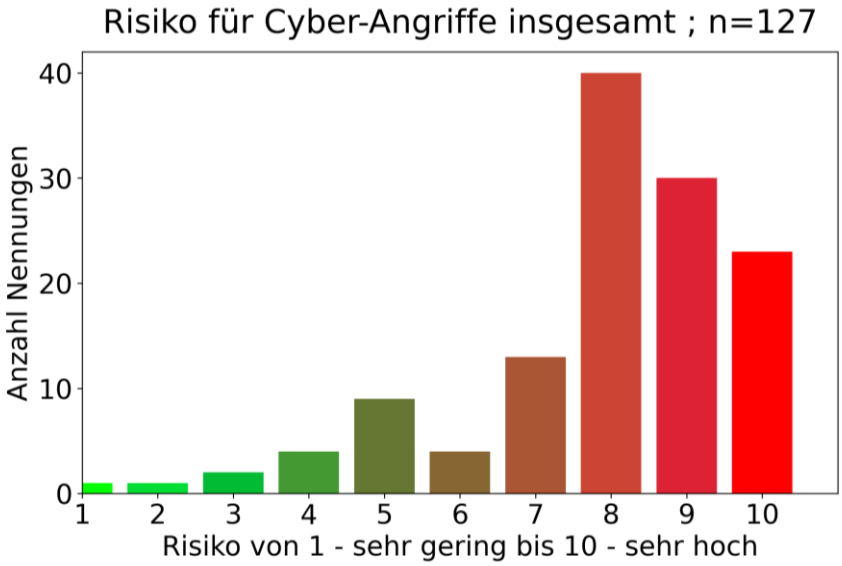





Größe der Hochschule zu Dienstleister IR - Schweiz
Nennungen Prozent
100
80
60
40
20
0
Ja
Nein
Bis zu 5.000
5.001 bis 15.000
15.001 bis 30.000
Größe der Hochschule

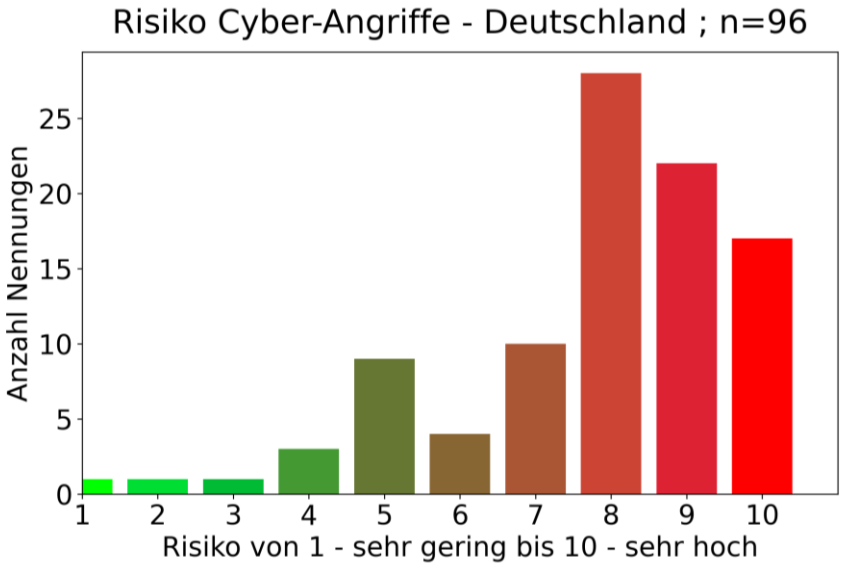
Wie schätzen Sie das Risiko von Cyberangriffen auf Ihre Einrichtung ein?

Im Folgenden sind die Einschätzungen der Teilnehmenden in Bezug auf eine Gefährdung der eigenen Hochschule für Cyberangriffe dargestellt.

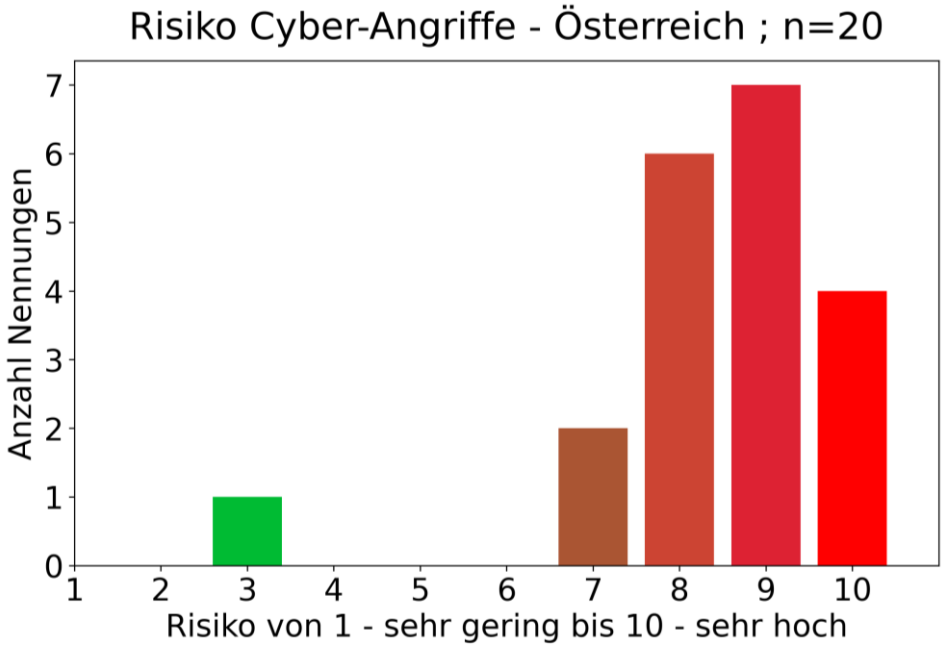


Der Mittelwert über alle Länder hinweg beträgt 7,9.

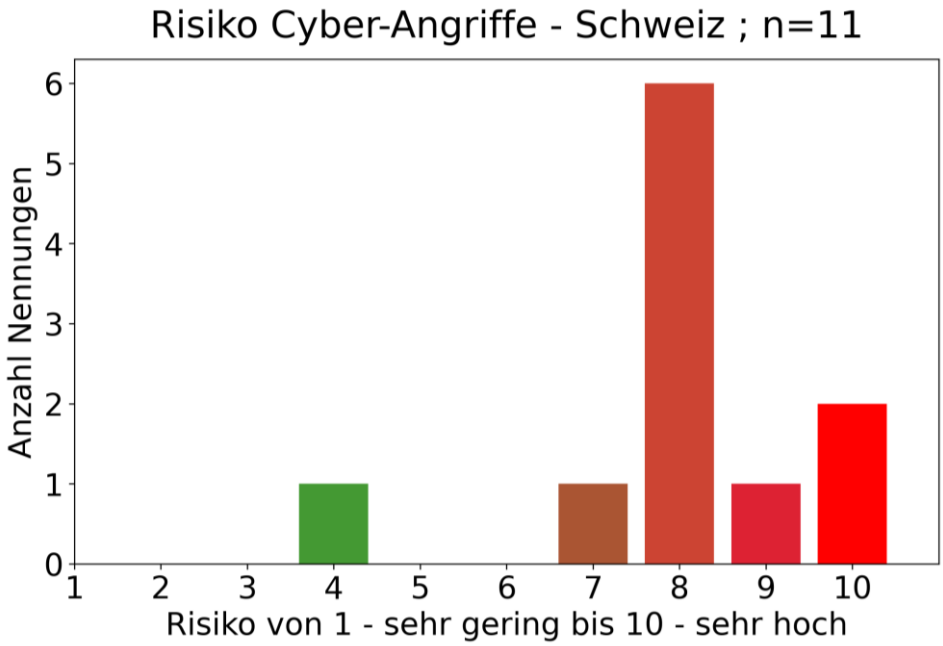
Die folgende Grafik zeigt die Einschätzungen aus Deutschland. Der Mittelwert beträgt 7,8.



Die folgende Grafik zeigt die Bewertung des Risikos für Cyberangriffe durch die Teilnehmenden aus Österreich. Der Mittelwert beträgt 8,4.



In den teilnehmenden Hochschulen aus der Schweiz wird das Risiko für Cyberangriffe im Mittelwert mit 8,0 angegeben.



Veränderungen bei den Top-Trends zum Vorjahr

Diese Fragen sollen beleuchten, wie sich die für IT-Einrichtungen relevanten Top-Trends an Hochschulen und Forschungseinrichtungen über die Jahre verändern.

Im Vergleich zum Vorjahr hat sich die Bedeutung der Top-Trends wie folgt verändert:

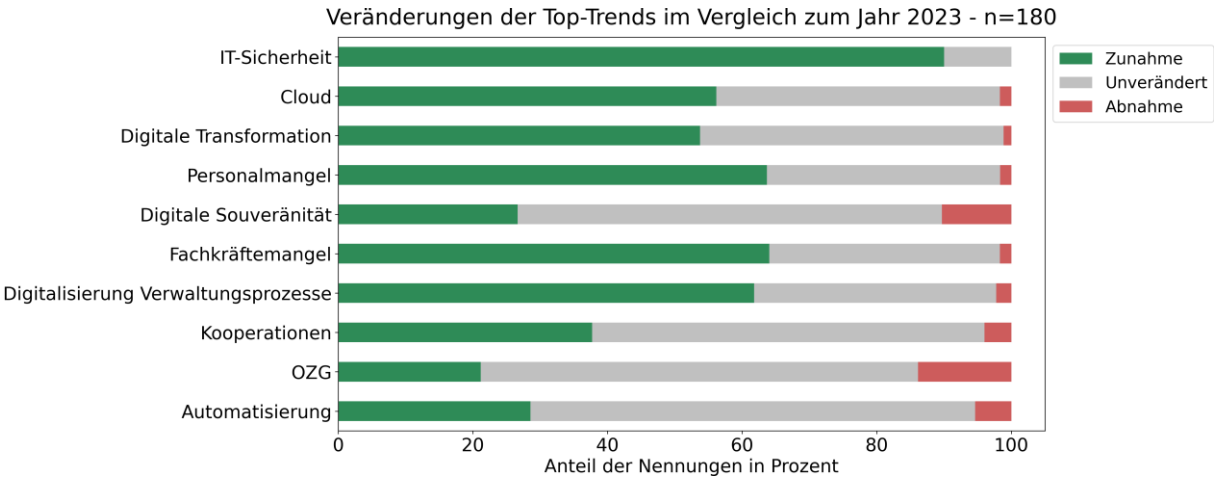


Abbildung 1: Veränderung der Bedeutung der Top-Trends im Vergleich zum letzten Jahr - n=180

Die Top-Themen mit zunehmender Bedeutung sind:

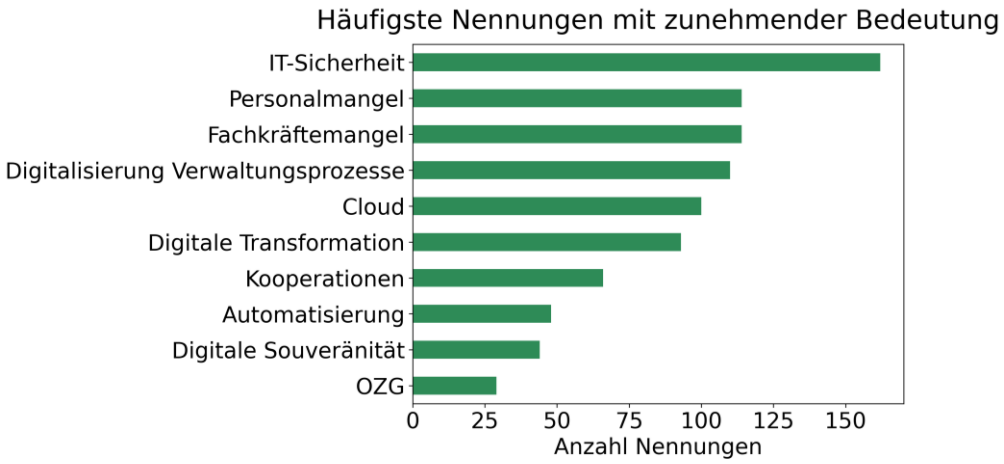


Abbildung 2: Top-Themen mit zunehmender Bedeutung sortiert nach Anzahl der Nennungen

Die Top-Themen mit der größten abnehmenden Bedeutung sind:

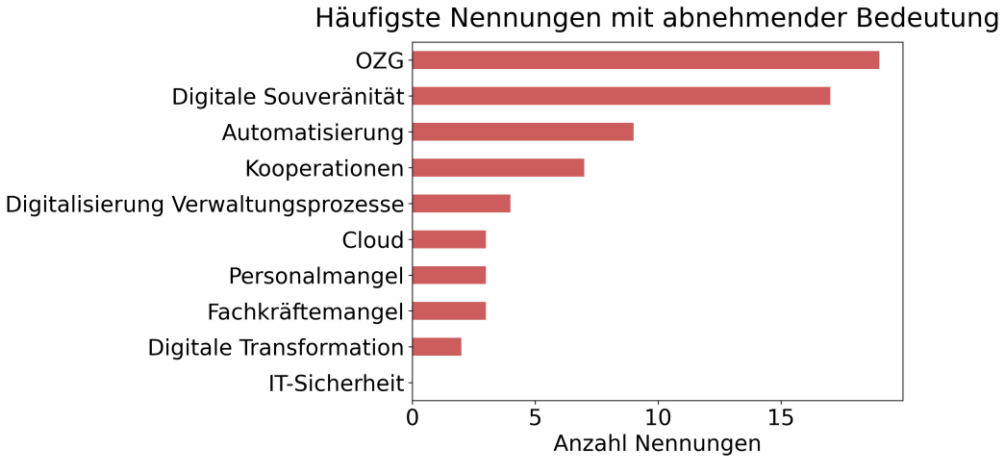
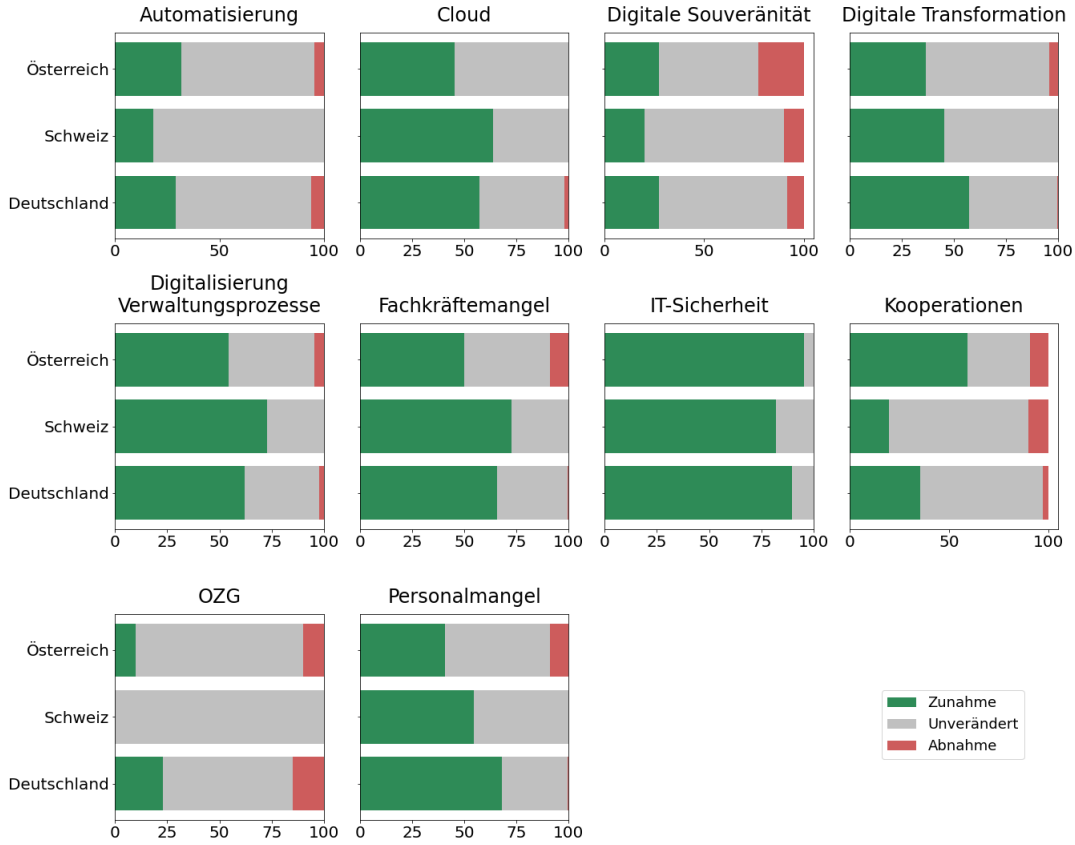


Abbildung 3: Top-Themen mit abnehmender Bedeutung sortiert nach Anzahl der Nennungen

Die folgende Darstellung illustriert die Bewertung der Veränderungen der Bedeutung im Vergleich zum letzten Jahr für die Themen mit zunehmender Bedeutung in den teilnehmenden Ländern.



Aus der folgenden Darstellung auf der Basis der Angaben von 2023 wird deutlich, wie sich die Themen zwischen 2021 und 2024 in den Platzierungen innerhalb der Top-Trends verändert haben.

Für das Jahr 2024 ergeben sich einige Mehrdeutigkeiten, da z.B. die Kategorien „Personalmangel“ und „Fachkräftemangel“ teilweise getrennt voneinander benannt wurden und z.B. Digitalisierung noch nicht so stark in die Unterbereiche „Digitalisierung allgemein“ und „Digitalisierung der Verwaltung“ unterteilt wurden.

	Platz in den relevanten Top-Trends			
Trend	**2024**	**2023**	**2022**	**2021**
IT-Sicherheit	1	1	1	2
Cloud	5	2	2	1
Digitale Transformation	4	3	5	3
Personalmangel	3	4	3	9
Digitale Souveränität		5	9	
Fachkräftemangel	3	6		
Digitalisierung Verwaltung	4	7	3	
Kooperationen	6	8		8
OZG		9		
Automatisierung	4	10		

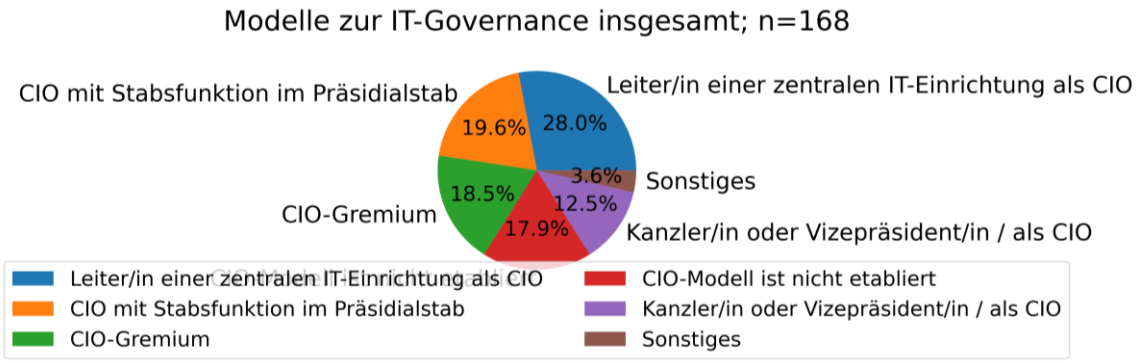
Abbildung 4: Veränderung der Top-Trends im Vergleich zu den Ergebnissen von 2021 bis 2024 sortiert nach Top-Nennungen 2023

IT-Governance

Neben der Frage nach dem Modell zur IT-Governance wurde seit 2022 auch danach gefragt, ob die Position eines Chief Digital Officers (CDO) an der Einrichtung eingerichtet ist.

Welches organisatorische Modell zur IT-Governance wird an Ihrer Hochschule oder Forschungseinrichtung eingesetzt?

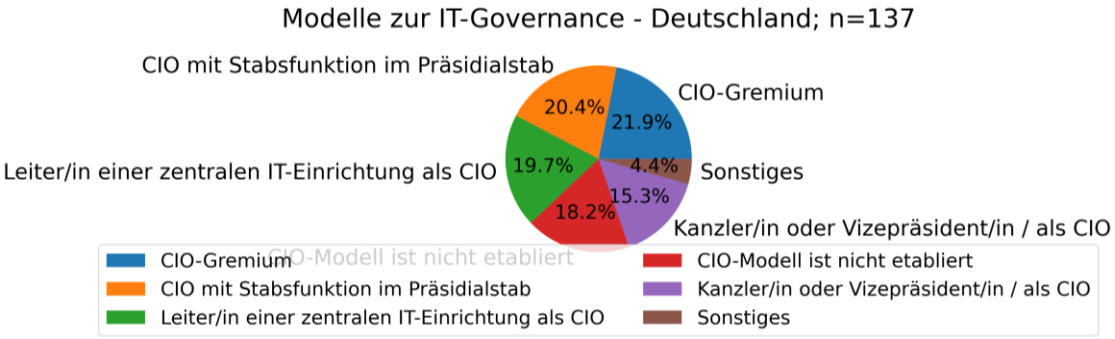
Die Verteilung für die teilnehmenden Einrichtungen im Jahr 2024 zeigt die folgende Darstellung.



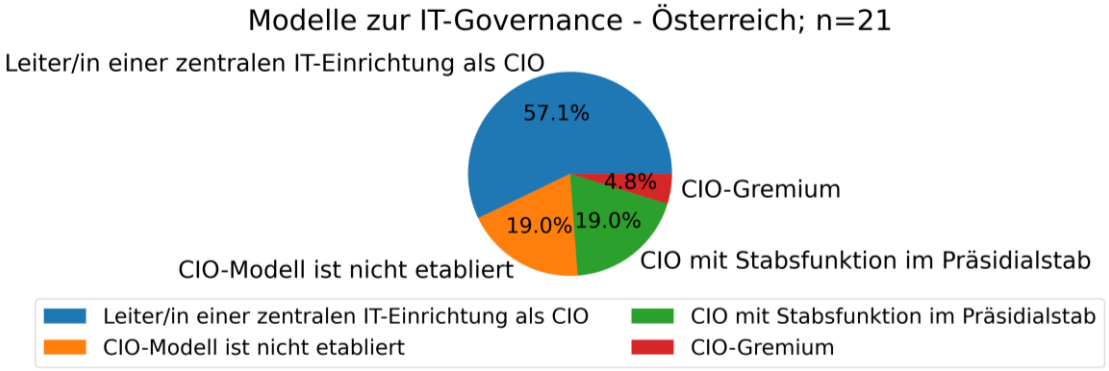
Die Tabelle zeigt die Anzahl der Nennungen.

Modell der IT-Governance	**Anzahl Nennungen**
Leiter/in einer zentralen IT-Einrichtung als CIO	47
CIO mit Stabsfunktion im Präsidialstab	33
CIO-Gremium	31
CIO-Modell ist nicht etabliert	30
Kanzler/in oder Vizepräsident/in / als CIO	21
Sonstiges	6

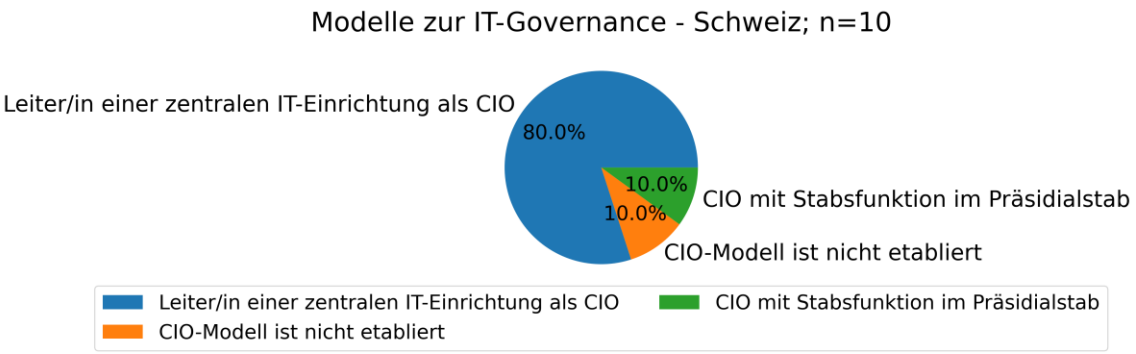
Im Folgenden werden die Verteilungen für das Modell zur IT-Governance für die einzelnen Länder der teilnehmenden Hochschulen angegeben.



Modell der IT-Governance in Deutschland	Anzahl Nennungen
CIO-Gremium	30
CIO mit Stabsfunktion im Präsidialstab	28
Leiter/in einer zentralen IT-Einrichtung als CIO	27
CIO-Modell ist nicht etabliert	25
Kanzler/in oder Vizepräsident/in / als CIO	21
Sonstiges	6

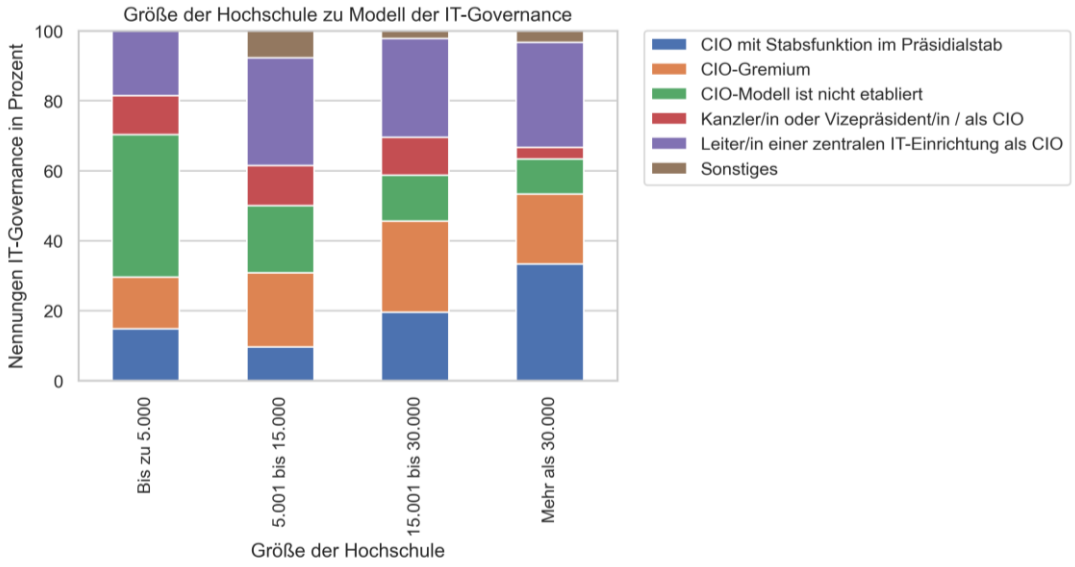


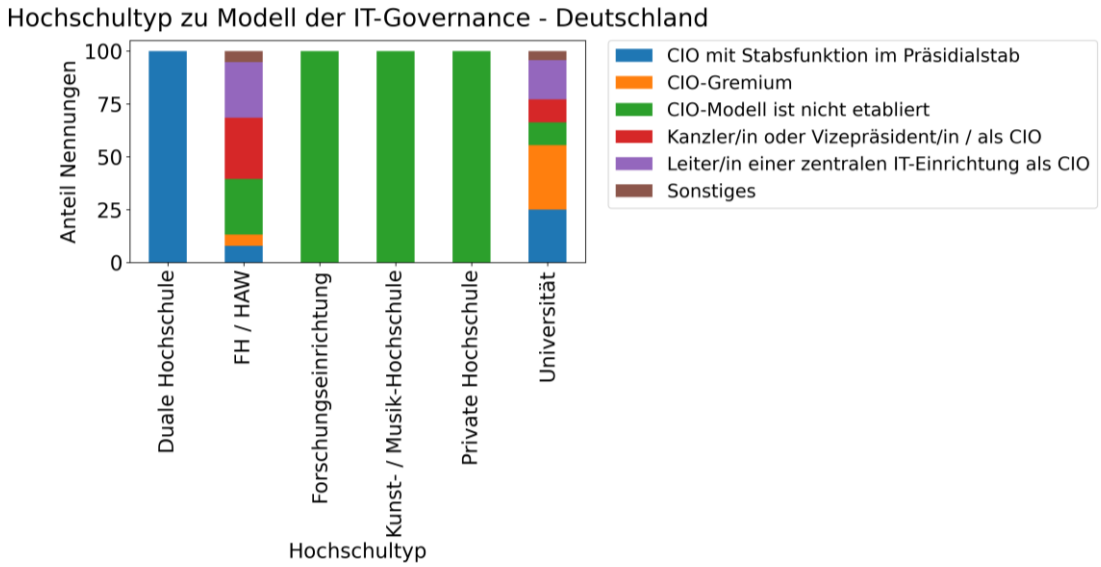
Modell der IT-Governance in Österreich	Anzahl Nennungen
Leiter/in einer zentralen IT-Einrichtung als CIO	12
CIO-Modell ist nicht etabliert	4
CIO mit Stabsfunktion im Präsidialstab	4
CIO-Gremium	1

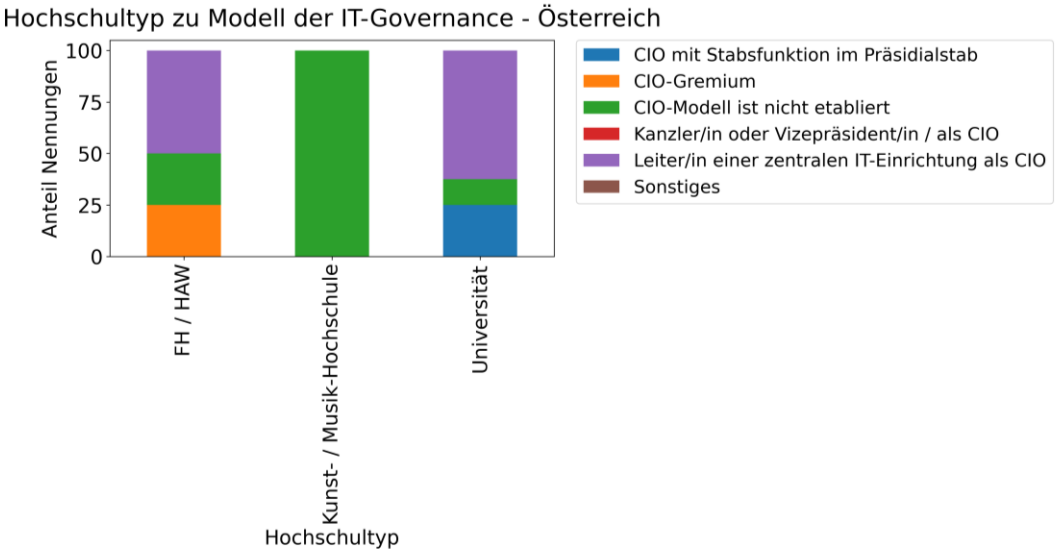


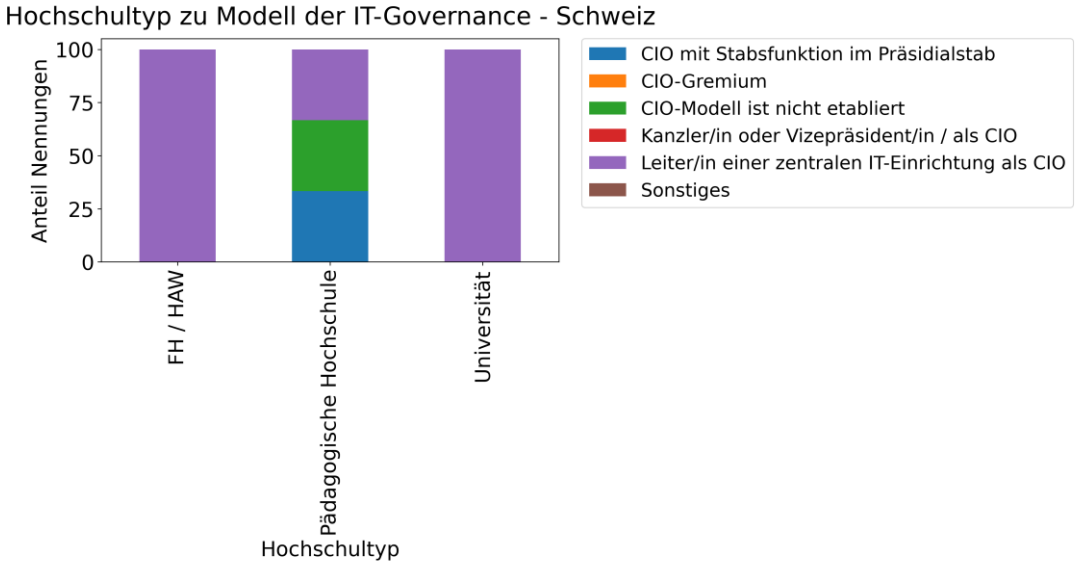
Modell der IT-Governance in Schweiz	**Anzahl Nennungen**
Leiter/in einer zentralen IT-Einrichtung als CIO	8
CIO-Modell ist nicht etabliert	1
CIO mit Stabsfunktion im Präsidialstab	1

Die folgenden Darstellungen zeigen den Einsatz von Modellen zur IT-Governance nach Typ der Hochschulen.

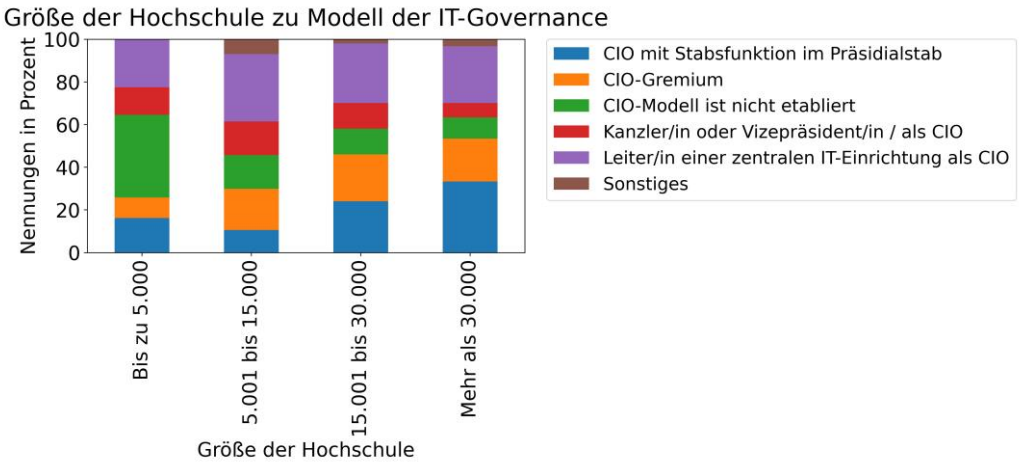


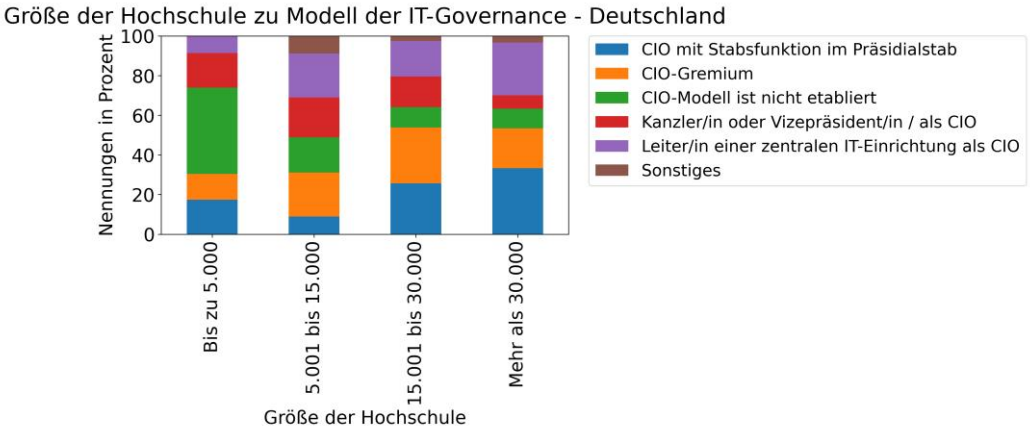


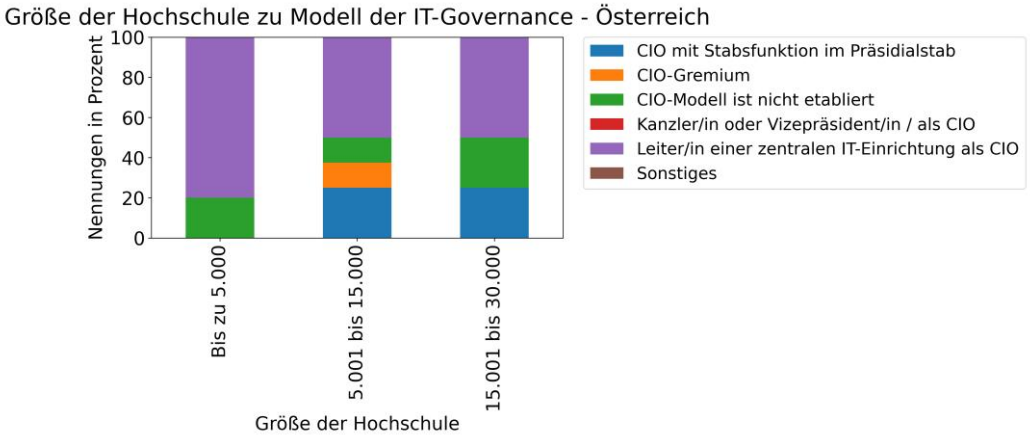

Hochschultyp zu Modell der IT-Governance - Österreich
Anteil Nennungen
100
75
50
25
0
FH / HAW
Kunst- / Musik-Hochschule
Universität
Hochschultyp
CIO mit Stabsfunktion im Präsidialstab
CIO-Gremium
CIO-Modell ist nicht etabliert
Kanzler/in oder Vizepräsident/in / als CIO
Leiter/in einer zentralen IT-Einrichtung als CIO
Sonstiges

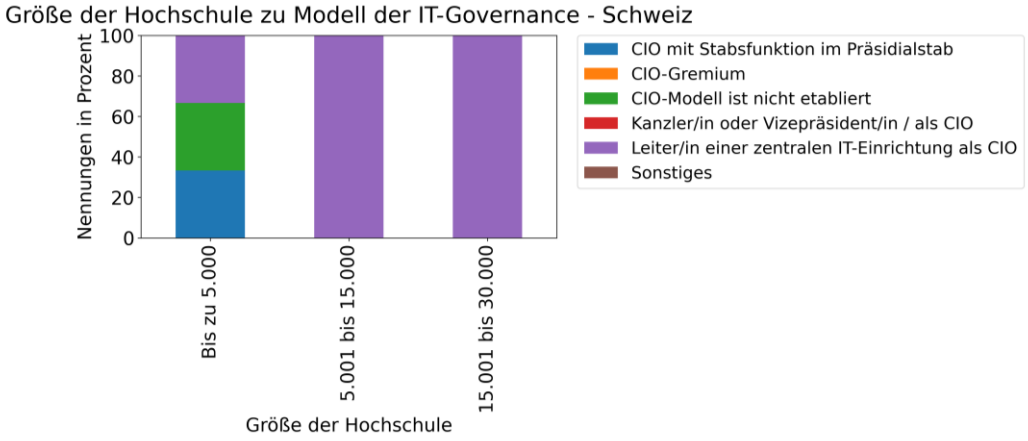

Hochschultyp zu Modell der IT-Governance - Schweiz
Anteil Nennungen
100
75
50
25
0
FH / HAW
Pädagogische Hochschule
Universität
Hochschultyp
CIO mit Stabsfunktion im Präsidialstab
CIO-Gremium
CIO-Modell ist nicht etabliert
Kanzler/in oder Vizepräsident/in / als CIO
Leiter/in einer zentralen IT-Einrichtung als CIO
Sonstiges

Die folgenden Darstellungen zeigen die Verteilung des Modells der IT-Governance nach den Größen der Hochschulen.







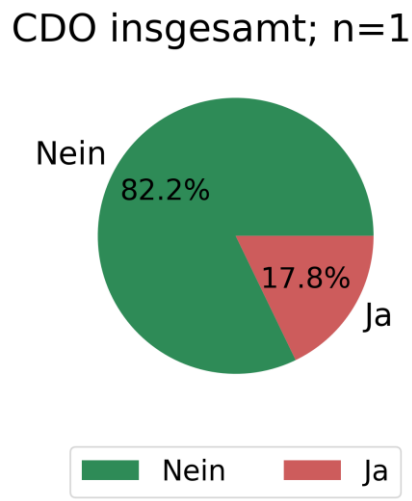

Größe der Hochschule zu Modell der IT-Governance - Schweiz
Nennungen in Prozent
100
80
60
40
20
0
Bis zu 5.000
5.001 bis 15.000
15.001 bis 30.000
Größe der Hochschule
CIO mit Stabsfunktion im Präsidialstab
CIO-Gremium
CIO-Modell ist nicht etabliert
Kanzler/in oder Vizepräsident/in / als CIO
Leiter/in einer zentralen IT-Einrichtung als CIO
Sonstiges

Gibt es an Ihrer Einrichtung die Position eines Chief Digital Officers (CDO)?

Seit dem Jahr 2022 wurde zusätzlich gefragt, ob an der eigenen Einrichtung die Position eines Chief Digital Officers (CDO) etabliert wurde. Außerhalb dieser Umfrage werden als Aufgabenbereiche von CDOs häufig die Unterstützung der Digitalen Transformation, die Entwicklung einer Digitalstrategie, die Digitalisierung von Prozessen, die Koordination unterschiedlicher Bereiche der Hochschulen und die Förderung von Digitalkompetenzen berichtet.

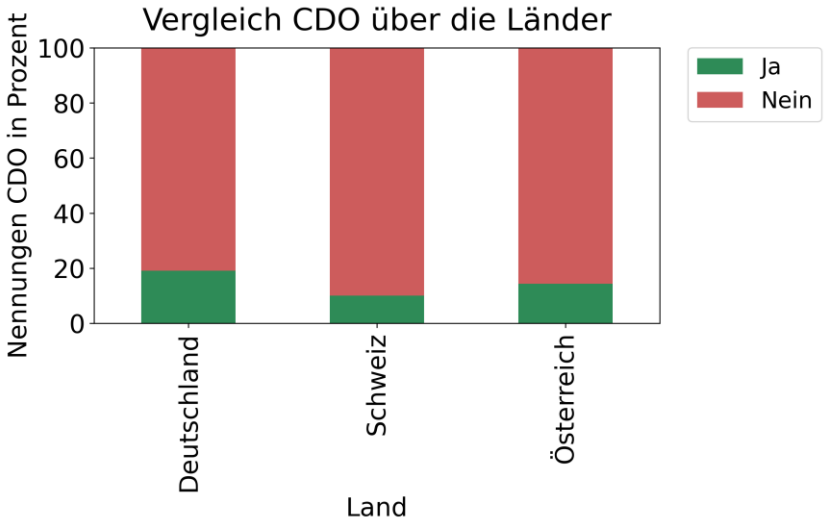
Im Vorjahr 2023 gaben 14% der Teilnehmenden an, dass diese Position an ihrer Einrichtung bereits eingerichtet wurde.

Insgesamt ist die Rolle bei über 80% der teilnehmenden Hochschulen nicht ausgeprägt.

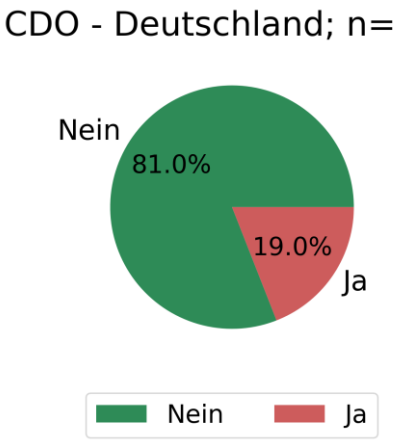


CDO	Anzahl Nennungen
Nein	129
Ja	28

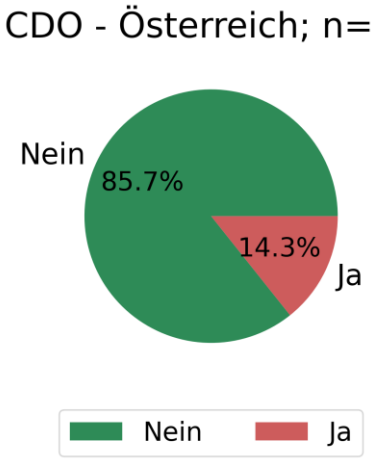
Die Verteilung über die Länder der teilnehmenden Hochschulen zeigt die folgende Darstellung.



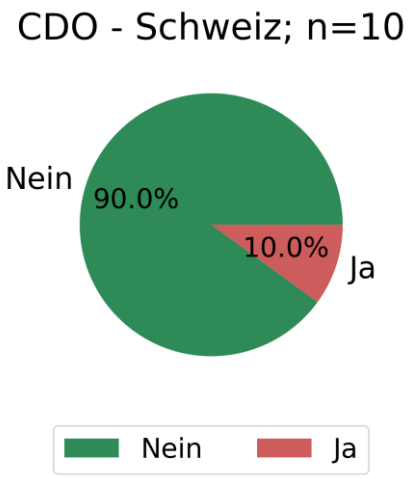
Die Angaben für die einzelnen Länder sind wie folgt.



CDO in Deutschland	Anzahl Nennungen
Nein	102
Ja	24

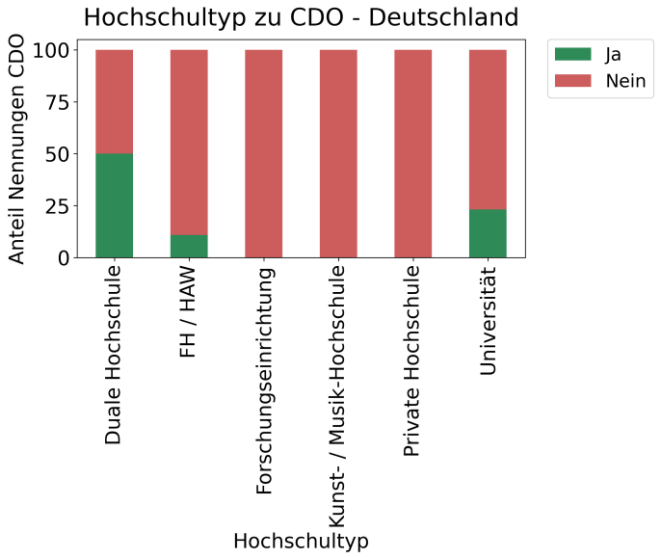


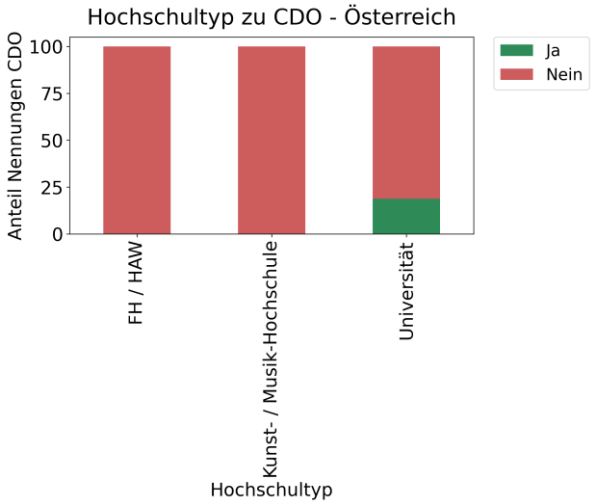
CDO in Österreich	Anzahl Nennungen
Nein	18
Ja	3

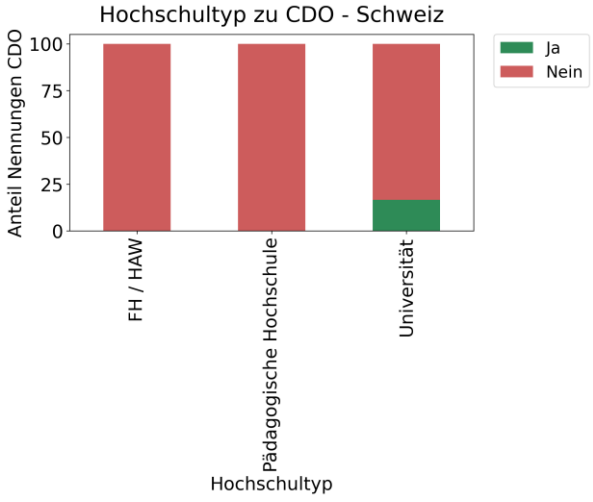


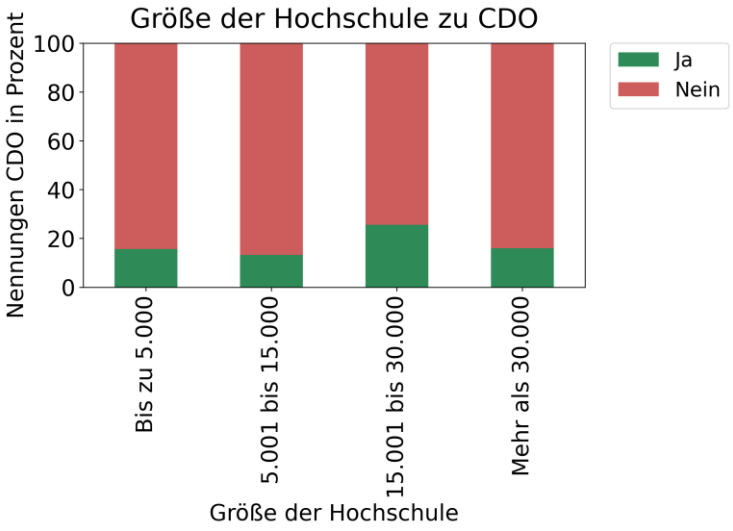
CDO in Schweiz	Anzahl Nennungen
Nein	9
Ja	1

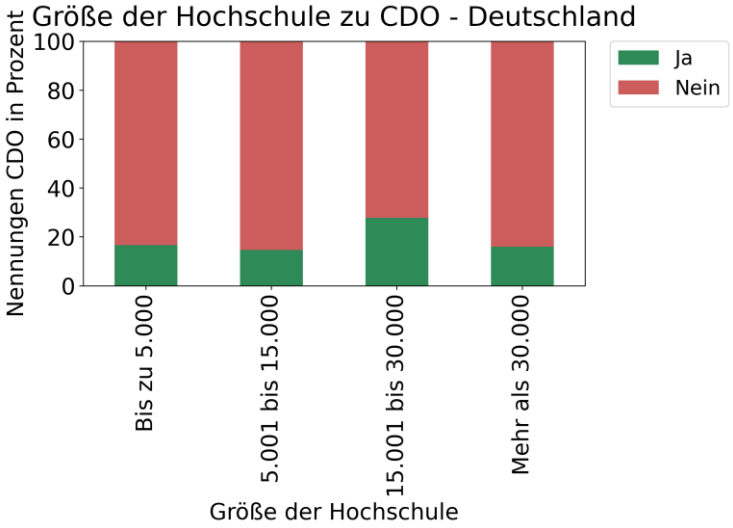
Die folgenden Darstellungen zeigen den Stand zur Einrichtung von CDOs nach Typ der Hochschulen und nach Größe der Hochschulen in den Ländern der teilnehmenden Hochschulen.

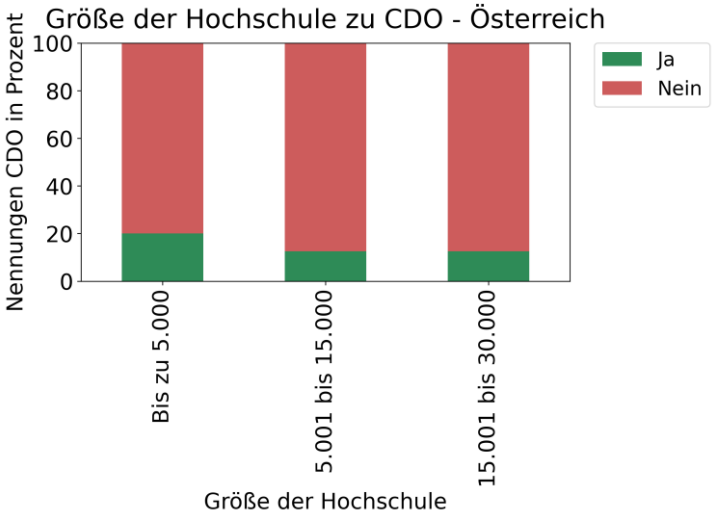


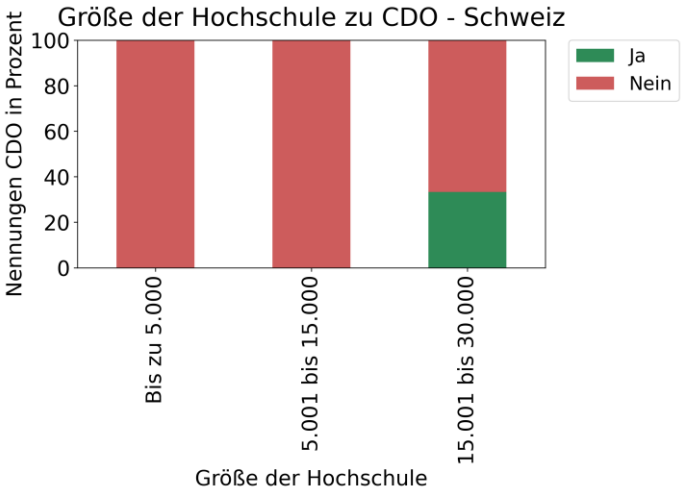





Größe der Hochschule zu CDO
Nennungen CDO in Prozent
100
80
60
40
20
0
Ja
Nein
Bis zu 5.000
5.001 bis 15.000
15.001 bis 30.000
Mehr als 30.000
Größe der Hochschule


Größe der Hochschule zu CDO - Deutschland
Nennungen CDO in Prozent
100
80
60
40
20
0
Ja
Nein
Bis zu 5.000
5.001 bis 15.000
15.001 bis 30.000
Mehr als 30.000
Größe der Hochschule


Größe der Hochschule zu CDO - Österreich
Nennungen CDO in Prozent
100
80
60
40
20
0
Ja
Nein
Bis zu 5.000
5.001 bis 15.000
15.001 bis 30.000
Größe der Hochschule

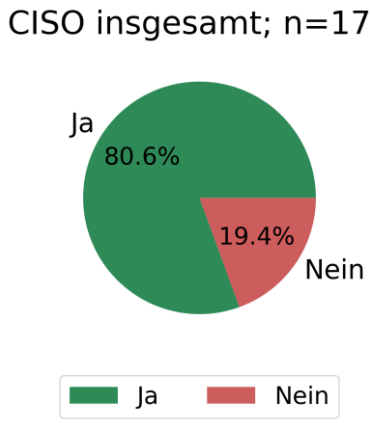

Größe der Hochschule zu CDO - Schweiz
Nennungen CDO in Prozent
100
80
60
40
20
0
Ja
Nein
Bis zu 5.000
5.001 bis 15.000
15.001 bis 30.000
Größe der Hochschule

Gibt es an Ihrer Einrichtung die Position eines Chief Information Security Officers (CISO)?

Chief Information Security Officers oder auch IT-Sicherheitsbeauftragte sind in der Regel für den Aufbau und den Betrieb des Informationssicherheitsmanagementsystems an den Hochschulen zuständig. Sie betreiben das Risikomanagement, etablieren und prüfen IT-Sicherheitsstandards, führen Schulungs- und Awarenessmaßnahmen durch, unterstützen beim Krisenmanagement und koordinieren das Zusammenwirken der unterschiedlichen Einrichtungen einer Hochschule zur IT-Sicherheit. Sie nehmen dadurch eine Schlüsselrolle für die IT-Sicherheit von Hochschulen ein.

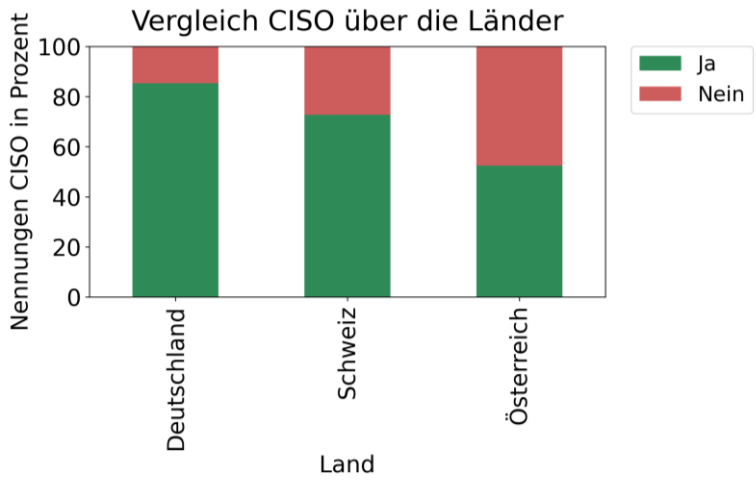
Vor diesem Hintergrund wurde in diesem Jahr die Frage zur Einrichtung einer entsprechenden Position mit aufgenommen. Bei über 80% der teilnehmenden Einrichtungen wurde eine entsprechende Position bereits geschaffen. Im Ländervergleich zeigt sich ein etwas geringerer Anteil für Österreich und die Schweiz. Wobei der Anteil mit zunehmender Größe einer Einrichtung zunimmt. Einrichtungen mit mehr als 15.000 Studierenden haben in allen Ländern fast durchgängig bereits vergleichbare Positionen eingerichtet.

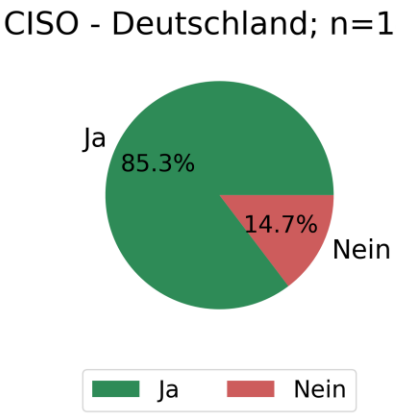
Für diese Frage gab es Antworten von 175 Teilnehmenden.



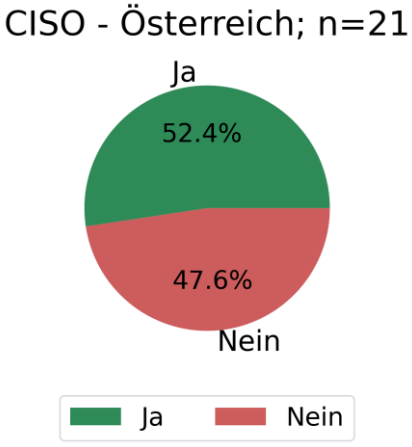
CISO	Anzahl Nennungen
Ja	141
Nein	34

Die folgenden Darstellungen bietet einen Vergleich über die teilnehmenden Länder.

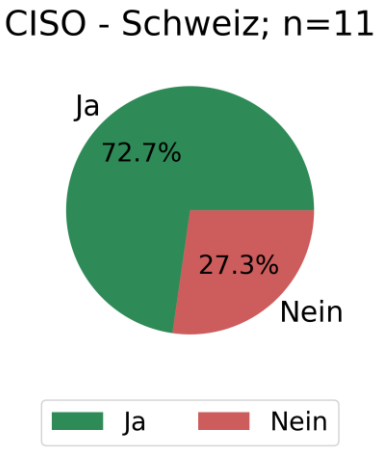




CISO in Deutschland	Anzahl Nennungen
Ja	122
Nein	21

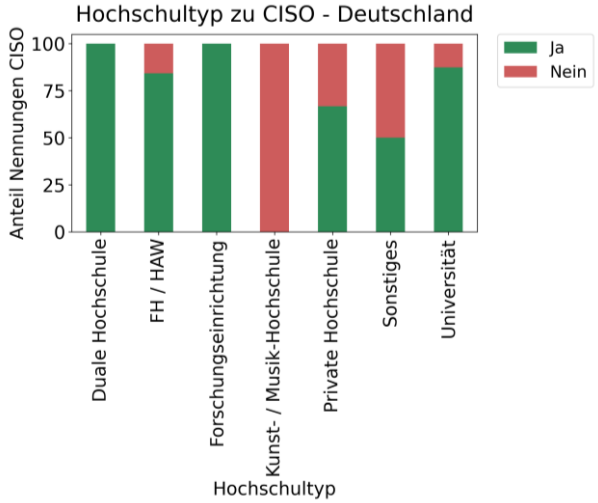


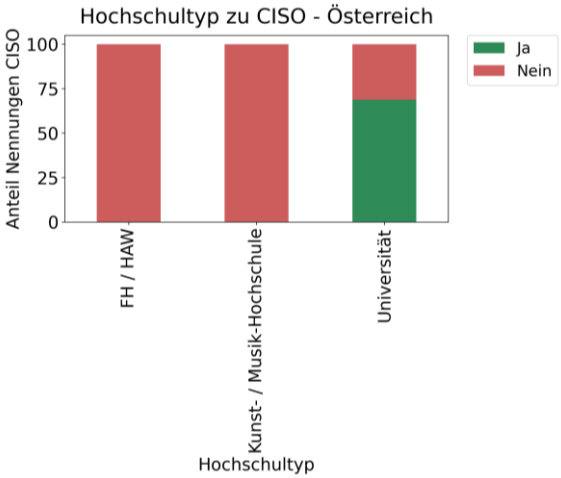
CISO in Österreich	Anzahl Nennungen
Ja	11
Nein	10

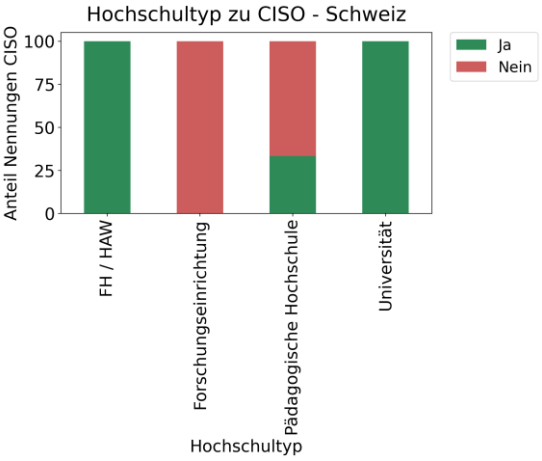


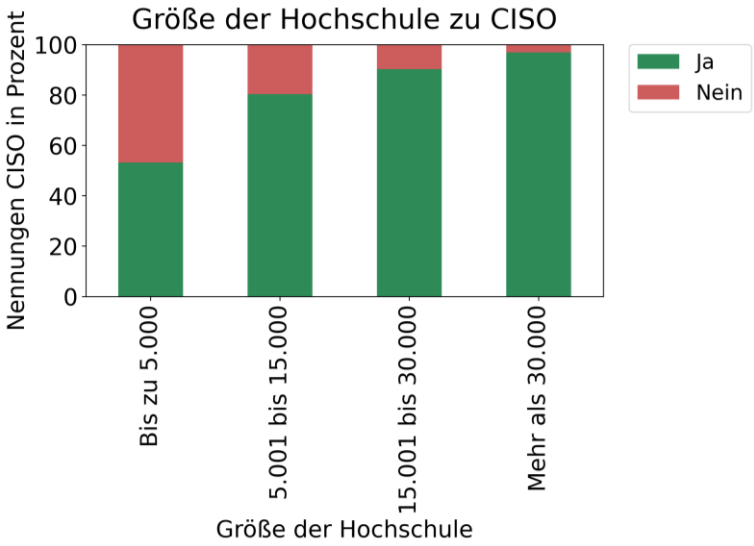
CISO in Schweiz	Anzahl Nennungen
Ja	8
Nein	3

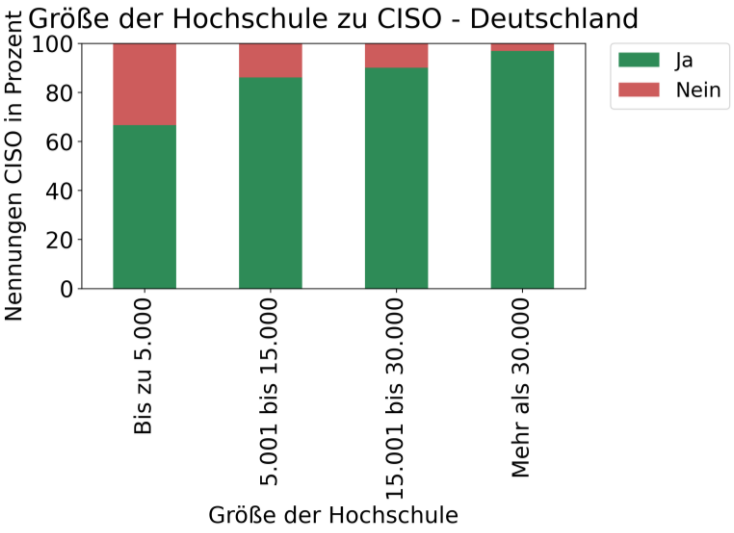
Die folgenden Darstellungen geben die Antworten zur Einrichtung einer CISO-Rolle in Bezug auf den Typ und die Größe der Hochschule wieder.

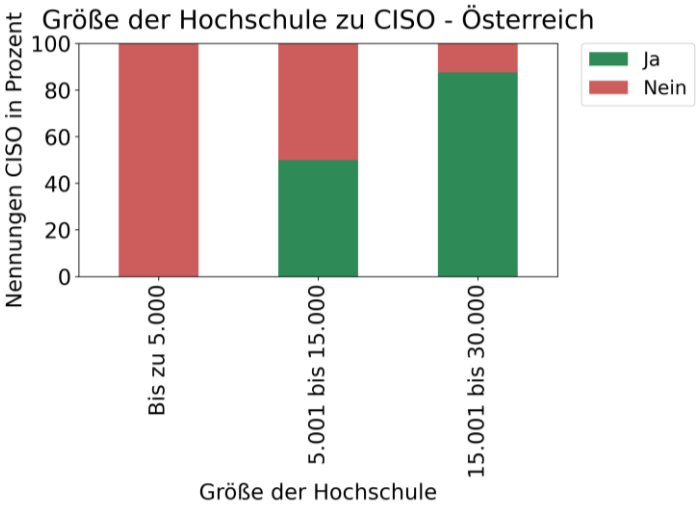


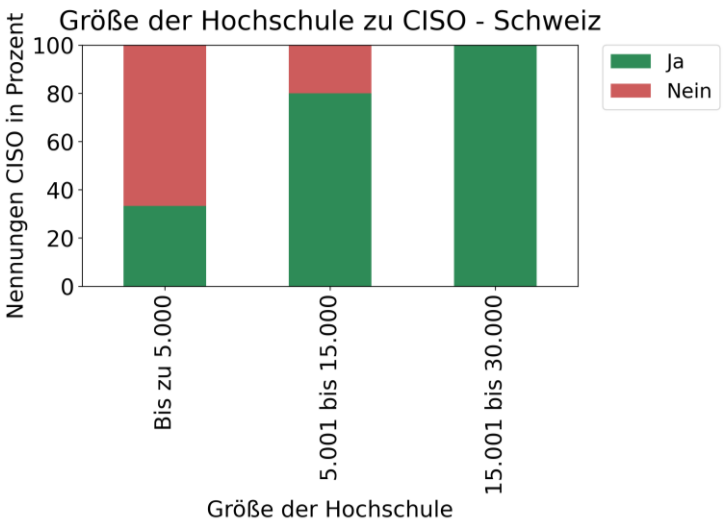





Größe der Hochschule zu CISO
Nennungen CISO in Prozent
100
80
60
40
20
0
Bis zu 5.000
5.001 bis 15.000
15.001 bis 30.000
Mehr als 30.000
Größe der Hochschule
Ja
Nein


Größe der Hochschule zu CISO - Deutschland
Nennungen CISO in Prozent
100
80
60
40
20
0
Bis zu 5.000
5.001 bis 15.000
15.001 bis 30.000
Mehr als 30.000
Größe der Hochschule
Ja
Nein


Größe der Hochschule zu CISO - Österreich
Nennungen CISO in Prozent
100
80
60
40
20
0
Bis zu 5.000
5.001 bis 15.000
15.001 bis 30.000
Größe der Hochschule
Ja
Nein


Größe der Hochschule zu CISO - Schweiz
Nennungen CISO in Prozent
100
80
60
40
20
0
Ja
Nein
Bis zu 5.000
5.001 bis 15.000
15.001 bis 30.000
Größe der Hochschule

Ergebnisse der Kernumfrage

In jedem Jahr werden zwölf gleichbleibende Fragen in der Umfrage gestellt, die als Freitext beantwortet werden. Die Antworttexte wurden normalisiert und es wurden Kategorien aus den Antworten abgeleitet. Teilweise wurden dabei Teile von besonders häufig genannten Aspekten in die Beschreibung der Kategorie integriert. Dann wurde die Anzahl der Nennungen für die Kategorien gezählt.

Welche Top-Trends sehen Sie allgemein im IT-Bereich?

Es haben 92 Teilnehmende bis zu 5 Antworten für diese Frage angegeben. Auf die Kategorien zugeordnet ergeben sich die folgenden Häufigkeiten.

Kategorie	**Anzahl**
Künstliche Intelligenz (KI) und Maschinelles Lernen (ML)	61
Cloud-Technologien und Infrastruktur	56
IT-Sicherheit	51
Cybersicherheit	38
Digitalisierung und Automatisierung	22
Personalmangel und Fachkräftemangel	21
Digitale Souveränität und Unabhängigkeit	19
Kooperation und Vernetzung	7
Nachhaltigkeit und Green IT	5
Personalmanagement	2

Die allgemeinen Top-Trends mit mindestens zwei Nennungen lassen sich in die folgenden Kategorien einteilen.

Künstliche Intelligenz (KI) und Maschinelles Lernen (ML): Diese Kategorie umfasst alle Nennungen, die sich auf KI/AI/ML beziehen, einschließlich des Einsatzes von KI-Tools, der Integration von KI in verschiedene Bereiche wie Lehre, Verwaltung und Support sowie der Nutzung von KI für Entscheidungsunterstützung.

Cloud-Technologien und Infrastruktur: Diese Kategorie umfasst alle Nennungen, die sich auf Cloud-Technologien beziehen, einschließlich der Nutzung von Cloud-Diensten, der Migration von Software und Systemen in die Cloud, der Optimierung von Cloud-Lösungen und der Zusammenarbeit mit großen Cloud-Providern.

IT-Sicherheit: Diese Kategorie umfasst alle Nennungen, die sich auf IT-Sicherheit beziehen, einschließlich der Implementierung von Sicherheitsmaßnahmen, der Verbesserung der IT-Sicherheit, der Sicherstellung der Compliance und der Förderung von Sicherheitsbewusstsein.

Cybersicherheit: Diese Kategorie umfasst alle Nennungen, die sich auf Cybersecurity beziehen, einschließlich des Schutzes vor Cyberangriffen und der Vorbereitung auf Sicherheitsvorfälle.

Digitalisierung und Automatisierung: Diese Kategorie umfasst alle Nennungen, die sich auf Automatisierung beziehen, einschließlich der Nutzung von KI-basierten Automatisierungswerkzeugen und der Implementierung von automatisierten Prozessen.

Personalmangel und Fachkräftemangel: Diese Kategorie umfasst alle Nennungen, die sich auf den Fachkräftemangel im IT-Bereich beziehen, einschließlich des Mangels an qualifizierten Fachkräften im Bereich IT-Sicherheit und der Herausforderungen beim Recruiting von Fachkräften.

Digitale Souveränität und Unabhängigkeit: Diese Kategorie umfasst alle Nennungen, die sich auf digitale Souveränität beziehen, einschließlich der Gewährleistung von Datensouveränität, der Einhaltung rechtlicher Vorgaben und der Implementierung von Sicherheitsmaßnahmen, um die digitale Souveränität zu gewährleisten.

Kooperation und Vernetzung: Diese Kategorie umfasst alle Nennungen, die sich auf Zusammenarbeit mit anderen Hochschulen beziehen.

Nachhaltigkeit und Green IT: Diese Kategorie umfasst alle Nennungen, die sich auf nachhaltige IT-Maßnahmen beziehen, einschließlich des effizienteren Betriebs von Rechenzentren, der Nutzung von energieeffizienten Technologien und der Förderung von Nachhaltigkeitsaspekten.

Personalmanagement: Diese Kategorie umfasst alle Nennungen, die sich auf Personalmanagement beziehen, einschließlich der Herausforderungen beim Thema Gehalt und der Einführung von flexiblen und zeitgemäßen Arbeitsweisen.

Welche Top-Trends sind für Sie besonders relevant?

92 Hochschulen haben für diese Frage bis zu 5 Antworten gegeben. Verteilt auf die Kategorien ergibt sich dabei das folgende Ergebnis. Die Angaben sind überwiegend identisch zwischen den Ländern und es zeigen sich nur kleinere Unterschiede in den Platzierungen. Lediglich der Bereich Cloud-Dienste und Cloud-Technologien wird in Österreich in geringerem Umfang genannt.

Kategorie	**Anzahl**
IT- und Cybersicherheit	41
Künstliche Intelligenz (KI) und Maschinelles Lernen (ML)	34
Personalmangel und Fachkräftemangel	24
Digitalisierung und Automatisierung	21
Cloud-Technologien und Infrastruktur	15
Kooperation und Vernetzung	12
Finanzierung und Wirtschaftlichkeit	12
Cyberkriminalität und Bedrohungsmanagement	12
Rechtliche Aspekte und Compliance-Management	11
Neue Technologien und Innovationen	10
Digitale Souveränität und Unabhängigkeit	10
Nachhaltigkeit und Green IT	9
Bildung und Forschung im digitalen Zeitalter	9
Moderne Arbeitsformen und Organisationsmodelle	7
Langzeitarchivierung und Datenmanagement	6

Für Österreich mit 15 teilnehmenden Hochschulen bei dieser Frage ergeben sich die folgenden Häufigkeiten.

Kategorie	**Anzahl**
IT- und Cybersicherheit	9
Künstliche Intelligenz (KI) und Maschinelles Lernen (ML)	5
Personalmangel und Fachkräftemangel	3
Cyberkriminalität und Bedrohungsmanagement	3
Digitalisierung und Automatisierung	2
Rechtliche Aspekte und Compliance-Management	2
Digitale Souveränität und Unabhängigkeit	2

Für die Schweiz ergeben sich bei 11 teilnehmenden Hochschulen zu dieser Frage die folgenden Ergebnisse.

Kategorie	**Anzahl**
Künstliche Intelligenz (KI) und Maschinelles Lernen (ML)	8
IT- und Cybersicherheit	7
Cloud-Technologien und Infrastruktur	4
Personalmangel und Fachkräftemangel	4
Digitalisierung und Automatisierung	2
Cyberkriminalität und Bedrohungsmanagement	2
Moderne Arbeitsformen und Organisationsmodelle	2

Die relevanten Top-Trends für 2024 lassen sich in die folgenden Kategorien gliedern.

IT- und Cybersicherheit: Diese Kategorie umfasst Themen rund um die Sicherheit von Informationstechnologien, den Schutz vor Cyberangriffen und allgemeine Datensicherheitsmaßnahmen.

Künstliche Intelligenz (KI) und Maschinelles Lernen (ML): Diese Kategorie befasst sich mit der Entwicklung und Anwendung von Algorithmen, die maschinelles Lernen und künstliche Intelligenz umfassen.

Personalmangel und Fachkräftemangel: Adressiert den Mangel an qualifizierten Fachkräften, insbesondere im IT-Bereich, und die Herausforderungen bei der Personalakquise.

Digitalisierung und Automatisierung: Fokussiert auf die Umstellung von manuellen auf digitale Prozesse, die Nutzung digitaler Technologien zur Effizienzsteigerung und die Automatisierung von Verwaltungsabläufen.

Cloud-Technologien und Infrastruktur: Bezieht sich auf die Nutzung und Verwaltung von Cloud-basierten Diensten, Speicherlösungen und Infrastrukturen.

Kooperation und Vernetzung: Betrifft die Zusammenarbeit zwischen verschiedenen Institutionen, die Vernetzung innerhalb der Bildungssektoren und die gemeinsame Nutzung von Ressourcen.

Finanzierung und Wirtschaftlichkeit: Umfasst finanzielle Herausforderungen, wie Budgetbeschränkungen und steigende Kosten im Zusammenhang mit der Digitalisierung und IT-Infrastruktur.

Cyberkriminalität und Bedrohungsmanagement: Bezieht sich auf die wachsenden Herausforderungen durch Cyberkriminalität und die Entwicklung von Strategien zum Bedrohungsmanagement.

Rechtliche Aspekte und Compliance-Management: Beinhaltet Themen rund um rechtliche Vorgaben, Datenschutzbestimmungen und die Einhaltung von Industriestandards im IT-Bereich.

Neue Technologien und Innovationen: Fokussiert auf die Einführung neuer Technologien und innovativer Lösungen im Hochschulumfeld.

Digitale Souveränität und Unabhängigkeit: Betrifft die Fähigkeit, unabhängige und selbstbestimmte Entscheidungen im digitalen Raum zu treffen.

Nachhaltigkeit und Green IT: Konzentriert sich auf die umweltfreundliche Gestaltung von IT-Systemen und die Reduzierung des ökologischen Fußabdrucks von Technologien.

Bildung und Forschung im digitalen Zeitalter: Fokussiert auf die Transformation des Bildungs- und Forschungssektors durch digitale Technologien, einschließlich neuer Lehr- und Lernmethoden.

Moderne Arbeitsformen und Organisationsmodelle: Konzentriert sich auf die Anpassung von Arbeitsweisen und Organisationsstrukturen an moderne, digitale Anforderungen.

Langzeitarchivierung und Datenmanagement: Beinhaltet Strategien zur langfristigen Datensicherung, Verwaltung großer Datenmengen und Gewährleistung der Datenintegrität.

Welche gesetzgeberischen Regelungen sehen Sie im nächsten Jahr als besonders relevant?

Es haben 68 Hochschulen bis zu 5 relevante gesetzgeberische Regelungen angegeben, die für das Jahr 2024 besonders relevant für IT-Zentren sind.

Die Antworten lassen sich in die folgenden Kategorien abbilden.

Datenschutz und Datenschutz-Regulierungen: DSGVO, Datenschutzgesetze, EU-US Data Privacy Framework, Schweizer Datenschutzgesetz.

Cybersicherheit und Informationssicherheit: NIS2, Cyber Resilience Act, NRW Hochschulvereinbarung zur Cybersicherheit, ISMS, KRITIS

Digitale Transformation und E-Government: OZG (Onlinezugangsgesetz), EGov, Digitale Amtssignatur, eIDAS. SDG

Umwelt- und Energiegesetzgebung: EEG (Erneuerbare-Energien-Gesetz), EnEfG (Energieeffizienzgesetz), Green IT-Gesetzgebung.

Arbeitsrecht und Remote-Arbeit: Arbeitsrechtliche Regelungen für Remote-Arbeit, Barrierefreiheits-stärkungsgesetz.

Hochschul- und Bildungsregulierung: NRW Hochschuldigitalverordnung, Entscheidungen zur Finanzierung von Universitäten.

KI-Regulierung: KI-Act, Umgang mit KI bei der Arbeit.

Compliance und Standards: ISO 9001, Cloud Act.

Internationale Handels- und Datenschutzabkommen: Datenschutzabkommen EU/USA, Lieferkettengesetze, Sanktionslisten.

Öffentliches Beschaffungswesen: Vergaberecht, öffentliches Beschaffungswesen, verschärfte Bestimmungen der öffentlichen Beschaffung.

Steuerrecht: Umsatzsteuergesetz, Mehrwertsteuerpflicht

Barrierefreiheit und Inklusion: Barrierefreiheit

Die eindeutigen Nennungen dabei sind:

- Angemessenheitsbeschluss (Data Privacy Framework)
- Arbeitsrechtliche Regelungen für Remote-Arbeit
- Artificial Intelligence Act - AI Act
- Barrierefreiheit
- Barrierefreiheitsstärkungsgesetz für Websites ab 2025
- BüPF
- Cloud Act
- Cyber Resiliance Act (CRA)
- Datenschutz und Datenschutz-Grundverordnung (DSGVO)
- Datenschutzabkommen EU/USA
- Digital Services Act (DSA)
- Digitale (Amts-)Signaturen
- Effizienter und ökologischer Serverraum-Betrieb
- E-Government-Gesetz (eGovG)
- Electronic Identification, Authentication and Trust Services (eIDAS)
- Energieeffizienzgesetz (EnEfG)
- Environmental, Social und Governance (ESG)
- Erneuerbare-Energien-Gesetz (EEG 2023)
- Geodatenzugangsgesetz (GeoZG)
- ID Austria
- ISO 9001
- Kritische Infrastrukturen - KRITIS
- Lieferkettengesetz
- Nachfolge Safe Harbour Abkommen
- Neues kantonales Datenschutzgesetz (im 2025)
- Onlinezugangsgesetz (OZG)
- Reformation Vergabegesetz
- Registermodernisierungsgesetz (Regmog)
- Sanktionslisten
- Schweizer Datenschutzgesetz (DSG)
- Single Digital Gateway Verordnung (SDG-VO)
- The Network and Information Security (NIS2) Directive - NIS-2-Richtlinie
- Umgang mit KI bei der Arbeit
- Umsatzsteuer für Forschungseinrichtungen (§ 2b UStG)
- Verarbeitungssystem für die Überwachung des Post- und Fernmeldeverkehrs (VVS-ÜPF)
- Verordnung zur Durchführung der Überwachung des Post- und Fernmeldeverkehrs. (VD-ÜPF)

Welche Themen bearbeiten Sie derzeit strategisch?

Die Häufigkeiten der Nennungen in Bezug auf diese Kategorien von 85 Hochschulen zeigt die folgende Tabelle.

Kategorie	Anzahl
Digitalisierung der Verwaltung	49
Digitalisierung	33
IT-Organisationsrestrukturierung	31
KI-Nutzung	26
IT- und Informationssicherheit	23
Sourcing	12
Resiliente IT-Infrastrukturen	9
BCM	8
Personalrekrutierung	6
Arbeitsrechtliche Regelungen für Remote-Arbeit	5
ECM und DMS	4

Die Antworten lassen sich in die folgenden Kategorien einteilen.

Digitalisierung der Verwaltung: Diese Kategorie umfasst Maßnahmen zur Verbesserung und Automatisierung von Verwaltungsprozessen durch den Einsatz von Technologie.

Digitalisierung: Diese allgemeine Kategorie umfasst den Übergang von analogen zu digitalen Prozessen und Systemen in verschiedenen Bereichen.

IT-Organisationsrestrukturierung: Dies bezieht sich auf Veränderungen innerhalb der IT-Abteilung, um ihre Effizienz und Leistungsfähigkeit zu verbessern.

KI-Nutzung: Diese Kategorie beinhaltet den Einsatz von Künstlicher Intelligenz (KI), um Prozesse zu optimieren, Entscheidungen zu unterstützen oder neue Funktionen zu entwickeln.

IT- und Informationssicherheit: Diese Kategorie umfasst Maßnahmen zur Absicherung der IT-Systeme und zur Gewährleistung der Vertraulichkeit und Integrität von Daten.

Sourcing: Hier geht es darum, Ressourcen und Dienstleistungen extern zu konktrahieren, um die eigene IT-Infrastruktur zu ergänzen oder zu erweitern.

Resiliente IT-Infrastrukturen: Diese Kategorie beinhaltet Maßnahmen zur Stabilisierung und Widerstandsfähigkeit der IT-Infrastruktur gegen Ausfälle oder andere Störungen.

BCM: Business Continuity Management (BCM) bezieht sich auf die Planung und Durchführung von Maßnahmen zur Wiederherstellung von Geschäftsprozessen nach Störungen oder Katastrophen.

Personalrekrutierung: Hier geht es darum, qualifiziertes Personal für die IT-Abteilung anzuwerben und zu binden.

Arbeitsrechtliche Regelungen für Remote-Arbeit: Hier geht es um rechtliche Aspekte und Vorkehrungen für das Mobile Arbeiten.

ECM und DMS: Enterprise Content Management (ECM) und Dokumenten Management Systeme beziehen sich auf die Organisation, Verwaltung und Bereitstellung von Inhalten, wie z.B. Dokumenten, Bildern und Videos.

Welche neuen Aufgaben im Bereich Management bearbeiten Sie zurzeit?

Die Anzahl der Nennungen für jede Kategorie von 63 teilnehmenden Hochschulen wird in der folgenden Tabelle dargestellt.

Kategorie	Anzahl
IT-Management und -Governance	14
Projektmanagement und -koordination	11
Strategische Ausrichtung und Planung	11
Personalentwicklung und -gewinnung	10
IT-Sicherheit und -Risikomanagement	10
IT-Organisationsstruktur und -Restrukturierung	8
Digitale Transformation und Innovation	8
IT-Infrastruktur und -Technologie	8
Agilität und Flexibilität	6
Kommunikation und Führung	5
Koordination und Zusammenarbeit	4
Kundenorientierung und -zufriedenheit	3

Die Antworten lassen sich in die folgenden Kategorien einteilen.

IT-Management und -governance: In dieser Kategorie geht es um das Management von IT-Projekten und -prozessen innerhalb einer Organisation. Es umfasst Themen wie Projektplanung, Ressourcenverwaltung, Qualitätsmanagement und Compliance mit rechtlichen und weiteren Anforderungen.

Projektmanagement und -koordination: Diese Kategorie befasst sich mit der Planung, Durchführung und Überwachung von IT-Projekten. Es geht darum, wie Projekte strukturiert und organisiert werden können, um Ziele zu erreichen und Kosten zu kontrollieren.

Strategische Ausrichtung und Planung: Diese Kategorie befasst sich mit der Entwicklung und Umsetzung einer IT-Strategie. Es geht darum, wie IT-Maßnahmen geplant und koordiniert werden können, um die strategischen Ziele zu unterstützen.

Personalentwicklung und -gewinnung: Diese Kategorie befasst sich mit dem Aufbau und der Weiterentwicklung des IT-Teams sowie der Gewinnung neuer Mitarbeitenden. Es geht darum, wie man talentierte Fachkräfte anzieht, sie weiterbildet und motiviert.

IT-Sicherheit und -Risikomanagement: In dieser Kategorie geht es um Maßnahmen zum Schutz von Daten und Systemen vor Bedrohungen und Risiken. Es umfasst Themen wie Firewalls, Verschlüsselung, Datensicherung und Sicherheitsaudits, um potenzielle Schwachstellen zu identifizieren und zu beheben.

IT-Organisationsstruktur und -Restrukturierung: Diese Kategorie befasst sich mit der Gestaltung und Umgestaltung von Organisationsstrukturen im Bereich Informationstechnologie. Es geht darum, wie IT-Abteilungen organisiert sind, welche Rollen und Verantwortlichkeiten es gibt und wie diese Strukturen angepasst oder verändert werden können.

Digitale Transformation und Innovation: Diese Kategorie beschäftigt sich mit der Nutzung digitaler Technologien zur Verbesserung von Geschäftsprozessen und zur Schaffung neuer Produkte und

Dienstleistungen. Es geht darum, wie digitale Lösungen entwickelt und implementiert werden können.

IT-Infrastruktur und -Technologie: Diese Kategorie befasst sich mit der technischen Basisinfrastruktur der Hochschulen, einschließlich Hardware, Software und Netzwerkinfrastruktur. Es geht darum, wie diese Komponenten ausgewählt, installiert und gewartet werden.

Agilität und Flexibilität: Diese Kategorie betrifft die Fähigkeit, sich schnell an verändernde Marktanforderungen anzupassen und flexibel auf neue Herausforderungen zu reagieren. Es geht darum, wie IT-Teams agil arbeiten können, um schnelle und innovative Lösungen zu entwickeln.

Kommunikation und Führung: In dieser Kategorie geht es um die effektive Kommunikation innerhalb eines Teams und die Führung von Mitarbeitenden. Es umfasst Themen wie Feedback, Konfliktlösung und Motivation, um eine positive Arbeitsatmosphäre zu schaffen und das Team zu führen.

Koordination und Zusammenarbeit: In dieser Kategorie geht es um die Zusammenarbeit und Kommunikation zwischen verschiedenen Abteilungen und Teams innerhalb einer Organisation. Es wird darauf abgezielt, effiziente Prozesse zu schaffen und sicherzustellen, dass alle Beteiligten auf dem gleichen Stand sind.

Kundenorientierung und -zufriedenheit: In dieser Kategorie stehen die Nutzenden im Mittelpunkt. Es geht darum, wie IT-Lösungen entwickelt und implementiert werden können, um die Bedürfnisse und Erwartungen der Nutzenden zu erfüllen.

In welchem Bereich werden externe Dienstleistungen wichtiger für Sie?

Es haben 78 teilnehmende Hochschulen bis zu 5 Antworten auf diese Frage gegeben. Verteilt auf die Kategorien ergeben sich die folgenden Anzahlen.

Kategorie	**Anzahl**
IT-Sicherheit	25
Datenschutz	13
Cloudservices	9
Basisdienstleistungen	9
IT-Beratung	8
IT-Infrastruktur	6
Netzwerksicherheit	6
Personalgewinnung	6
Kompetente Ansprechpartner im Bereich Digitalisierung	5
Notfallplanung	5
Lehre und Medientechnik	5
Big Data	4
Markterkundung	3
Containerorchestrierung und Kubernetes	3

Die Antworten lassen sich in die folgenden Kategorien einteilen.

IT-Sicherheit: Diese Kategorie umfasst externe Dienstleistungen, die sich mit der Sicherheit von IT-Systemen befassen, wie z.B. SOC, IR, Incident Detection und Response, Forensik, IT-Consulting und Awareness-Trainings

Datenschutz: Diese Kategorie umfasst externe Dienstleistungen, die beim Schutz personenbezogener Daten helfen.

Cloudservices: Diese Kategorie bezieht sich auf externe Dienstleistungen, die im Zusammenhang mit Cloudcomputing stehen, wie z.B. Cloud-Dienste, Managed Services und Cloud-basierte Lösungen.

Basisdienstleistungen: Diese Kategorie beinhaltet externe Dienstleistungen, die allgemeine IT-Funktionen abdecken, wie z.B. E-Mail, Printing usw.

IT-Beratung: Diese Kategorie umfasst externe Dienstleistungen, die bei der Beratung und Planung von IT-Projekten helfen, wie z.B. IT-Beratung und Consulting.

IT-Infrastruktur: Diese Kategorie umfasst externe Dienstleistungen, die bei der Wartung und Verwaltung der IT-Infrastruktur von Hochschulen helfen, wie z.B. Network-Operations und IT-Infrastruktur-Management.

Netzwerksicherheit: Diese Kategorie umfasst externe Dienstleistungen, die bei der Absicherung und Wartung der Sicherheit von Netzwerken behilflich sind.

Personalgewinnung: Diese Kategorie bezieht sich auf externe Dienstleistungen, die bei der Rekrutierung und Gewinnung von IT-Fachkräften helfen, wie z.B. Personalgewinnung und Recruiting.

Kompetente Ansprechpartner im Bereich Digitalisierung: Diese Kategorie umfasst externe Dienstleistungen, die bei der Digitalisierung unterstützen, wie z.B. Beratung, Datenanalysen oder Projektmanagement.

Notfallplanung: Diese Kategorie bezieht sich auf externe Dienstleistungen, die bei Notfällen und Ausfällen von IT-Systemen helfen, wie z.B. Notfallplanung und -unterstützung.

Lehre und Medientechnik: Diese Kategorie bezieht sich auf externe Dienstleistungen im Bereich Lehre, wie Learning Management Systeme, Video-Konferenzfunktionen oder z.B. Videokonferenzsysteme.

Big Data: Diese Kategorie bezieht sich auf externe Dienstleistungen, die bei der Verwaltung und Analyse großer Datenmengen helfen.

Markterkundung: Diese Kategorie bezieht sich auf externe Dienstleistungen, die bei der Beschaffung von IT-Produkten und -Dienstleistungen helfen, wie z.B. Outsourcing und Markterkundung für neue Softwareprodukte.

Containerorchestrierung: Externe Dienstleistungen zur Unterstützung bei der Orchestrierung von Containern und dem Deployment und Betrieb von Containerumgebungen.

In welchen Bereichen investieren Sie mehr als vorher?

Die Häufigkeiten der Antworten von 80 Hochschulen können den Kategorien wie in folgender Tabelle zugeordnet werden.

Kategorie	Anzahl
IT-Sicherheit	41
Digitalisierung	13
Aktualisierung von Hardware	10
Künstliche Intelligenz (KI)	8
Software-Lizenzen	8
Forschung und Wissenschaftliches Computing	7
Netzwerktechnik	6
Personalgewinnung und Entwicklung	6
Organisationsentwicklung	6
Governance und Compliance	5
Speicherlösungen	5
Serviceverträge	4
Campus Management Systeme	3

Für die Antworten auf diese Frage lassen sich die folgenden Kategorien angeben.

IT-Sicherheit: Dies bezieht sich auf Maßnahmen zur Absicherung von IT-Systemen und -Daten. Beispiele: „IT-Sicherheit“, „Cybersecurity“, „Firewall“

Digitalisierung: Dies bezieht sich auf den Einsatz digitaler Technologien zur Verbesserung von Prozessen und Dienstleistungen. Beispiele: „Digitalisierung“, „Digitalisierung der Prozesse“, „Automatisierung“.

Aktualisierung von Hardware: Dies bezieht sich auf die Aktualisierung veralteter Hardware, wie Computer, Server und Peripheriegeräte.

Künstliche Intelligenz (KI): Dies bezieht sich auf den Einsatz von Algorithmen und maschinellen Lernverfahren zur Analyse und Optimierung von Daten. Beispiele: „KI“, „KI Schulung/Anwendung“

Software-Lizenzen: Dies bezieht sich auf Kauf- oder Mietlizenzen für Software.

Forschung und Wissenschaftliches Computing: Dies bezieht sich auf die Bereitstellung von Ressourcen für die Durchführung von Berechnungen und Analysen. Beispiele: „GPU-Cluster“, „Rechenleistung“, „High Performance Computing“

Netzwerktechnik: Dies bezieht sich auf den Erwerb von Netzwerktechnik.

Personalgewinnung und Entwicklung: Dies bezieht sich auf Maßnahmen zur Einstellung und Weiterentwicklung des Personals in IT-Zentren.

Organisationsentwicklung: Maßnahmen zur Verbesserung der internen Strukturen und Abläufe einer Organisation.

Governance und Compliance: Richtlinien und Verfahren zur Überwachung und Kontrolle von IT-Projekten und -Maßnahmen.

Speicherlösungen: Dies bezieht sich auf den Erwerb und die Aktualisierung von Speichersystemen.

Serviceverträge: Dies bezieht sich auf Vereinbarungen zwischen den Hochschulen und externen Dienstleistern für IT-bezogene Leistungen.

Campus Management Systeme: Die Einführung und Erweiterung von Campus-Management-Systemen.

Welche Technologien werden für Sie wichtiger?

Die Antworten von 68 Hochschulen können tabellarisch wie folgt zusammengefasst werden.

Kategorie	Anzahl
Künstliche Intelligenz (KI)	44
Cloud Computing	24
Automatisierung	15
Sicherheitstechnologien und Cybersecurity	14
Containertechnologie	9
Big Data und Datenanalyse	7
Digitale Transformation	7
Energieeffizienz und grüne IT	6
Resilienz und Redundanz	5

Aus den Antworten lassen sich die folgenden Kategorien bilden.

Künstliche Intelligenz (KI): Diese Kategorie umfasst Technologien, die auf maschinellem Lernen basieren, wie KI-Modelle als Dienstleistungen, KI-Technologien im Zusammenhang mit Cybersecurity oder generative KI.

Cloud Computing: Diese Kategorie umfasst Technologien, die auf der Verwendung von Cloud-basierten Services basieren, wie SaaS, Cloud-Dienste, virtuelle Speichersysteme, private Cloud, Cloud-Management und Cloud-Dienste in Lehre und Forschung.

Automatisierung: Diese Kategorie umfasst Technologien, die darauf abzielen, Prozesse und Arbeitsabläufe automatisiert zu gestalten, wie Automatisierungstechnologien und KI-basierte Automatisierung.

Sicherheitstechnologien und Cybersecurity: Diese Kategorie umfasst Technologien, die darauf abzielen, IT-Systeme vor Bedrohungen zu schützen, wie Sicherheitstechnologien, Single Sign On, Zero Trust, Multicloud Management und Echtzeitüberwachung.

Containertechnologie: Diese Kategorie umfasst Technologien, die darauf abzielen, Anwendungen in isolierten Umgebungen zu verwalten, wie Containerisierung, Kubernetes und Container-Lösungen.

Big Data und Datenanalyse: Technologien, die darauf abzielen, große Mengen an Daten zu analysieren.

Digitale Transformation: Technologien, die darauf abzielen, Organisationen digital zu transformieren und ihre Abläufe zu optimieren, wie digitale Unterstützung von Workflows in verschiedenen Bereichen.

Energieeffizienz und grüne IT: Technologien, die darauf abzielen, den Energieverbrauch von IT-Systemen zu reduzieren und ihre Nachhaltigkeit zu verbessern.

Resilienz und Redundanz: Diese Kategorie umfasst Technologien, die darauf abzielen, IT-Systeme redundant und resilient zu gestalten, um Ausfallzeiten zu minimieren und die Leistungsfähigkeit zu steigern.

Welche neuen Dienste oder Technologien führen Sie derzeit ein?

Die Antworten von 68 Hochschulen verteilen sich in den Häufigkeiten wie folgt.

Kategorie	Anzahl
Künstliche Intelligenz (KI) und ML	17
Cloud-Technologien	14
Campus-Management und Verwaltung	12
IDM/IAM	11
Dokumenten- und Workflow-Management	11
Cybersicherheit und Datenschutz	9
Data Management und Storage	9
Microsoft 365 (M365) und MS365	8
Softwareentwicklung und -verteilung	8
Kommunikation und Kollaboration	6

Die Antworten lassen wie in folgende Kategorien fassen.

Künstliche Intelligenz (KI): Dies umfasst alles im Zusammenhang mit KI- und ML-Technologien, einschließlich Wissenssystemen mit KI-Unterstützung und GenAI.

Cloud-Technologien: Dies umfasst Technologien wie OpenStack, Cloud-Telefonie, Container/Kubernetes und den Total Cloud Approach mit Microsoft Cloud.

Campus-Management und Verwaltung: Dies bezieht sich auf Dienste zur Verwaltung von Hochschulcampus und -verwaltung, einschließlich Campus-Management-Systemen, Bewerberportalen und Gremienmanagement.

Identitäts- und Zugriffsmanagement (IDM/IAM): Dies umfasst Dienste zur Verwaltung von Benutzeridentitäten und Zugriffsrechten, wie Active Directory-Schutz, Single Sign-On (SSO) und Multi-Faktor-Authentifizierung (MFA).

Dokumenten- und Workflow-Management: Hierunter fallen Dienste zur Verwaltung von Dokumenten und Workflow-Prozessen, einschließlich Dokumentenmanagement, elektronisches Laborbuch und Formular-/Workflowmanagement und Low-Code-Plattformen

Cybersicherheit und Datenschutz: Hierzu gehören Dienste und Technologien wie Ransomware-Schutz, Endpoint Security, Next Generation Firewall und SIEM/SOC.

Data Management und Storage: Dies bezieht sich auf Dienste zur Verwaltung von Daten und Speicher, einschließlich Datenkompetenzzentren und Storage-Erweiterungen.

Microsoft 365 (M365): Dies bezieht sich auf Dienste und Technologien im Zusammenhang mit der Microsoft 365 Suite.

Softwareentwicklung und -verteilung: Hierzu gehören Dienste zur Softwareentwicklung, -verteilung und -verwaltung, einschließlich Software Defined Access und Software Asset Management.

Kommunikation und Kollaboration: Hierzu gehören Dienste wie Messenger, VoIP, Intranet/Confluence und Kollaboration-Tools.

Es gab einige sehr spezifische Antworten für diese Frage, die hier gelistet werden sollen.

Elektronisches Labormanagement: Digitale Plattform zur Erfassung, Speicherung und Verwaltung von wissenschaftlichen Daten und Protokollen.

Software Defined Access: Ein Konzept zur Definition und Verwaltung des Zugriffs auf IT-Ressourcen über Software.

Cloud-Telefonie: Telefoniesysteme, die über das Internet arbeiten und Voice over Internet Protocol (VoIP)-Technologie nutzen.

Knowledge-System mit KI-Unterstützung: Informationssysteme, die große Mengen an Wissen speichern und analysieren, um Vorhersagen zu treffen.

Automatisierte Serververwaltung: Softwaretools zur automatischen Steuerung und Verwaltung von Servern.

KI Large Language Modelle: Fortgeschrittene KI-Algorithmen zur Analyse großer Textmengen und Extraktion von Informationen.

Etablierung von OpenStack / Private Cloud: Offene Quellcode-Plattform zur Implementierung einer privaten Cloud-Infrastruktur.

KI unterstütztes Lernen: Integration von KI in Lernerfahrungen zur Personalisierung des Lernerlebens.

CEPH Clusterstorage: Softwarelösung zur Verwaltung großer Datenmengen in einem Speichercluster.

Welche Fähigkeiten möchten Sie im nächsten Jahr in Ihrer Organisation aufbauen?

Die Verteilung der Antworten von 62 Hochschulen zu dieser Frage werden in der folgenden Tabelle dargestellt.

Kategorie	Anzahl
IT-Sicherheit	10
Künstliche Intelligenz und Maschinelles Lernen	6
Digitale Transformation	5
Automatisierung	4
Cloud-Management	4
Ereignisdetektion und -reaktion	3
Agiles Projektmanagement	3
Krisenmanagement und Resilienz	3
IT-Service-Management	3
Multiprojektmanagement	2
Kommunikation und Change-Management	2
Standardisierung und Qualitätsmanagement	2

Für diese Frage lassen sich aus den Antworten die folgenden Kategorien beschreiben.

IT-Sicherheit: Schutz vor Cyberangriffen, Verbesserung der IT-Sicherheit oder Einführung von Sicherheitsmaßnahmen.

Künstliche Intelligenz und Maschinelles Lernen: Einführung und Nutzung von KI-Technologien und maschinellem Lernen.

Digitale Transformation: Entwicklung und Implementierung neuer digitaler Technologien und Prozesse, um manuelle Vorgänge zu ersetzen.

Automatisierung: Automatisierung von Prozessen und Aufgaben.

Cloud-Management: Einsatz, Verwaltung und Optimierung von Cloud-basierten Lösungen.

Ereignisdetektion und -reaktion: Frühzeitigen Erkennung und angemessenen Reaktion auf IT-Ereignisse und -vorfälle.

Agiles Projektmanagement: Anwendung agiler Methoden zur Unterstützung von Projekten im Umfeld der Digitalen Transformation.

Krisenmanagement und Resilienz: Stärkung der Widerstandsfähigkeit der Organisation gegenüber Cyberangriffen und anderen Herausforderungen.

IT-Service-Management: die Gesamtheit der Systeme und Prozesse, mit denen Organisationen die Art und Weise verbessern, wie IT genutzt wird

Multiprojektmanagement: Effektive Verwaltung von mehreren, parallellaufenden Projekten.

Kommunikation und Change-Management: Verbesserung der Kommunikationsfähigkeit und Fähigkeiten zur Umsetzung und Bewältigung von Veränderungen.

Standardisierung und Qualitätsmanagement: Vereinheitlichung von Prozessen und Standards sowie Einführung und Durchsetzung von Qualitätsstandards.

Besonders erwähnenswerte Einzelnennungen waren hierbei

MS 365: Dies bezieht sich auf den Einsatz von Microsoft 365 als Productivity-Software.

AppsAnywhere: AppsAnywhere ist eine Softwarelösung, die die Bereitstellung von Anwendungen und Software in Bildungseinrichtungen vereinfacht.

Azure-Know-how: Microsoft Azure hin, eine Cloud-Computing-Plattform von Microsoft.

Knowhow und Betrieb von Cloud-Lösungen: Dies bezieht sich auf das Wissen und die Fähigkeiten im Bereich des Betriebs von Cloud-Lösungen, unabhängig von der spezifischen Plattform.

Knowhow und Betrieb von Lowcode-Lösungen: Einführung von Low-Code-Entwicklungsplattformen, um Anwendungen schneller zu erstellen.

Zentrales MECM-Management in der Active Directory Domain: Zentrales Management von Microsoft Endpoint Configuration Manager (MECM) in einer Active Directory-Domäne.

Open-Source-Alternativen in der Virtualisierung: Einsatz von Open-Source-Virtualisierungslösungen anstelle proprietärer Produkte, um Kosten zu senken oder Flexibilität zu erhöhen.

Welche Skills der Beschäftigten werden wichtiger?

Die Antworten der 73 teilnehmenden Hochschulen für diese Frage lassen sich wie folgt in Bezug auf die Kategorien darstellen.

Kategorie	Anzahl
Kommunikations- und Kooperationsfähigkeit	16
Projektmanagement	11
Bewusstsein für IT-Sicherheit und Datenschutz	13
Flexibilität	9
Lernbereitschaft	7
Anpassungsfähigkeit an flexible Arbeitsmethoden und Organisationsformen	6
Offenheit für alles Neue	6
Digitalkompetenz	6
Datenanalysefähigkeiten	6
Kommunikationsfähigkeit in Prozessen	5
Awareness (einschließlich Projekterfolg und Orchestrierung von On-Premise- und Cloud-Diensten)	4
IT-Forensik (einschließlich Bewertung von Sicherheitsvorfällen und sicherer Konfiguration von Systemen)	4
Microsoft Lösungen (einschließlich Umgang mit Microsoft Sentinel)	3
Systemisches Denken und Schnittstellenbewusstsein	2

Für diese Frage lassen sich die Antworten zu den folgenden Kategorien fassen.

Kommunikations- und Kooperationsfähigkeit: Die Fähigkeit, effektiv mit anderen zu kommunizieren und zusammenzuarbeiten, um gemeinsame Ziele zu erreichen.

Projektmanagement: Die Fähigkeit, Projekte effektiv zu planen, zu organisieren und zu führen, um Ziele innerhalb eines festgelegten Rahmens zu erreichen.

Bewusstsein für IT-Sicherheit und Datenschutz: Das Verständnis und die Einhaltung von Maßnahmen zur Gewährleistung der IT-Sicherheit und des Datenschutzes.

Flexibilität: Die Fähigkeit, sich schnell an Veränderungen anzupassen und flexibel auf neue Anforderungen zu reagieren.

Lernbereitschaft: Die Bereitschaft, kontinuierlich zu lernen und sich weiterzuentwickeln, um aktuelle Methoden und Technologien einsetzen zu können.

Anpassungsfähigkeit an flexible Arbeitsmethoden und Organisationsformen: Die Fähigkeit, sich schnell an neue Herausforderungen anzupassen und flexibel auf Veränderungen zu reagieren.

Offenheit für alles Neue: Die Bereitschaft, neue Ideen, Technologien und Ansätze zu akzeptieren und zu erkunden.

Digitalkompetenz: Die Fähigkeit, digitale Werkzeuge und Technologien zu nutzen und zu beherrschen.

Datenanalysefähigkeiten: Die Fähigkeit, große Datenmengen zu analysieren und daraus Erkenntnisse zu gewinnen, um fundierte Entscheidungen zu treffen.

Kommunikationsfähigkeit in Prozessen: Die Fähigkeit, Informationen effektiv in Prozessen zu kommunizieren und sicherzustellen, dass alle Beteiligten über den aktuellen Stand informiert sind.

Awareness für Projekterfolg: Das Bewusstsein für die Bedeutung von Projekterfolg und die Fähigkeit, On-Premises- und Cloud-Dienste zu orchestrieren.

IT-Forensik: Das Verständnis und die Beherrschung von IT-Forensik, einschließlich der Bewertung von Sicherheitsvorfällen und der sicheren Konfiguration von Systemen.

Microsoft Lösungen: Das Verständnis und die Beherrschung von Microsoft-basierten Lösungen, einschließlich des Umgangs mit Microsoft Sentinel.

Systemisches Denken und Schnittstellenbewusstsein: Das Vermögen, komplexe Systeme zu analysieren und zu verstehen, sowie die Fähigkeit, verschiedene Aspekte miteinander zu verknüpfen.

Besonders erwähnenswerte einzelne Nennungen waren:

„Künstliche Intelligenz als Kollege“: Diese Antwort hebt hervor, wie wichtig es ist, Fähigkeiten im Umgang mit künstlicher Intelligenz zu entwickeln, um sie als einen „Kollegen“ in der Arbeit zu betrachten.

„Self Repair“: Diese Antwort deutet auf die Fähigkeit hin, Probleme eigenständig zu erkennen und zu beheben, was eine wichtige Selbstmanagementfähigkeit sein könnte.

„Cybersecurity in allen Bereichen (z.B., Secure Coding)“: Die Betonung von „Secure Coding“ zeigt, wie wichtig es ist, sicherheitsrelevante Praktiken in der Softwareentwicklung zu integrieren.

Welche Skills der Beschäftigten werden weniger wichtig?

43 Hochschulen beteiligten sich an den Antworten für diese Frage. Die Verteilung zeigt die folgende Tabelle.

Kategorie	Anzahl
Systemadministration	9
Spezialisierung	8
IT-Fachwissen	6
Softwareprogrammierung	6
Hardware	5

Die Antworten für diese Fragen lassen sich für das Jahr 2024 in die folgenden Kategorien einteilen.

Systemadministration: Hierzu gehören die Nennungen „Systemadministration“, „Klassische Systemadministration (on-premises)“ und „Altbackene Anwendungen“ weiter zu betreiben

Spezialisierung: Hierzu gehören die Nennungen „Spezialisierung auf ein Thema“, „Expertentum“ und „Tiefgehendes Expertenwissen“.

IT-Fachwissen: Diese Kategorie enthält die Nennungen „IT-Fachwissen“, „Rein technische Themen“ und „Betrieb von klassischen Servern on-premises“.

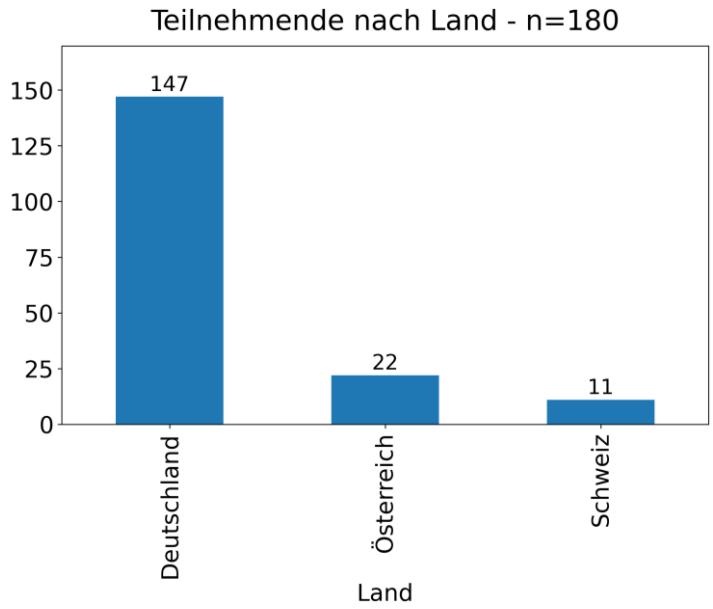
Hardware: Hierzu gehören die Nennungen „Hardware“, „Arbeit an physischer Hardware“ und „Hardwareknowledge“.

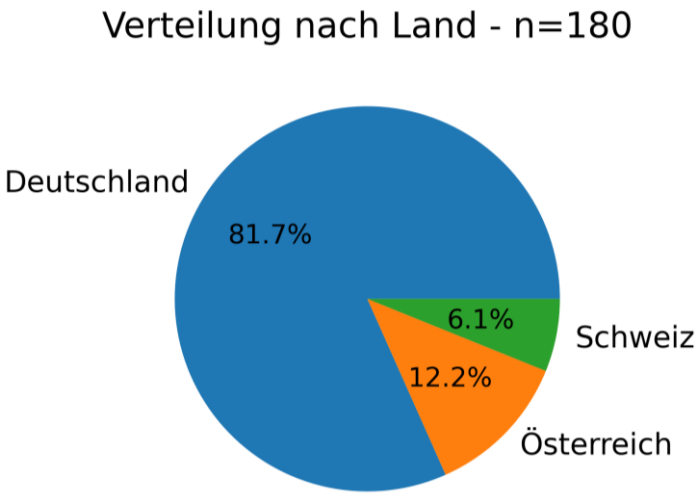
Softwareprogrammierung: Diese Kategorie umfasst die Nennungen „Programmieren“, „Softwareprogrammierung“ und „Eigenbau von PC und Servern“.

Fragen zu den teilnehmenden Einrichtungen und Personen

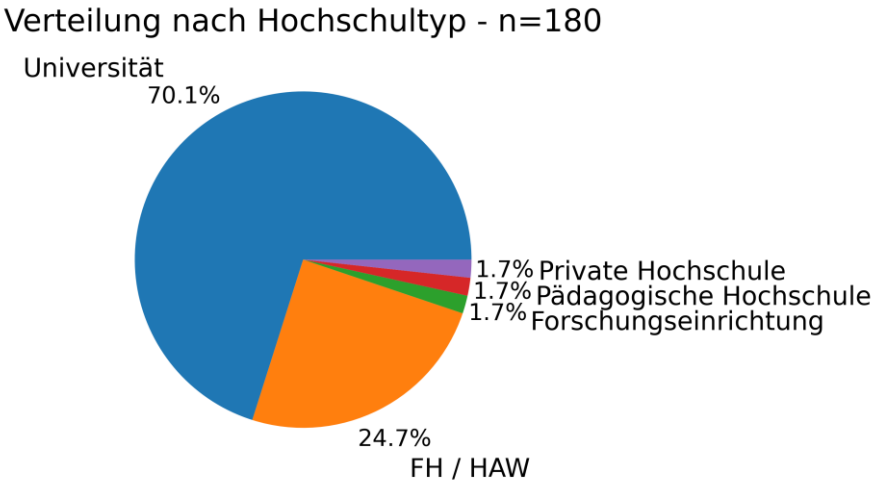
Die folgenden Darstellungen geben einen Überblick zu Typ und Größe der Einrichtungen sowie zu den Rollen der teilnehmenden Personen.

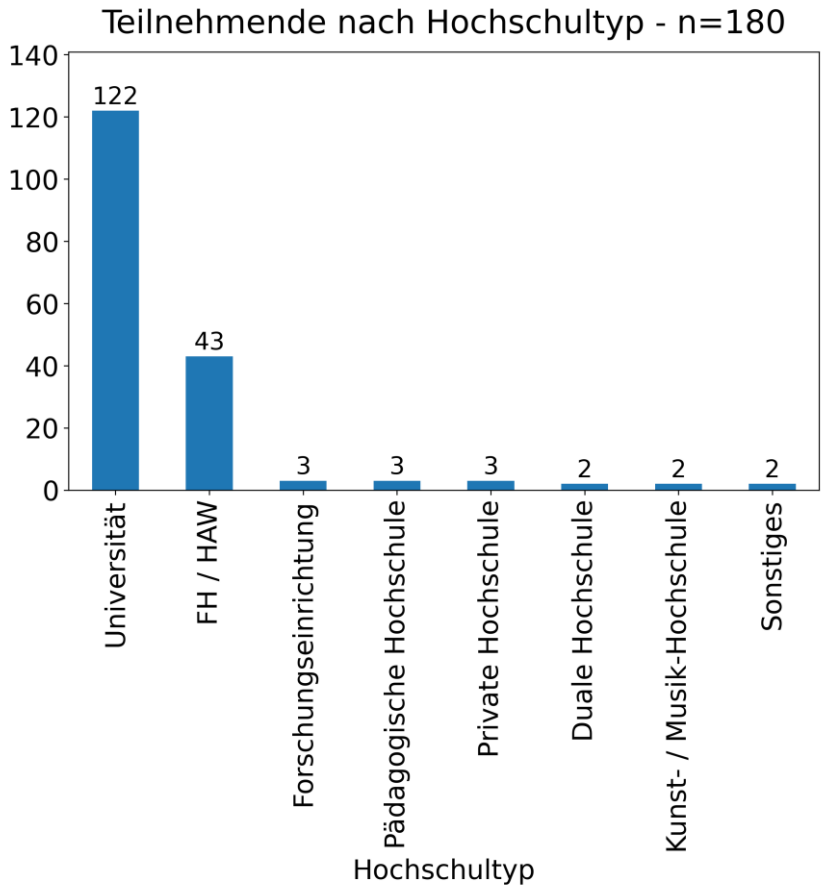
Die teilnehmenden Hochschulen verteilen sich wie folgt auf die Länder.



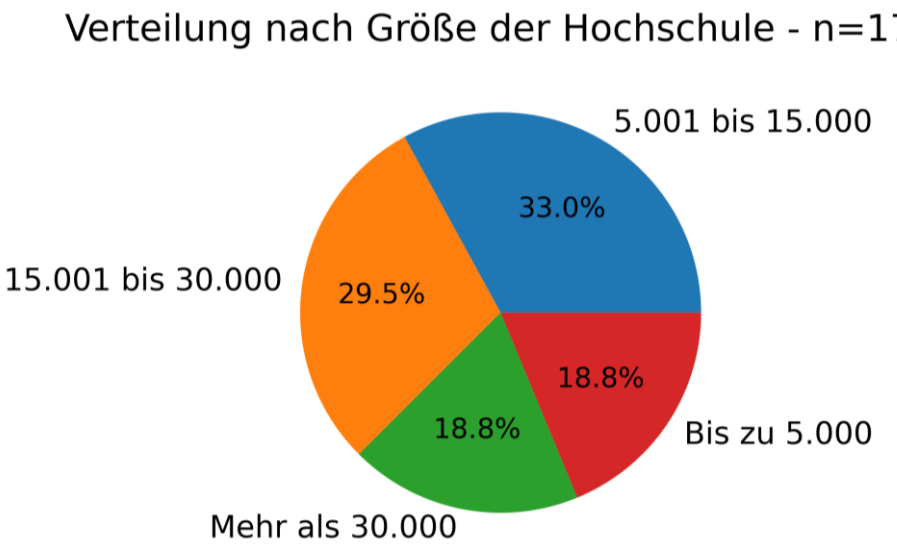


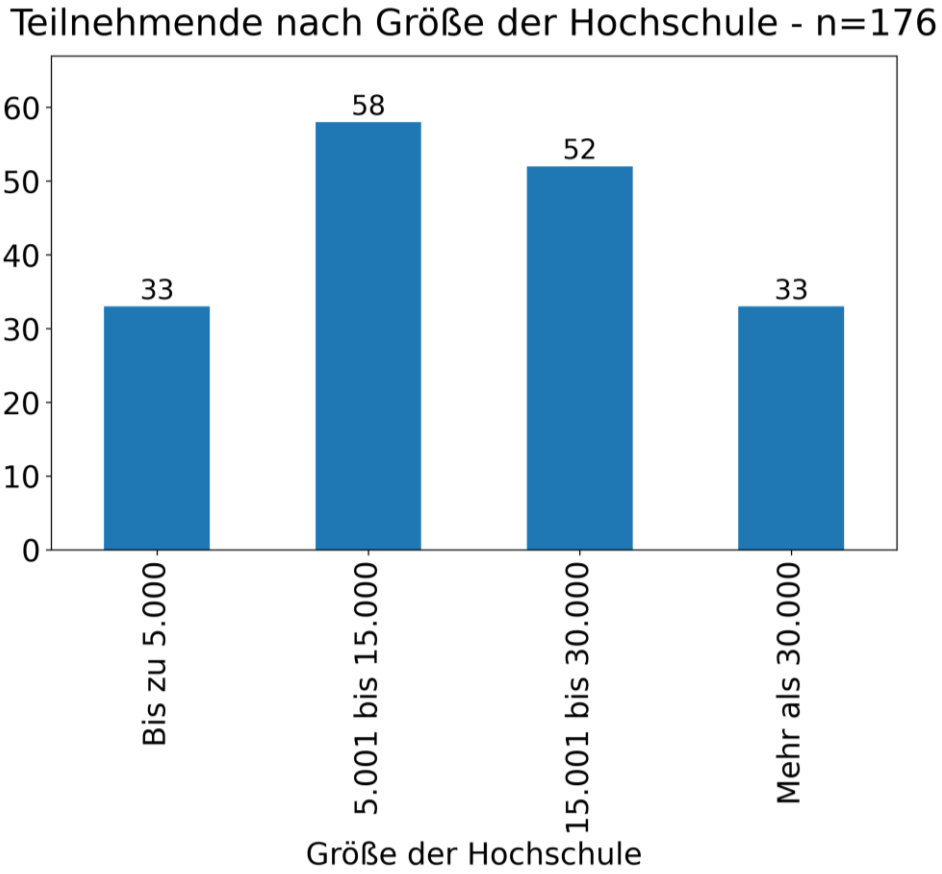
Dargestellt nach dem Typ der Hochschule ergibt sich die folgende Grafik.



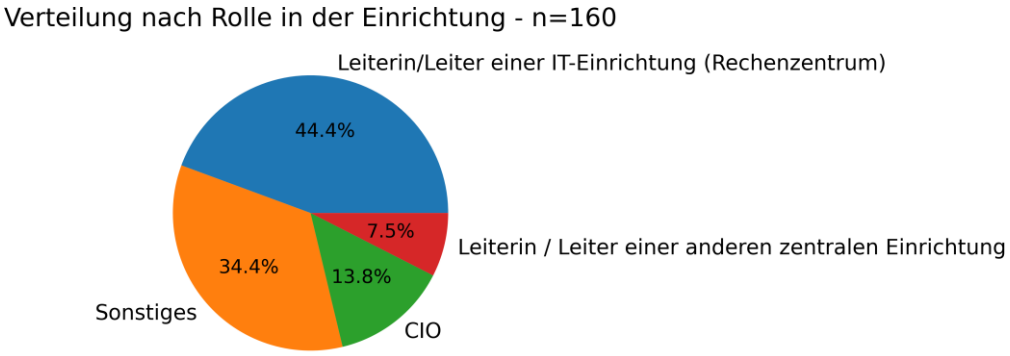


Die teilnehmenden Hochschulen verteilen sich wie folgt auf die Größen der Hochschulen.

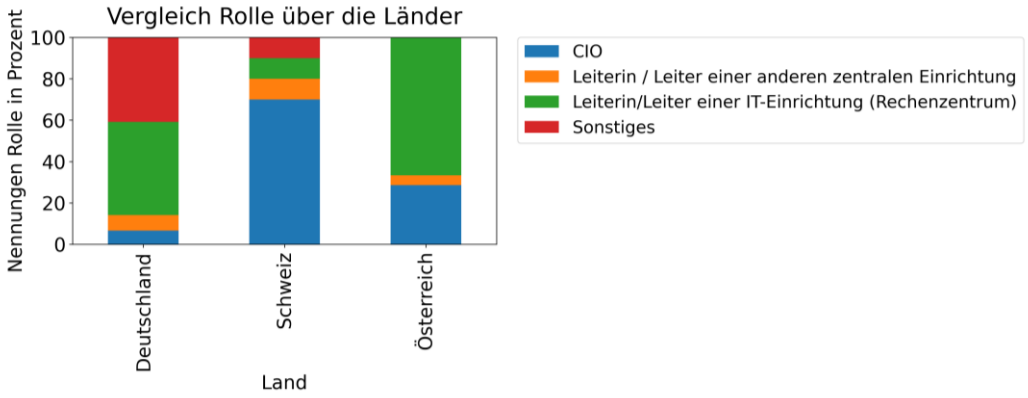

Verteilung nach Größe der Hochschule - n=176
5.001 bis 15.000
33.0%
15.001 bis 30.000
29.5%
18.8%
18.8%
Bis zu 5.000
Mehr als 30.000


Teilnehmende nach Größe der Hochschule - n=176
60
50
40
30
20
10
0
58
52
33
33
Bis zu 5.000
5.001 bis 15.000
15.001 bis 30.000
Mehr als 30.000
Größe der Hochschule

Die Rollen der teilnehmenden Personen zeigt die folgende Darstellung.

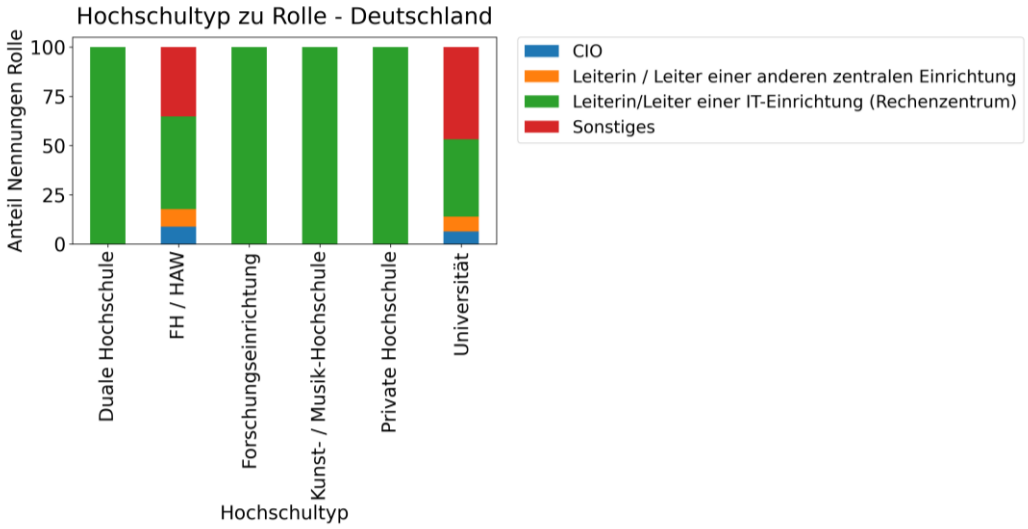


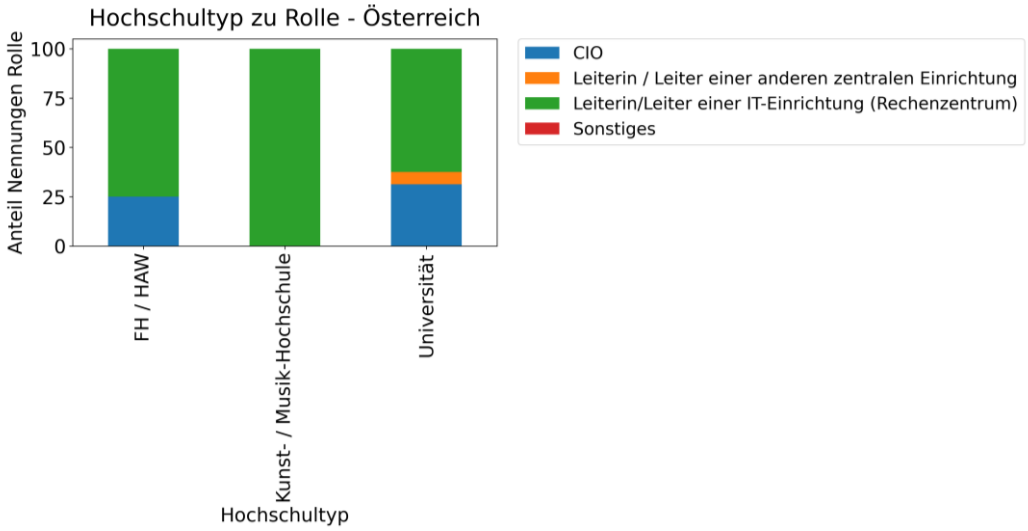
Im Folgenden werden die Rollen der teilnehmenden Person an ihrer Hochschule verteilt auf die Länder dargestellt.

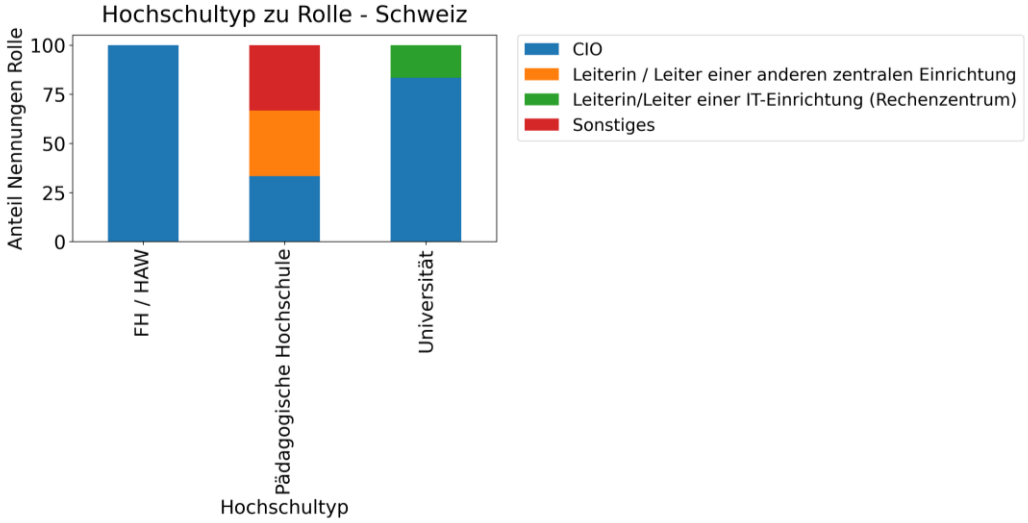


Rolle	**Anzahl Nennungen**
Leiterin/Leiter einer IT-Einrichtung (Rechenzentrum)	69
Sonstiges	50
CIO	21
Leiterin / Leiter einer anderen zentralen Einrichtung	11

Die Teilnehmenden Personen unterscheiden sich in den Ländern je nach Typ der Hochschule relativ stark, weshalb die Verteilung hier für jedes Land dargestellt werden soll.







Fragenkatalog der Umfrage

Von welchem Hochschultyp oder welcher Art Forschungseinrichtung kommen Sie?

Bitte wählen Sie eine der folgenden Antworten:

- Universität
- Hochschule für angewandte Wissenschaften
- Kunst- / Musik-Hochschule
- Pädagogische Hochschule
- Kirchliche Hochschule
- Duale Hochschule
- Staatlich anerkannte private Hochschule
- Forschungseinrichtung
- Sonstiges

Welche Rolle haben Sie in der Organisation?

Bitte wählen Sie eine der folgenden Antworten:

- CIO
- Leiterin/Leiter einer IT-Einrichtung (Rechenzentrum)
- Leiterin / Leiter einer anderen zentralen Einrichtung
- Sonstiges

In welchem Land befindet sich Ihre Einrichtung?

Bitte wählen Sie eine der folgenden Antworten:

- Deutschland
- Österreich
- Schweiz

Wie viele Studierende hat Ihre Hochschule?

Bitte wählen Sie eine der folgenden Antworten:

- Bis zu 5.000
- 5.001 bis 15.000
- 15.001 bis 30.000
- Mehr als 30.000

Governance-Modell

Welches organisatorische Modell zur IT-Governance wird an Ihrer Hochschule oder Forschungseinrichtung eingesetzt?

Bitte wählen Sie eine der folgenden Antworten:

- CIO mit Stabsfunktion im Präsidialstab
- Leiter/in einer zentralen IT-Einrichtung als CIO
- CIO-Gremium
- CIO-Modell ist nicht etabliert
- Kanzler/in oder Vizepräsident/in / als CIO
- Sonstiges

Gibt es an Ihrer Einrichtung die Position eines Chief Digital Officers (CDO)?

Bitte wählen Sie eine der folgenden Antworten:

- Ja
- Nein

Gibt es an Ihrer Einrichtung die Position eines Informationssicherheitsbeauftragten, IT-SiBe oder CISO?

- Ja
- Nein

Veränderungen zum Vorjahr

In diesem Bereich werden die Top-Antworten des letzten Jahres gelistet. Bitte geben Sie an, wie sich die Relevanz der Themen aus Ihrer Sicht verändert hat.

Bitte geben Sie an, ob sich aus Ihrer Sicht die Relevanz des Themas seit dem letzten Jahr verstärkt, gemindert oder nicht verändert hat.

Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

Zunahme Unverändert Abnahme

Fragen zum Schwerpunktthema „Digitale Souveränität“

Was sind aus Ihrer Sicht die wichtigsten Dimensionen oder Aufgabenbereiche, die „Digitale Souveränität“ Ihrer Hochschule ausmachen?

Welche Rolle spielen Open-Source-Technologien in Ihren Bemühungen um digitale Souveränität?

Welche Rolle spielen Cloud-Dienste und -Infrastrukturen außerhalb Ihrer Einrichtung bei der Umsetzung Ihrer digitalen Souveränitätsstrategie, und wie sichern Sie diese ab?

Welche Partnerschaften und Kooperationen mit anderen Hochschulen oder Forschungseinrichtungen unterhält Ihre Einrichtung, um die digitale Souveränität zu stärken?

Welche Maßnahmen hat Ihre Einrichtung ergriffen, um die Sicherheit und Integrität ihrer IT-Infrastruktur zu gewährleisten?

Nach welchem Standard wird das Informationssicherheitsmanagementsystem ISMS an Ihrer Einrichtung entwickelt?

- ISO 27
- BSI - IT-Grundschutz
- BSI - ZKI IT-Grundschutz-Profil für Hochschulen
- Eigener Ansatz
- Anderer Standard

Haben Sie einen Dienstleister für „Incident Response“ eingebunden?

- Ja
- Nein

Wie schätzen Sie das Risiko von Cyberangriffen auf Ihre Einrichtung ein?

- Von 1 - sehr gering bis 10 - sehr hoch

Kernumfrage

Die Kernumfrage besteht aus 12 Fragen.

Welche Top-Trends sehen Sie allgemein im IT-Bereich?

Welche Top-Trends sind für Sie besonders relevant?

Welche gesetzgeberischen Regelungen sehen Sie für sich im nächsten Jahr als besonders relevant?

Welche Themen bearbeiten Sie derzeit strategisch?

Welche neuen Aufgaben im Bereich Management bearbeiten Sie zurzeit?

In welchem Bereich werden externe Dienstleistungen wichtiger für Sie?

In welchen Bereichen investieren Sie mehr als vorher?

Welche Technologien werden für Sie wichtiger?

Welche neuen Dienste oder Technologien führen Sie derzeit ein?

Welche Fähigkeiten möchten Sie im nächsten Jahr gerne bzgl. IT in Ihrer Organisation aufbauen?

Welche Skills der Beschäftigten werden wichtiger?

Welche Skills der Beschäftigten werden weniger wichtig?

Umfragen der Vorjahre

2023

Umfrage: https://zenodo.org/doi/10.5281/zenodo.7599852

Englische Version der Auswertung: https://easychair.org/publications/download/9wWw

2022

Umfrage: https://doi.org/10.5281/zenodo.6012935

Englische Version der Auswertung: https://doi.org/10.5281/zenodo.7599926

2021

Umfrage: https://doi.org/10.5281/zenodo.4530714

Datenanhang: https://doi.org/10.5281/zenodo.4530743

Englische Version der Ergebnisauswertung: https://doi.org/10.5281/zenodo.4775115

2020

Umfrage: https://doi.org/10.5281/zenodo.3666168

Datenanhang: https://doi.org/10.5281/zenodo.3666170

2019

Umfrage: https://doi.org/10.5281/zenodo.2590659

Datenanhang: https://doi.org/10.5281/zenodo.2590683

2018

Umfrage: https://zenodo.org/record/1196427

Datenanhang: https://zenodo.org/record/1183499

Für die Auswertung der Umfrage wurden die folgenden Tools eingesetzt: Python mit Pandas, Matplotlib und Seaborn, Scikit-learn, Difflib, Gradio, Docx Library, ein lokales Sauerkraut 70B LLM