Lifelong Learning im Open C³S

Akademischen Weiterbildung im Bereich Cyber-Sicherheit: Zielgruppen, Inhalte, Organisationsformen und Anrechnung beruflicher Kompetenzen

Erwartungen von Experten im Umfeld von Open C³S

Eine Studie des Instituts für Soziologie der Technischen Universität Darmstadt und dem Institut für wissenschaftliche Weiterbildung der Hochschule Albstadt-Sigmaringen

Steve Kovács, Mario Stephan Seger und Christina Waldeyer

Gefördert vom:
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
AUFSTIEG DURCH BILDUNG OFFENE HOCHSCHULEN

Inhalt:

Befragung zur akademischen Weiterbildung im Bereich Cyber-Sicherheit: Zielgruppen, Inhalte, Organisationsformen und Anrechnung beruflicher Kompetenzen - Erwartungen von Experten im Umfeld von Open C³S

1. Einführung\Fragestellung

Im Rahmen des BMBF-geförderten Kooperationsprojektes Open Competence Center for Cyber Security (kurz Open C³S) und im Sinne des projektinternen Qualitätsmanagements wurde eine empirische Erhebung zu Fragen der Ausgestaltung akademischer Weiterbildungen im Bereich Cyber-Sicherheit durchgeführt. Die zentralen Schwerpunkte dieser Studie umfassen die Ermittlung der Zielgruppen sowie der Erwartungen hinsichtlich der Inhalte und Organisationsformen im Kontext der Anrechnung beruflicher Kompetenzen auf hochschulische und universitäre Studiengänge.

Zielsetzung dieser Umfrage ist letztlich die Identifizierung der inhatllichen und organisatorischen Anforderungen an die akademischen Weiterbildungsangebote im Kontext von Cyber-Sicherheit bzw. Open C³S. Das schließt vor dem Hintergrund von „Anrechnung beruflicher Lernergebnisse auf Studiengänge“ und „passgenauer Konzeption von Bildungsangeboten“ auch ein Blick auf die Bildungsherkunft der potenziell Nachfragenden ein.

Die Befragung erfolgte pilothaft in Kooperation des Instituts für Soziologie der Technischen Universität Darmstadt (TU) und dem Institut für wissenschaftliche Weiterbildung (IWW) an der Hochschule Albstadt-Sigmaringen (HSAS).

2. Anlage und Ausgestaltung der Studie

Die Befragung wurde als interner Forschungsauftrag mit projektrelevanten und projektnahestehenden Organisationen in anonymisierter Form durchgeführt.

In Abstimmung der beiden verantwortlichen Institute wurde der verwendete elektronische Fragebogen konzipiert und systematisch auf die wesentlichen Aspekte komprimiert. Auf insgesamt zehn Seiten wurden Fragen zur IT-Aus- und Weiterbildung, dem Bedarf an Weiterbildung im Bereich Cyber-Sicherheit, der Ausgestaltung dieser Weiterbildung sowie zur Anrechnung beruflich erworbener Kompetenzen auf Hochschulstudiengänge im Bereich Cyber-Sicherheit formuliert. Ergänzt wurden die Fragen - zu welchen überwiegend Mehrfachnennungen zugelassen waren - durch offene Antwortkategorien. Die Offenheit der Fragen sollte eine weitestgehend vollständige Analyse des Meinungsbildes gewährleisten. Abgerundet wurde der Fragebogen durch einige persönliche Daten zu den jeweiligen Organisationen, Instituten und Unternehmen der befragten Experten. Die teilstandardisierte Befragung erfolgte online durch einen zuvor versandten Link an die ausgewählten Teilnehmer. Der Rücklauf der gesamten Befragung ergab bei einer Auswahl von 67 Personen eine Teilnehmeranzahl von 29 Personen (43,3 %). Die Datenbasis der Studie resultiert aus einem ausgewählten Expertenkreis im Umfeld von Open C³S und ist somit nur

auf den Kontext von Open C³S bezogen.

3. Analysebegriffe und Lesehinweise der Studie

Die zweiundzwanzig Fragen der vorliegenden Studie werden jeweils texteinleitend dargestellt. Jede Frage wurde mit einer Kennziffer „K" versehen und durchgehend nummeriert. Es ergeben sich somit insgesamt 22 Kennzahlen.

Die verwendeten Diagramme der Studie sind zwecks Erleichterung der Zuordnung entsprechend den zweiundzwanzig Fragen der Umfrage mit den jeweiligen Kennziffern nummeriert.

In den einzelnen Diagrammen und Texten werden jeweils die ermittelten Prozentsätze angegeben. Die Stichprobengröße (N = 29) und die Anzahl der gültigen Fälle sind in jedem Diagramm ausgezeichnet. Die Datensätze mit sämtlichen absoluten Zahlen sind außerdem im Anhang hinterlegt.

Aus Gründen der besseren Lesbarkeit wurde i.d.R. auf ein Binnen-I oder ein Gender Gap verzichtet und die maskuline Schreibweise verwendet. Es soll darauf hingewiesen werden, dass sowohl die maskuline als auch die feminine Schreibweise für die entsprechenden Beiträge impliziert wird.

4. Auswertung der Studie
4.1 IT-Aus- und Weiterbildung: Verteilung in den Organistionen

Einleitend der Bereich "IT-Aus und Weiterbildung" (K 1 bis K 4). Dieser Abschnitt beinhaltet die Auswertung der Fragen zur Ausprägung der staatlich geprüften IT- Aus- und Weiterbildungen ebenso wie zu privat-rechtlich zertifizierten Weiterbildungen in den befragten Unternehmen. Zudem wird nach der Anzahl der Beschäftigten im Bereich der Cyber-Sicherheit in den jeweiligen Organisationen gefragt.

K1.
Gibt es Beschäftigte in Ihrer Organisation, die eine berufliche IT-Aus- oder IT-Weiterbildung absolviert haben? (Mehrfachnennungen möglich)

- □ ja
- □ nein
- □ weiß ich nicht

Bei 20 gültigen Fällen, sind mit je 60,0 % die staatlich geprüften IT-Ausbildungen sowie die IT-Weiterbildungen der Operativen Professionals in den Organisationen der Befragten wahrgenommen worden. Dicht gefolgt von den Strategischen Professionals mit je 55,0 % und den IT-Spezialisten mit 40,0 %. Mit einem Wert von 35,0 % können die IT-Spezialisten zugleich als verhältnismäßig unbekannt innerhalb der jeweiligen Arbeitsumfelder gelten. Mit 10,0 bis 15,0 % kann das wahrgenommene Fehlen aller Zertifikate in den befragten Organisationen als verhältnismäßig niedrig erachtet werden.

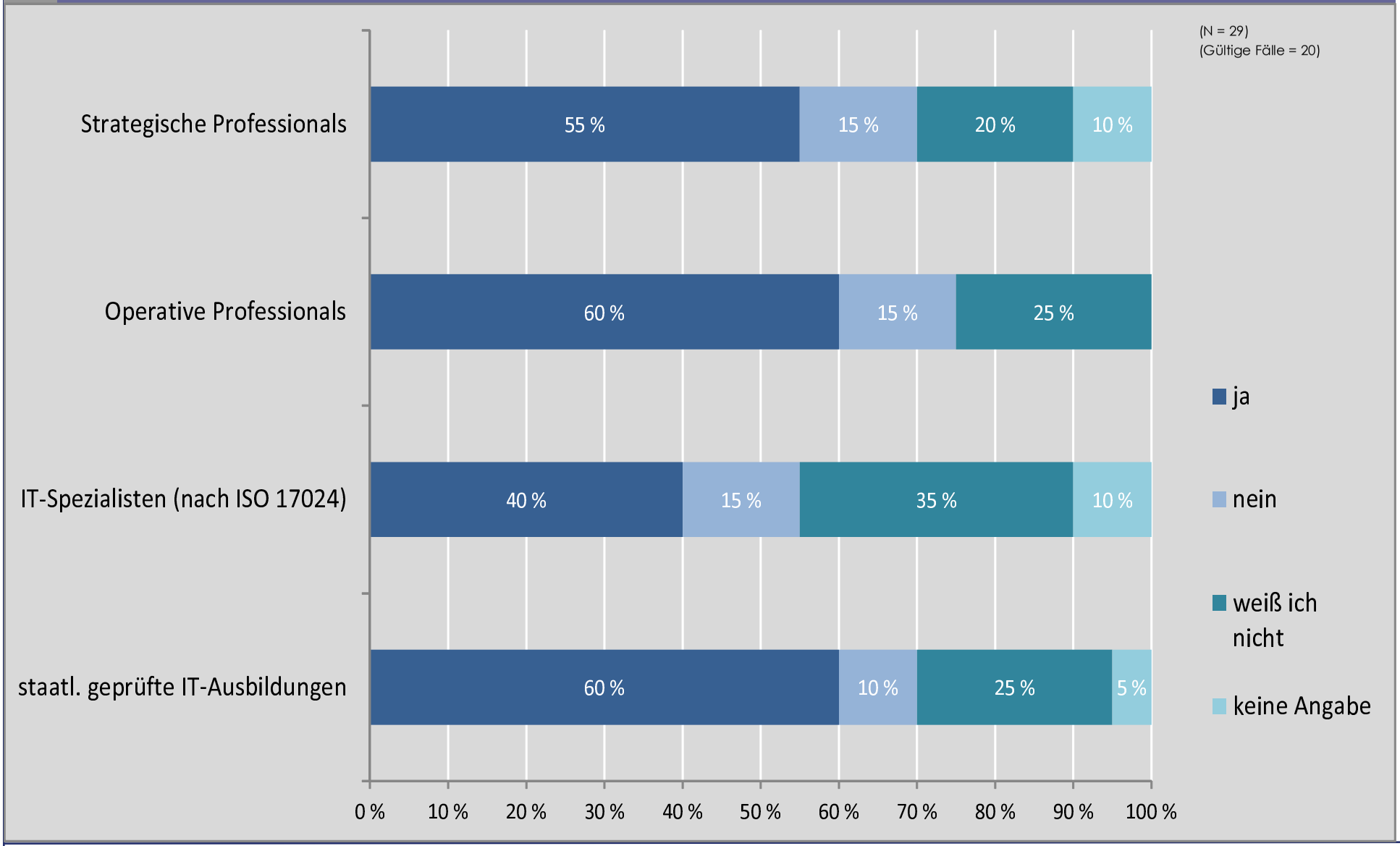
K2.

Wie viele Beschäftigte innerhalb Ihrer Organisation sind schätzungsweise mit Aufgaben der Cyber-Sicherheit betraut?

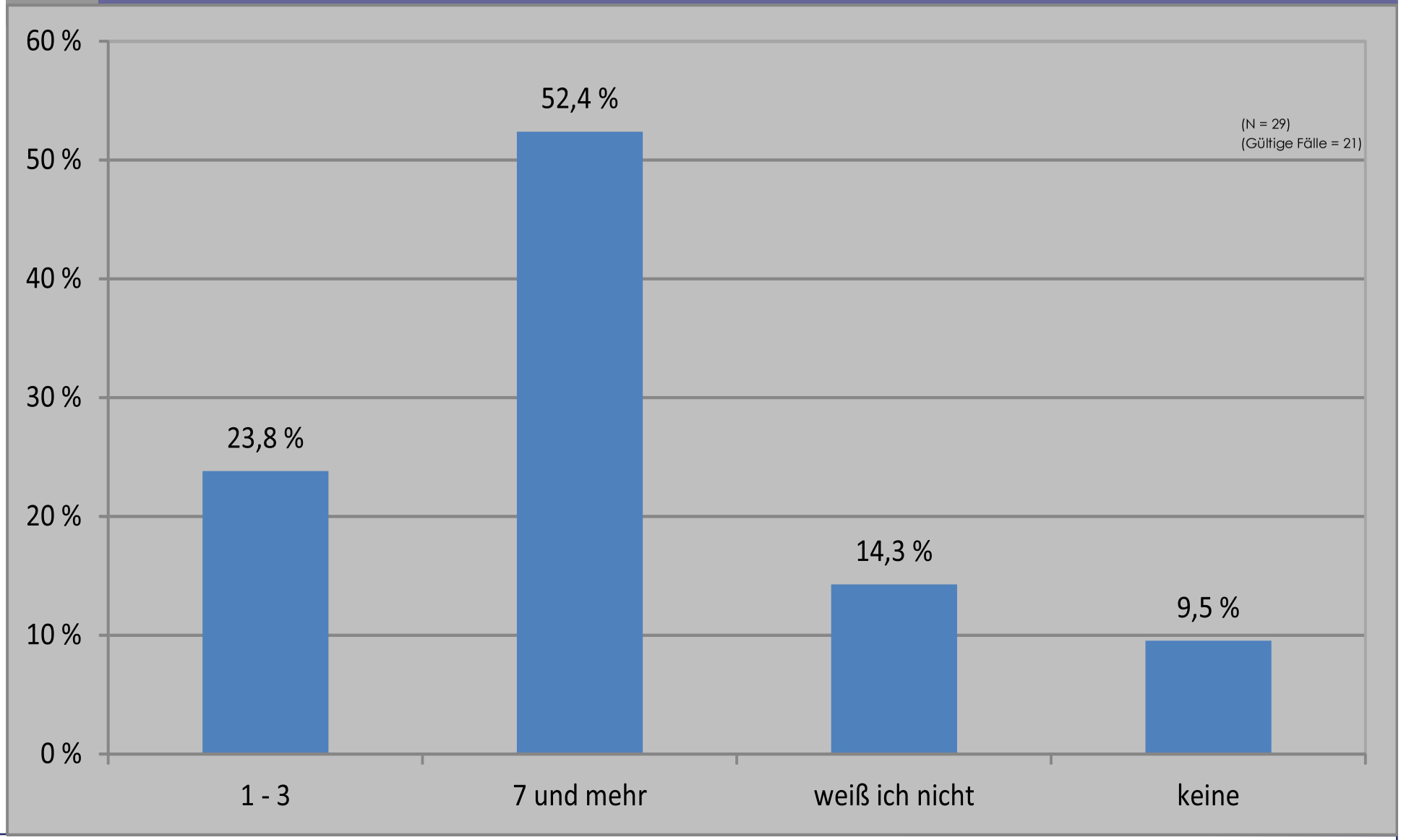
- □ keine
- □ 1-3
- □ 4-6
- □ 7 und mehr
- □ weiß ich nicht

Durchschnittlich gaben knapp die Hälften der Befragten (52,4 %) an, sieben oder mehr Beschäftigte in den Organisationen mit Aufgaben der Cyber-Sicherheit betraut zu wissen. 23,8 % der Befragten haben schätzungsweise ein bis drei Mitarbeiter in der Cyber-Sicherheit, 9,5 % haben keine und 14,3 % können keine Schätzung vornehmen.

K1 IT- Aus- und Weiterbildung (in Prozent)



K2 Cyber-Sicherheit in der Organisation (in Prozent)



K3.

Besitzen Beschäftigte innerhalb Ihrer Organisation eines der folgenden IT-Zertifikate?
(Mehrfachnennungen möglich)

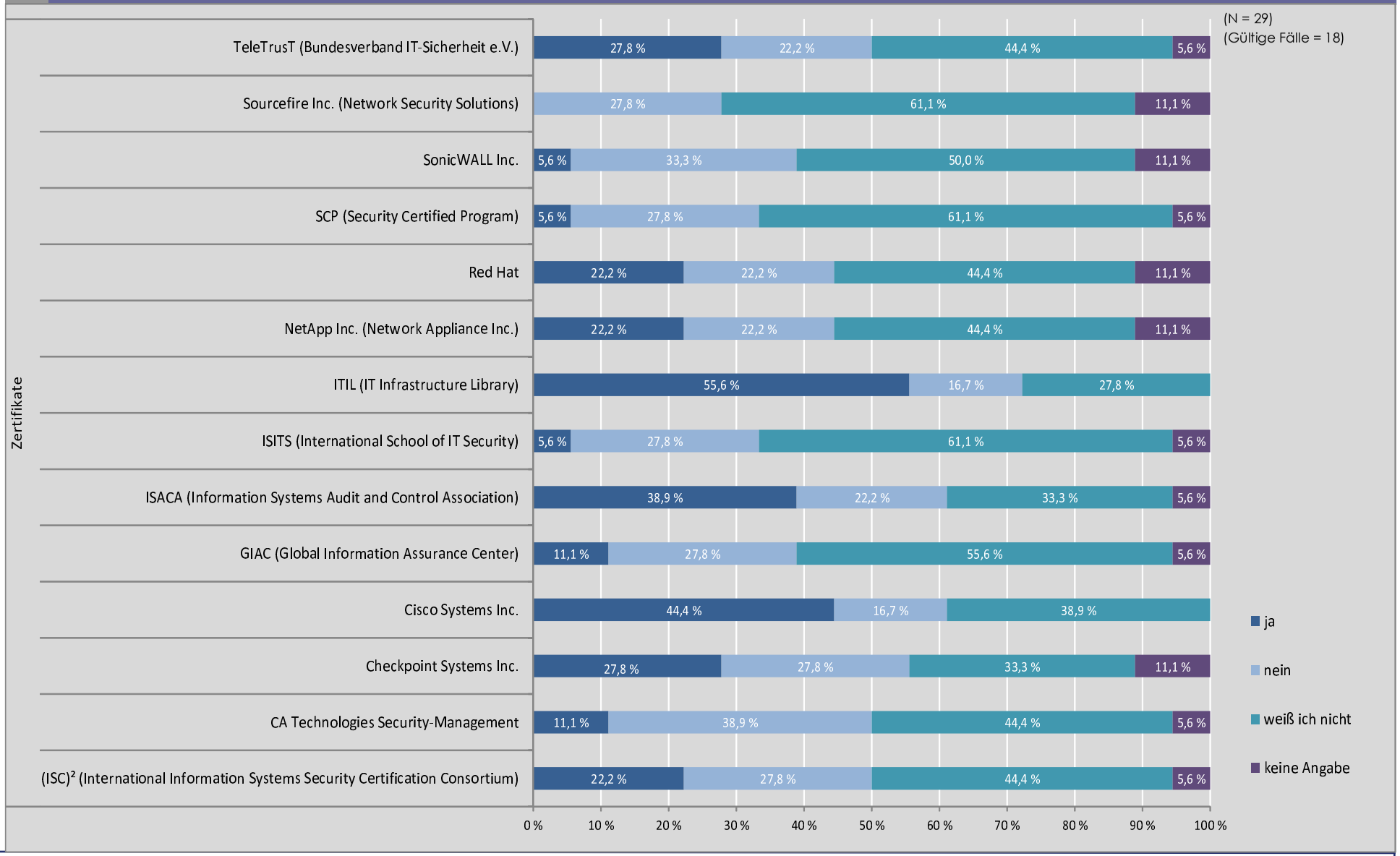
- □ (ISC)² (International Information Systems Security Certification Consortium)
- □ CA Technologies Security-Management
- □ Checkpoint Systems Inc.
- □ Cisco Systems Inc.
- □ GIAC (Global Information Assurance Center)
- □ ISACA (Information Systems Audit and Control Association)
- □ ISITS (International School of IT Security)
- □ ITIL (IT Infrastructure Library)
- □ NetApp Inc. (Network Appliance Inc.)
- □ Red Hat
- □ SCP (Security Certified Program)
- □ SonicWALL Inc.
- □ Sourcefire Inc. (Network Security Solutions)
- □ TeleTrusT (Bundesverband IT-Sicherheit e.V.)

Auf die Frage, welche Weiterbildungszertifikate in den jeweiligen Organisationen vertreten sind, wurden am häufigsten die Zertifikate von ITIL (IT Infrastructure Library) mit 55,6 %, Cisco Systems Inc. mit 44,4 % und ISACA (Information Systems Audit and Control Association) mit 38,9 % genannt. Wiederum gefolgt von Checkpoint Systems Inc. und TeleTrusT (Bundesverband IT-Sicherheit e.V.) mit je 27,8 % und (ISC)² (International Information Systems Security Certification Consortium), NetApp Inc. (Network Appliance Inc.) sowie Red Hat mit je 22,2 %. Im unterem Drittel liegen hingegen CA Technologies Security-Management (11,1 %), GIAC (Global Information Assurance Center) (11,1 %), ISITS (International School of IT Security), SCP (Security Certified Program) und SonicWALL Inc. mit je 5,6 %. Nicht genannt wurden hingegen die Zertifikate der Sourcefire Inc. (Network Security Solutions).

Als nicht in den Organisation vertreten gelten insbesondere die IT-Zertifikate von CA Technologie (38,9 %), SonicWALL (33,3 %) sowie (ISC)², Checkpoint Systems, GIAC, ISITS, SCP und Sourcefire mit je 27,8 %.

Im Vergleich gelten die Zertifikate von ISITS, SCP und Sourcefire als die Unbekanntesten in den Organisationen (je 61,1 %). Auch die GIAC-Zertifikate sind mit 55,6 % den Umfrageteilnehmern verhältnismäßig unbekannt.

K3 Weiterbildungszertifikate in der Organisation (in Prozent)



K4.

Sind Ihnen weitere IT-Zertifikate bekannt, die Beschäftigte in Ihrer Organisation absolviert haben?
(Falls es keine weiteren Zertifikate in Ihrem Zuständigkeitsbereich gibt, lassen Sie dieses Feld bitte frei)

Um einen möglichst ganzheitlichen Überblick über das Weiterbildungsspektrum in den befragten Unternehmen zu bekommen, hatten die Befragten ergänzend zur vorherigen Frage (K3) die Möglichkeit, weitere ihnen, aus ihren Unternehmen bekannte IT-Zertifikate zu benennen. Genannt wurden:

- AccessData ACE
- AMBCI
- CISA
- CISM
- Google AdWords Spezialist
- IEEE Certified Biometrics Professional (CBP)
- ISSECO Certified Professional for Secure Software Engineering (CPSSE)
- LPIC 1-3
- Novell
- PSA

4.2 Weiterbildungsbedarf aus Perspektive der Organisationen

Es folgt die Analyse des Bedarfs an Weiterbildungen im Bereich der Cyber-Sicherheit (K5 - K6). Es wird explizit nach dem Bedarf an Weiterbildungen im Rahmen von IT-Studiengängen und IT-Weiterbildungszertifikaten im Kontext von Hochschulstudiengängen bzw. äquivalenten Weiterbildungen gefragt.

K5.

Gibt es in Ihrer Organisation den Bedarf, Beschäftigte im Rahmen eines IT-Studiengangs oder eines IT-Weiterbildungszertifikats auf akademischem Niveau weiterzuqualifizieren?

□ ja
□ nein
□ weiß ich nicht

Der nächste Fragenkomplex thematisierte den Bedarf nach Weiterbildungen in den Organisationen der Umfrageteilnehmer. Es wurde unterschieden nach IT-Studiengängen und IT-Weiterbildungszertifikaten, wobei beide Fragenkategorien als Filterfragen Pflichtfelder waren.

Wie in der nachfolgenden Grafik illustriert, sehen 60,0 % der Befragten einen Weiterbildungsbedarf hinsichtlich des Angebots von IT-Studiengängen. Bei den IT-Weiterbildungszertifikaten sind es sogar 65,0 %. Verneint wird ein Bedarf an IT-Studiengängen zu 25,0 % und an IT-Weiterbildungszertifikaten zu 10,0 %. Mit 15,0 % beziehungsweise 25,0 % befinden sich die Anzahl der unentschlossenen und enthaltenen Nennungen im mittleren Bereich. Zusammengefasst spricht vieles für einen verhältnismäßig hohen Weiterbildungsbedarf in beiden Kategorien, mit einem Fokus auf den Weiterbildungszertifikaten.

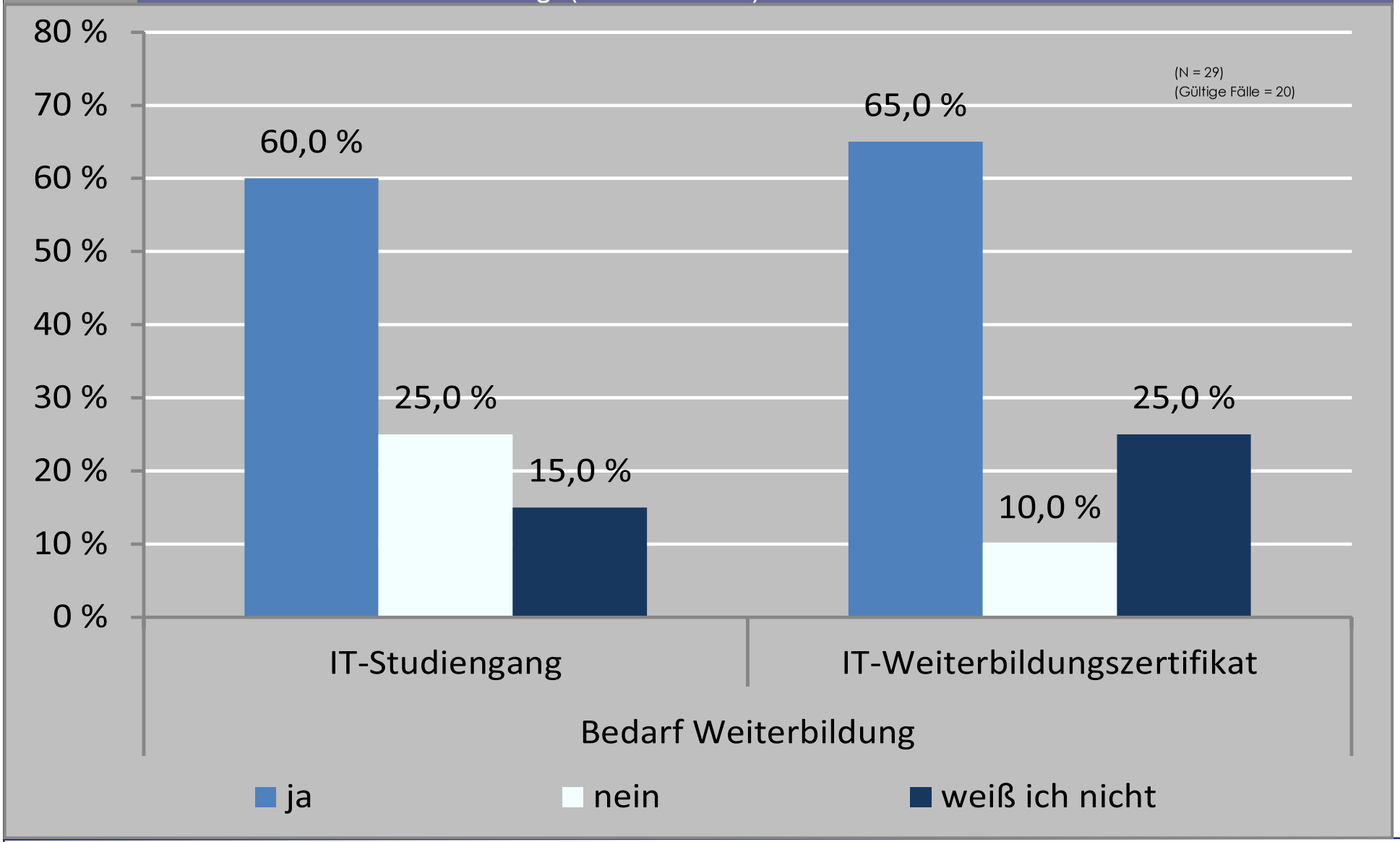
K6.

Was würden Sie sagen: Woraus resultiert in Ihrer Organisation der Bedarf, Beschäftigte auf akademischem Niveau weiterzuqualifizieren? (Falls Sie diesen nicht klar benennen können, lassen Sie dieses Feld bitte frei)

Der Bedarf Beschäftigte auf akademischen Niveau weiterzuqualifizieren resultiert eindeutig aus der Absicht fachlich fundierte Qualifikationen zu fördern.
Es wurden insgesamt genannt:

- Fundierung der Qualifikation bzgl. des technologischen Fortschritts.
- IT-/Forensik-Grundlagen für nicht Beamte/Tarifbeschäftigte, die keine IT-Ausbildung oder Studium haben.
- Anerkennung als IT-/Forensik-Sachverständige.
- Da aus unserer Sicht nur über derartige Angebote eine notwendige Fachtiefe erreicht werden kann.

K5 Bedarf an Weiterbildung (in Prozent)



4.3 Anforderungen an die Ausgestaltung der Weiterbildung

Nachfolgend die Ausdifferenzierung des wahrgenommen und konturierten Weiterbildungsbedarfs (K5 - K6). Um diesen Bedarf differenzierter betrachten zu können, beschreiben die nachfolgenden Kennzahlen die Form (K7), die Inhalte (K8), die Organisation (K9) und den Umfang (K10) der als sinnvoll erachteten Weiterbildungen. Abgerundet werden die Angaben schließlich durch „weitere Aspekte“ (K11).

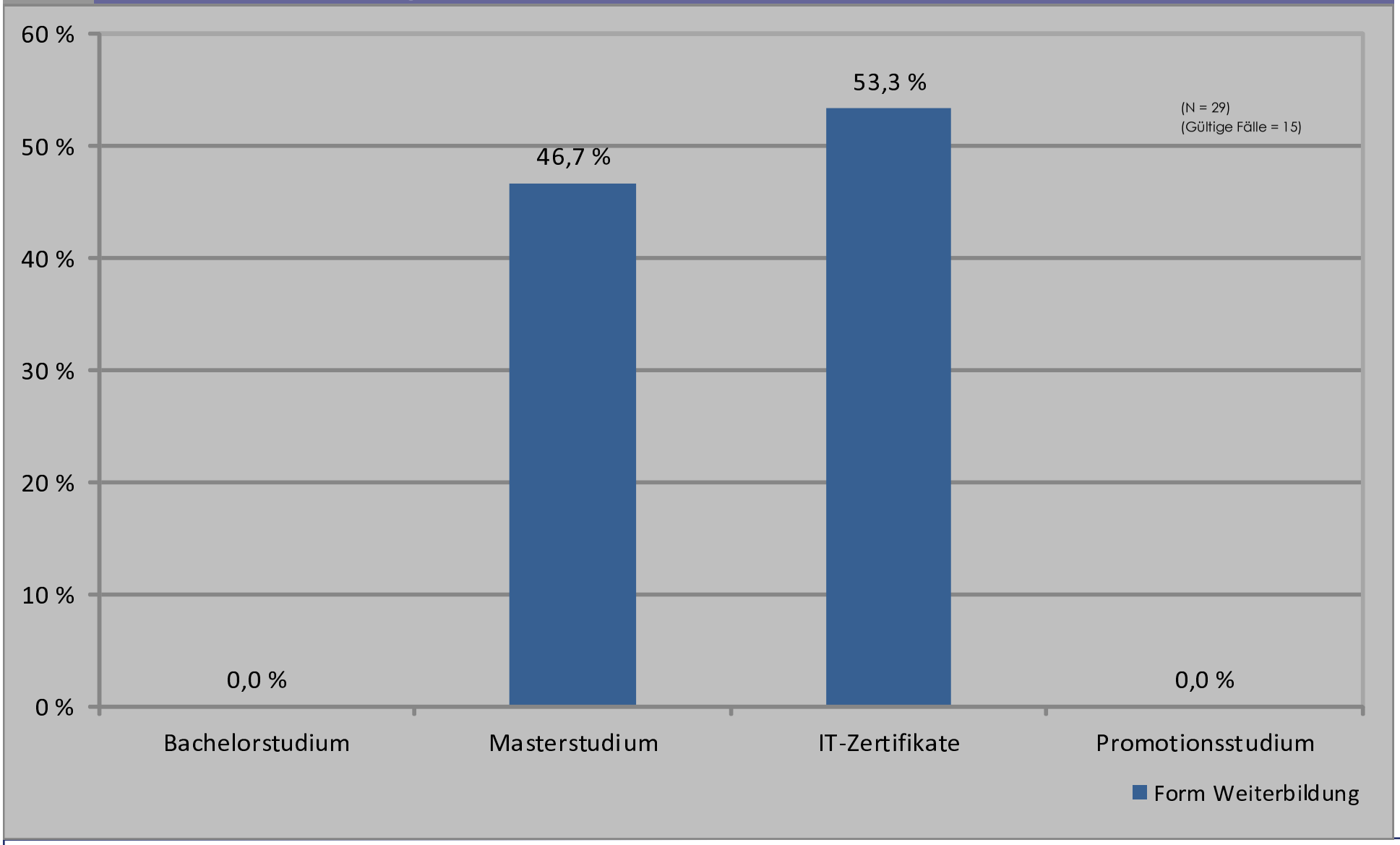
K7.

Welche Form der akademischen Weiterbildung im Bereich Cyber-Sicherheit sehen Sie prinzipiell als die Sinnvollste an?

- □ Bachelorstudium
- □ Masterstudium
- □ Promotionsstudium
- □ IT-Zertifikate

Als sinnvollste Weiterbildungsform innerhalb des Bereichs Cyber-Sicherheit wurden mit 53,3 % die IT-Zertifikate gewählt. Mit fast der Hälfte der Nennungen (46,7 %) wird auch das Masterstudium als sinnvolle Weiterbildung erachtet. Das bedeutet im Umkehrschluss, dass weder das Promotions- noch das Bachelorstudium als sinnvollste Weiterbildung im Bereich der Cyber-Sicherheit gelten.

K7 Form der Weiterbildung (in Prozent)



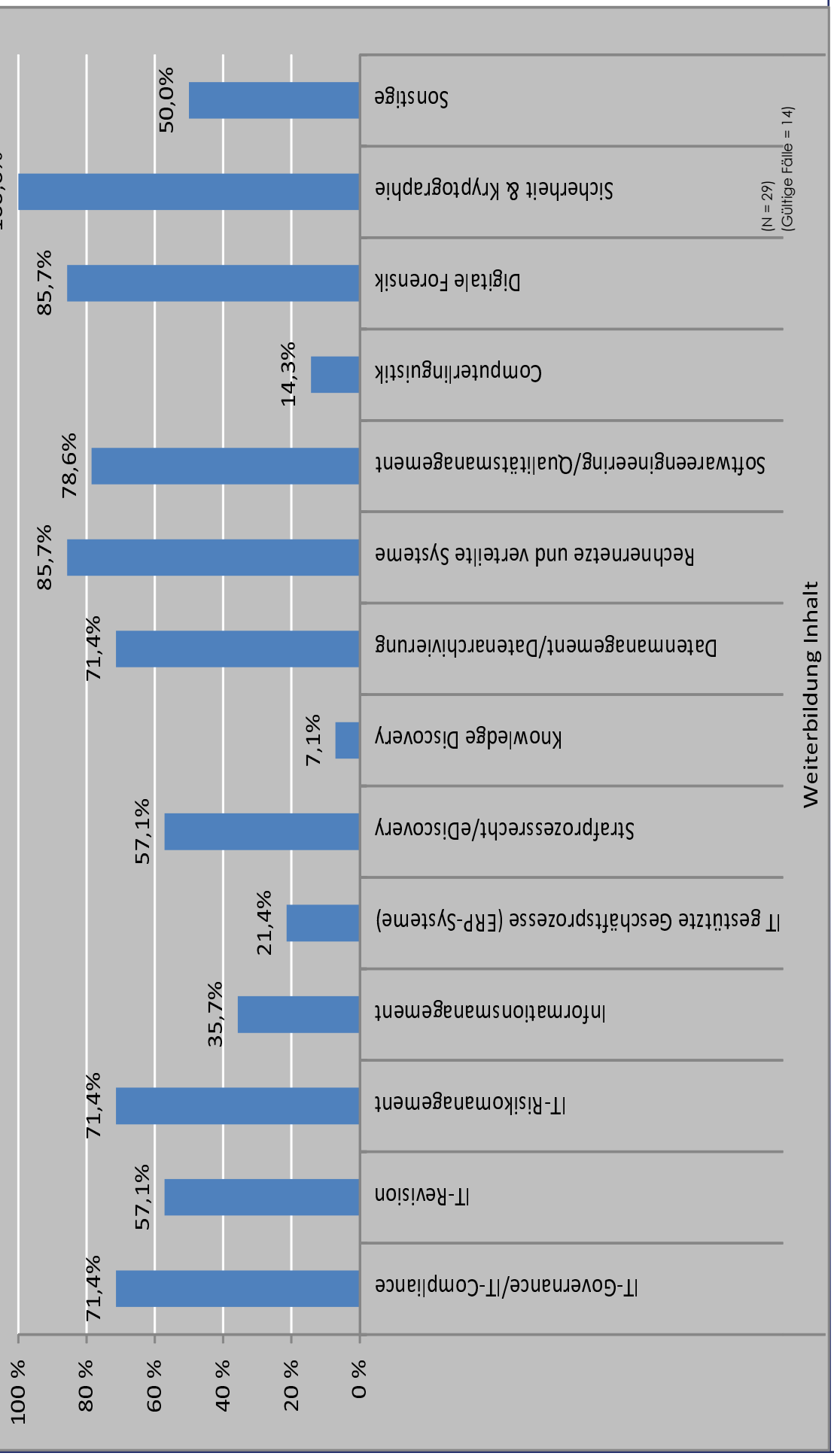
K8.

Welche Inhalte einer akademischen Weiterbildung im Bereich Cyber-Sicherheit erachten Sie als unverzichtbar? (Mehrfachnennungen möglich)

- □ IT-Governance/IT-Compliance
- □ IT-Revision
- □ IT-Risikomanagement
- □ Informationsmanagement
- □ IT geschützte Geschäftsprozesse (ERP-Systeme)
- □ Strafprozessrecht/eDiscovery
- □ Knowledge Discovery
- □ Datenmanagement/Datenarchivierung
- □ Rechnernetze und verteilte Systeme
- □ Softwareengineering/Qualitätsmanagement
- □ Computerlinguistik
- □ Digitale Forensik
- □ Sicherheit & Kryptographie
- □ Sonstige

Mit 100 % wird der Bereich „Sicherheit & Kryptographie“ als unverzichtbarer Bestandteil einer Cyber-Sicherheitsausbildung erachtet. Die höchsten Werte erreichen auch die Inhalte “Rechnernetze und verteilte Systeme” und “Digitale Forensik” mit je 85,7 %. Dicht gefolgt von “Softwareengineering/Qualitätsmanagement” 78,6 %, “IT-Governance/IT-Compliance”, “IT-Risikomanagement” sowie “Datenmanagement/Datenarchivierung“ mit je 71,4 %. Die Schwerpunkte “IT Revision” und „Strafprozessrecht/eDiscovery“ erhalten rund die Hälfte der Nennungen (57,1 %) und im unterem Drittel befinden sich “Informationsmanagement” (35,7 %), „IT gestützte Geschäftsprozesse (ERP-Systeme)“ (21,4 %) ebenso wie Computerlinguistik (14,3 %) und Knowledge Discovery (7,1 %).

K8 Inhalte der Weiterbildung (in Prozent)

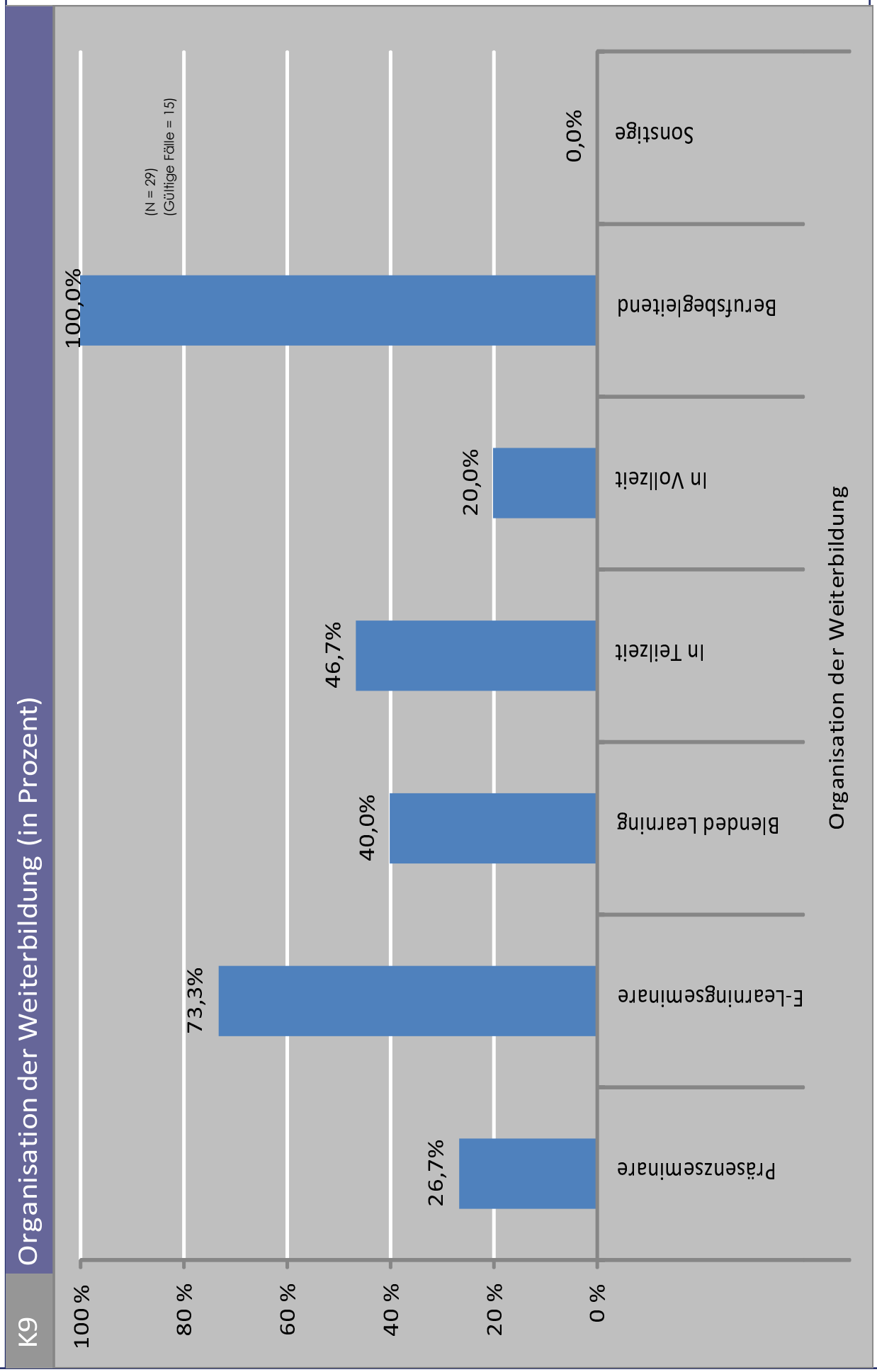


K9.

Wie sollte eine akademische Weiterbildung im Bereich Cyber-Sicherheit Ihrer Meinung nach optimaler Weise organisiert sein? (Mehrfachnennungen möglich)

- □ Präsenzseminare
- □ E-Learningseminare
- □ Blended Learning
- □ In Teilzeit
- □ In Vollzeit
- □ Berufsbegleitend
- □ Sonstige

Es sprechen sich 100 % für die berufsbegleitende Weiterbildung als optimale Organisation im Bereich Cyber-Sicherheit aus. Das Vollzeitstudium erhält nur 20,0 % der Nennungen. 73,3 % erreichen die E-Learningseminare. Das Blended Learning (40,0 %) und die Studienangebote in Teilzeit (46,7 %) liegen knapp unter fünfzig Prozent und Präsenzseminare werden mit 26,7 % deutlich geringer gewichtet.


K9
Organisation der Weiterbildung (in Prozent)
(N = 29)
(Gültige Fälle = 15)
100 %
80 %
60 %
40 %
20 %
0 %
26,7%
73,3%
40,0%
46,7%
20,0%
100,0%
0,0%
Präsenzseminare
E-Learningseminare
Blended Learning
In Teilzeit
In Vollzeit
Berufsbegleitend
Sonstige
Organisation der Weiterbildung

K10. Formulierung

Welchen zeitlichen Umfang halten Sie für eine akademische Weiterbildung im Bereich Cyber-Sicherheit für den Vertretbarsten?

- □ Wochenendseminare (Zertifikate)
- □ Seminare bis maximal 3 Monate (Zertifikate)
- □ Seminare bis maximal 6 Monate (Zertifikate)
- □ Seminare bis maximal 9 Monate (Zertifikate)
- □ Seminare bis maximal 1 Jahr (Zertifikate)
- □ 1 - 2 Jahre (Studium)
- □ 3 - 4 Jahre (Studium)
- □ mehr als 4 Jahre (Studium)
- □ Sonstiges

Hinsichtlich des Umfangs akademischer Ausbildungen im Bereich Cyber-Sicherheit (K10) sind zwei unterschiedliche Muster erkennbar. Je weiter die Struktur von diesen abweicht, desto geringer fällt der Prozentsatz aus:

- Das akademische Studium: als zeitlichen Umfang eines regulären Studiums werden 3 bis 4 Jahre veranschlagt (26,7 %). Auch Studiengänge im Umfang von 1 bis 2 Jahren sind denkbar (13,3 %). Ein Studienumfang von mehr als vier Jahren ist nicht als Option gewählt worden.

- Die Weiterbildungszertifikate: Zu 26,7 % wird ein Seminarumfang von maximal 3 Monaten favorisiert. Dieses entspricht dem Wert akademischer Studiengänge im Zeitraum von 3 bis 4 Jahren. Weiterbildungszertifikate mit einer Dauer von sechs Monaten oder maximal einem Jahr, werden als deutlich weniger vertretbar erachtet (20,0 % bzw. 13,3 %) und Zertifikatsangebote im Umfang von weniger als drei Monaten werden nicht gewählt.

Insgesamt favorisieren 60,0 % der Befragten Weiterbildung im Bereich IT-Sicherheit als Seminar. Dem steht ein Wert von 40,0 % für das akademische Studium gegenüber.

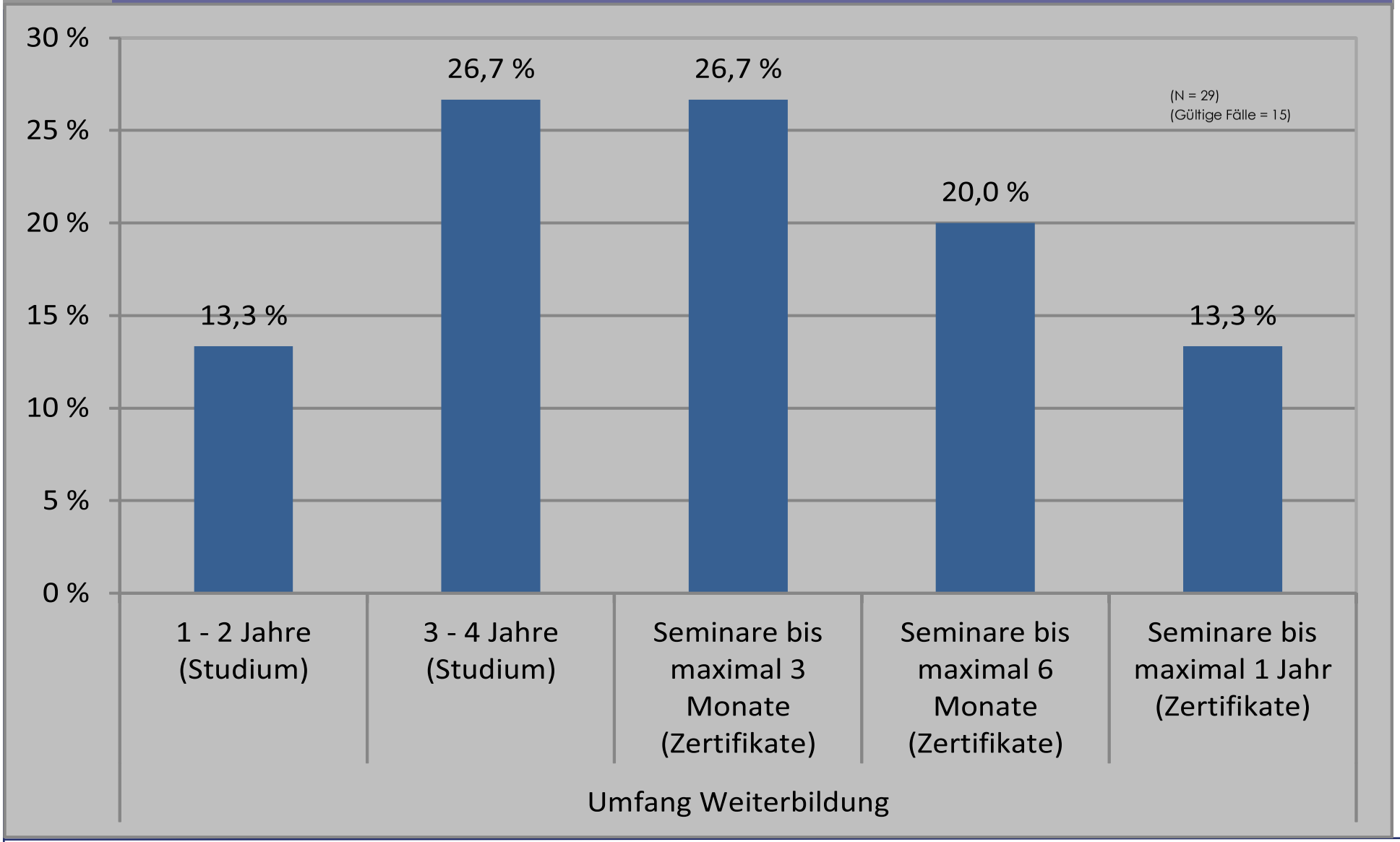
K11.

Gibt es außerdem noch andere zentrale Eckpunkte, die Sie im Kontext einer akademischen Cyber-Sicherheitsweiterbildung für unverzichtbar halten?

Als weitere zentrale Anforderungen an die Gestaltung einer akademischen Ausbildung im Bereich der Cyber-Sicherheit (K11) wurden folgende sechs Punkte genannt:

- Forum / Plattform für den Austausch der Teilnehmer/-innen,
- gutes Lernmaterial für das Selbststudium,
- internationale Anerkennung,
- praxisnahe Qualifizierung anhand realer Beispiele,
- Praxisbezug,
- hoher Level.

K10 Umfang Weiterbildung (in Prozent)



4.4 Erfahrungen mit Anrechnung

Im Abschnitt "Anrechnung beruflicher Kompetenzen auf Hochschulstudiengänge" (K12 - K13) wird nach der Auseinandersetzung mit der Thematik und der individuellen Bewertung ihrer Sinnhaftigkeit gefragt.

K12.

Haben Sie sich vor der Teilnahme an dieser Untersuchung mit der Thematik „Anrechnung beruflicher Kompetenzen auf Hochschulstudiengänge" beschäftigt?

- □ ja
- □ nein

Die Mehrheit - nämlich 52,6 % - gab an, sich vor Beginn der vorliegenden Untersuchung mit dem Thema der Anrechnung beruflicher Kompetenzen befasst zu haben. Folgerichtig verneinten 47,4 % der Teilnehmer die Frage.

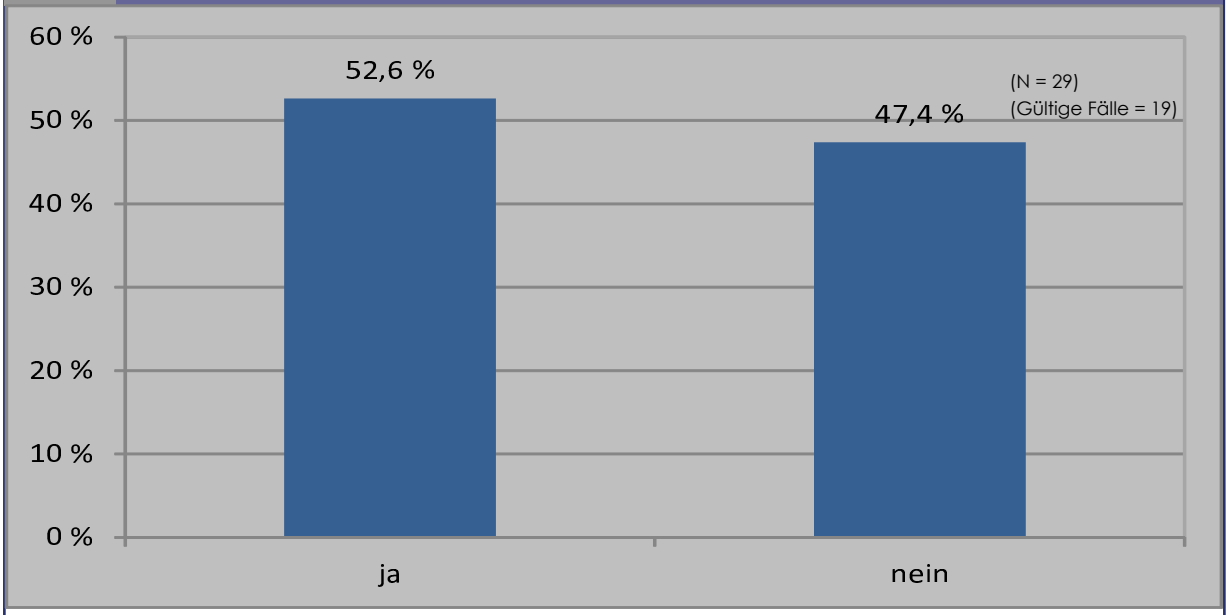
K13.

Finden Sie die Anrechnung beruflicher Kompetenzen auf ein IT-Hochschulstudium sinnvoll?

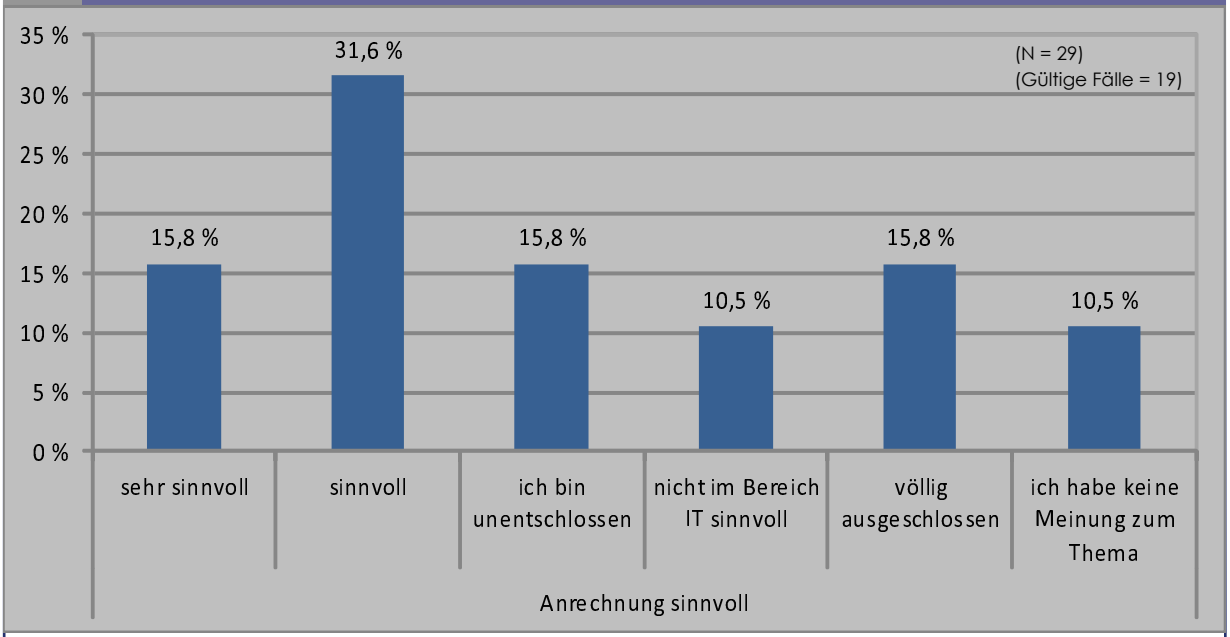
- □ sehr sinnvoll
- □ sinnvoll
- □ ich bin unentschlossen
- □ nicht im Bereich IT sinnvoll
- □ völlig ausgeschlossen
- □ ich habe keine Meinung zum Thema

Gefragt nach der Sinnhaftigkeit einer Anrechnung beruflicher Kompetenzen auf ein IT-Hochschulstudium (K13) entschieden sich 31,6 % für die Option sinnvoll, 15,8 % für sehr sinnvoll. Weitere 15,8 beziehungsweise 10,5 % gaben an, in der Frage unentschlossen zu sein oder keine Meinung zum Thema zu haben. Möglicherweise sind diese letztgenannten Werte mit der teilweise geringen Auseinandersetzung mit dem Themenfeld zu erklären, welches sich bereits in der Auswertung des K12 abgezeichnet hatte.

K12 Beschäftigung mit Anrechnung (in Prozent)



K13 Anrechnung sinnvoll beruflicher Kompetenzen (in Prozent)



4.5 Anforderungen an die Ausgestaltung der Anrechnung

Vom Allgemeinem ins Spezifische betrachtet thematisiert der Abschnitt "Ausgestaltung der Anrechnung" die "Anrechnungsziele" (K14 und K15) und das "Anrechnungspotenzial" (K16) privatrechtlicher IT-Weiterbildungszertifikate.

K14.

Welches Ziel verbinden Sie primär mit dem Gedanken „Anrechnung beruflicher Kompetenzen auf akademische Weiterbildungsangebote"?

- □ Ausbildungsverkürzung
- □ Vermeidung von Ausbildungsdopplungen
- □ Differenzierte Ausbildungen
- □ Soziale Chancengleichheit
- □ Fachkräftemangelabbau
- □ Keines der genannten

Die Anrechnung beruflicher Kompetenzen wird zu 37,5 % mit dem Ziel verbunden, Dopplungen in der Weiterbildung der Anrechnungsanwärter zu vermeiden. Mit je 25,0 % gilt auch die Bestrebung differenzierte Ausbildungen anzubieten und den Fachkräftemangel abzubauen als sinnvoll. Die Optionen "Ausbildungsverkürzung" und "Soziale Chancengleichheit" wurden hingegen nicht als primäre Anrechnungsziele gewählt. 12,5 % gaben wiederum an, keines der genannten Anrechnungsziele anzustreben.

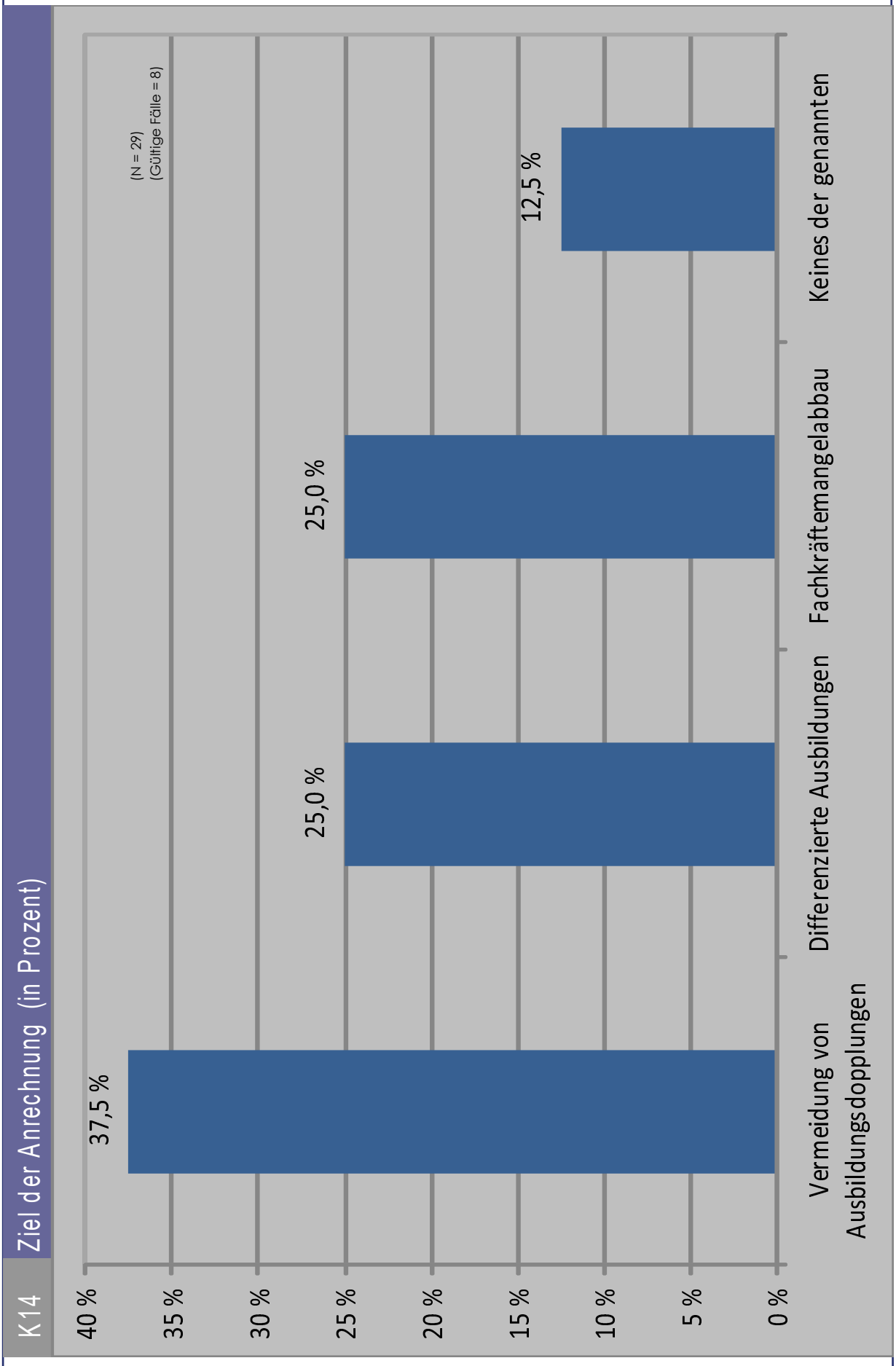
K15.

Mit Blick auf Ihre Kolleginnen und Kollegen bzw. Mitarbeiterinnen und Mitarbeiter: Ist Ihnen im Zusammenhang mit einer Anrechnung auf akademische Weiterbildung im Bereich Cyber-Sicherheit noch Weiteres wichtig? (Falls Ihnen nichts weiter wichtig ist, dieses Feld bitte frei lassen)

Als weitere wichtige Ziele in Bezug auf die Anrechnung beruflicher Kompetenzen wurden folgende zwei Punkte von den Experten* benannt:

- Ein außerhochschulischer Vertreter bemerkte: Gezielte und qualifizierte Weiterbildung - Mangel geeigneter Seminarangebote im Fachbereich der Forensik
- ein hochschulischer Vertreter bemerkte: Keine Geschenke: Anrechnung von Hochschulleistungen ok, Anrechnung von beruflichen Leistungen schwierig ggf. mit Prüfung verbunden.**

* die vorliegende Expertenunterscheidung erfolgte anhand einer Filtersetzung anhand der Organisationskategorien in K19
** laut FAU- Leitfaden zur Anrechnung von Studien- und Prüfungsleistungen auf der Grundlage von Kompetenzen (Abschnitt 3.2) sind mündliche oder schriftliche Prüfungen zur Ermittlung von Lernergebnissen nicht zulässig.


K 14 Ziel der Anrechnung (in Prozent)
(N = 29)
(Gültige Fälle = 8)
40 %
35 %
30 %
25 %
20 %
15 %
10 %
5 %
0 %
37,5 %
25,0 %
25,0 %
12,5 %
Vermeidung von Ausbildungsdopplungen
Differenzierte Ausbildungen
Fachkräftemangelabbau
Keines der genannten

K16.

Bitte beurteilen Sie: Welches Anrechnungspotenzial rechnen Sie den nachfolgenden IT-Zertifikaten mit Blick auf einen Weiterbildungsstudiengang im Bereich Cyber-Sicherheit zu?

niedriges Potenzial <------- -------- -------> hohes Potenzial weiß ich nicht

Bezüglich des erwarteten Potenzials der nachfolgend aufgelisteten privatrechtlichen Weiterbildungszertifikate auf einen akademischen Studiengang im Bereich Cyber-Sicherheit angerechnet zu werden ergaben sich folgende vier unterschiedliche Profile:

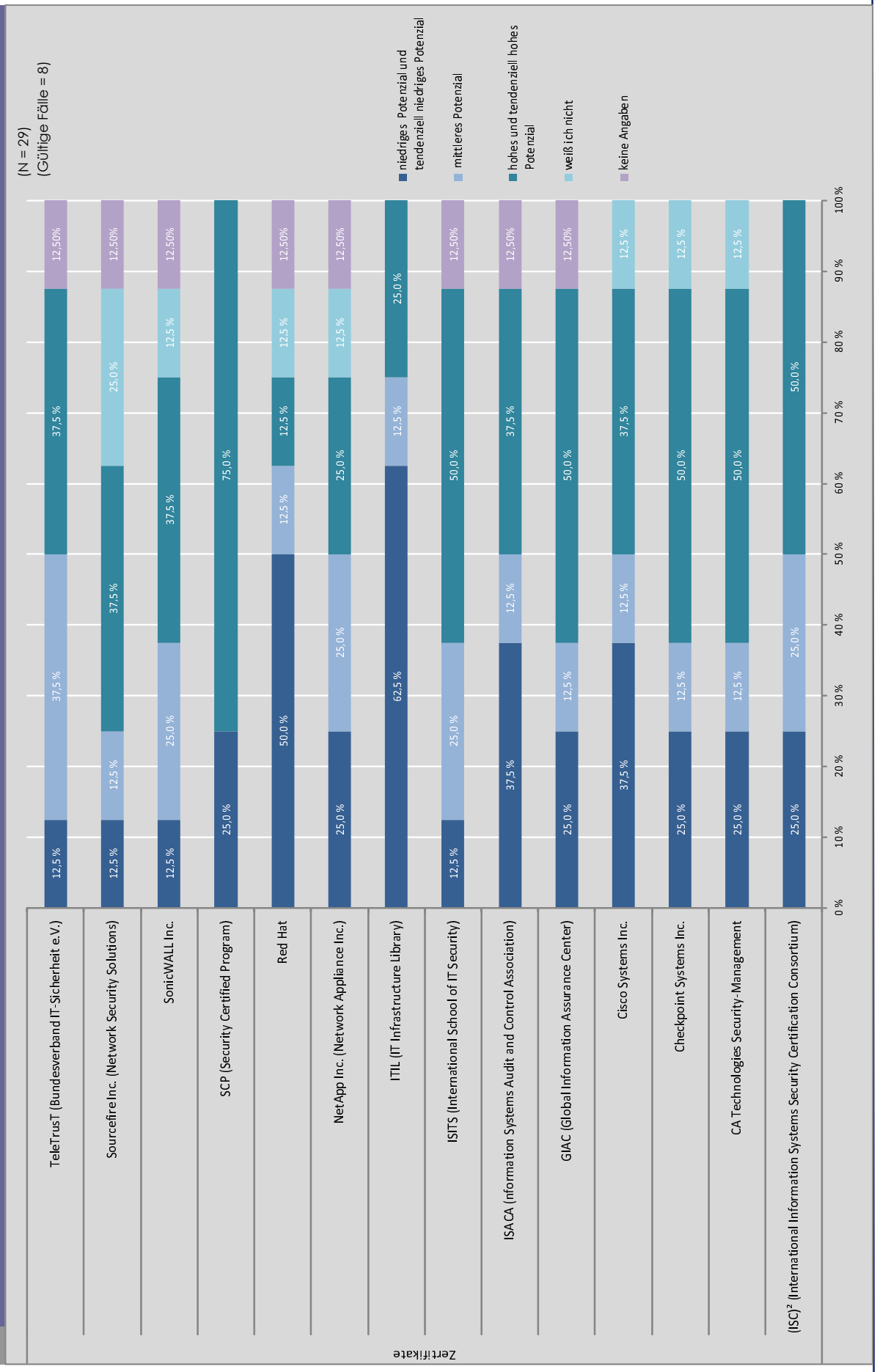
- Hohes Potenzial: das tendenziell hohe und höchste Anrechnungspotenzial wird im Vergleich bei Zertifikaten des SCP (Security Certified Program) mit 75,0 % wahrgenommen. Hohe Werte in dem Profil erreichen die Zertifikate von (ISC)² (International Information Systems Security Certification Consortium), CA Technologies Security-Management, Checkpoint Systems Inc., GIAC (Global Information Assurance Center) und ISITS (International School of IT Security) (je 50,0 %).

- Mittleres Potenzial: Mit 37,5 % wird mittleres Anrechnungspotenzial den Weiterbildungszertifikaten der TeleTrusT (Bundesverband IT-Sicherheit e.V.) zugesprochen. Es folgen (ISC)² (International Information Systems Security Certification Consortium), ISITS (International School of IT Security), NetApp Inc. (Network Appliance Inc.) und SonicWALL Inc. mit je 25,0 %.

- Niedrige Potenzials: Aus der Zusammenfassung der zwei Kategorien niedrigen beziehungsweise tendenziell niedriges Anrechnungspotenzial erreichen die Zertifikate von ITIL (IT Infrastructure Library) mit 62,5 % den höchsten Wert. Gefolgt werden sie von Red Hat mit 50,0 %, Cisco Systems Inc. und ISACA (Information Systems Audit and Control Association) (je 37,5 %). Mit je 25,0 % wird auch den Zertifikaten von (ISC)² (International Information Systems Security Certification Consortium), CA Technologies Security-Management, Checkpoint Systems Inc., GIAC (Global Information Assurance Center), NetApp Inc. (Network Appliance Inc.) und SCP (Security Certified Program) niedriges oder tendenziell niedriges Anrechnungspotenzial zugesprochen.

- Unbestimmbares Potenzial: 37,5 % gaben an, das Anrechnungspotenzial der Sourcefire Inc. (Network Security Solutions) nicht bestimmen zu können oder machten keine Angaben zu diesem Zertifikat. Insgesamt ist zudem bemerkenswert, dass bis auf die Zertifikate von (ISC)², ITIL und SCP jedes Zertifikat mindestens eine Nennung in diesen Kategorien erhielt. Dies lässt markante Informationslücken in den genannten Zertifikaten erahnen.

K16 Beurteilung Anrechnung IT-Zertifikate (in Prozent)



4.6 Persönliche Daten

Der letzte Abschnitt "Persönliche Daten" (K17 – K22) ergänzt die vorliegende Umfrage um Angaben zum Standort des Organisationshauptsitzes (K17 und K18), der Organisationsform (K19), den Tätigkeitsbereichen (K20), der Fach- und Personalverantwortung (K21) sowie der Mitarbeiteranzahl (K 22) in den Organisationen.

K17.

In welchem Land liegt ihr Organisationshauptsitz?

- □ Deutschland
- □ Österreich/Schweiz
- □ Großbritannien
- □ USA
- □ in einem anderen Land

Die überwiegende Mehrheit der Befragten - nämlich 82,4 % - gab an, ihren Organisationshauptsitz in Deutschland zu lokalisieren. Mit deutlichem Abstand liegen die Organisationshauptsitze der Befragten außerdem in Österreich oder in der Schweiz (11,8 %) und in den USA (5,9 %). Weitere Länder sind nicht vertreten.

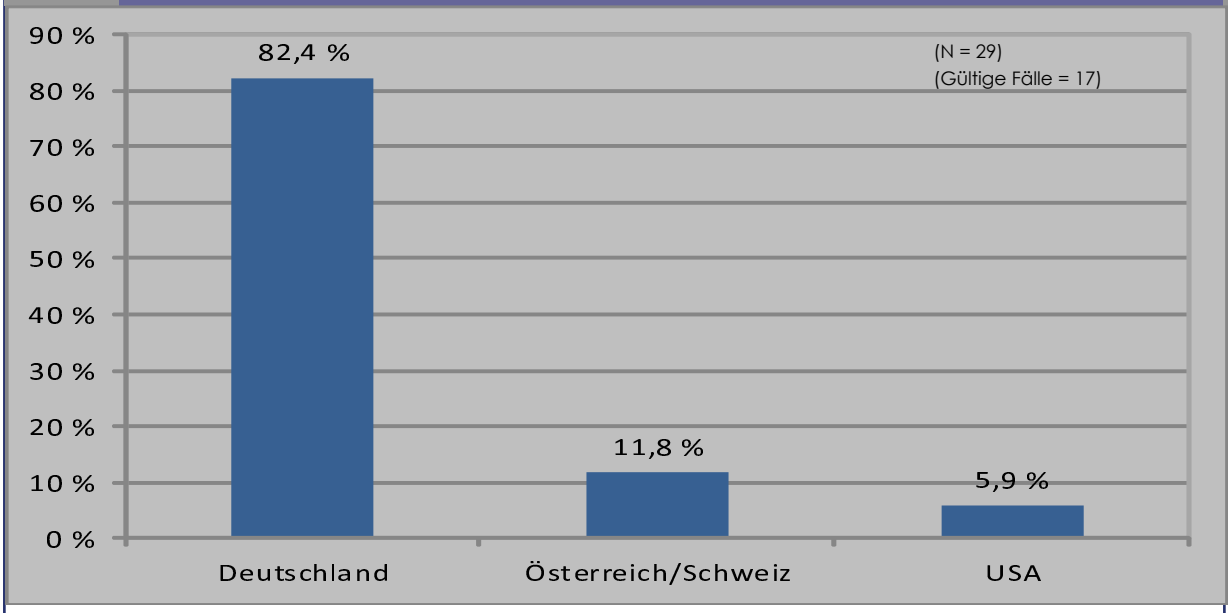
K18.

Deutschland: In welchem Bundesland liegt Ihr Organisationshauptsitz?

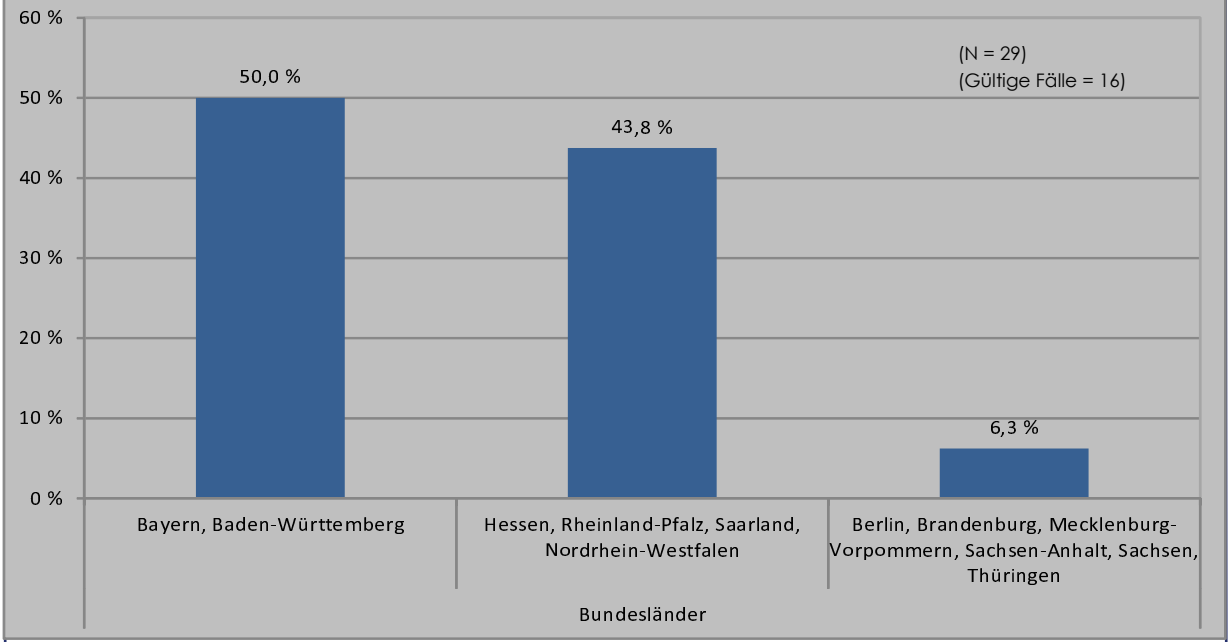
- □ Bayern, Baden-Württemberg
- □ Hessen, Rheinland-Pfalz, Saarland, Nordrhein-Westfalen
- □ Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt, Sachsen, Thüringen
- □ Schleswig-Holstein, Hamburg, Niedersachsen, Bremen

Innerhalb der Bundesrepublik Deutschland verteilen sich die Organisationshauptsitza uf die Bundesländer Bayern, Baden-Württemberg mit 50,0 % und Hessen, Rheinland-Pfalz, Saarland, Nordrhein-Westfalen (43,8 %). Schlusslicht bilden die Bundesländer Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt, Sachsen und Thüringen (6,3 %). Somit sind die Bundesländer Schleswig-Holstein, Hamburg, Niedersachsen und Bremen nicht vertreten.

K17 Oranisationshauptsitz (in Prozent)



K18 Deutschland: Sitz des Unternehmens (in Prozent)



K19.

In welcher Organisationsform sind Sie tätig?

- □ Polizei/Verband der Polizei
- □ Bundeswehr
- □ Medienunternehmen
- □ Versicherungsunternehmen
- □ Unternehmensberatung
- □ Bankwesen
- □ Hochschule/Universität
- □ Sonstige

Zusammenfassend betrachtet entstammen 81,2 % der Befragten aus dem Bereich Wirtschaft und Verwaltung sowie außerhochschulische Forschung. Der Bereich "Hochschule\Universität ist zu 18,8 % vertreten. Die Wirtschaft, Verwaltung und außerhochschulische Forschungseinrichtungen differenziert betrachtet ergibt folgende Verteilung: Die Kategorien "Polizei\Verband der Polizei" und "Unternehmensberatung" sind mit je 12,5 % vertreten. Medienunternehmen, Versicherungsunternehmen und das Bankwesen erreichen 6,3 %. Innerhalb der Kategorie "Sonstige" teilen sich die Organisationsformen: "Forschungseinrichtungen", „Industrie" und "Wirtschaftsunternehmen" zu je einem Drittel auf.

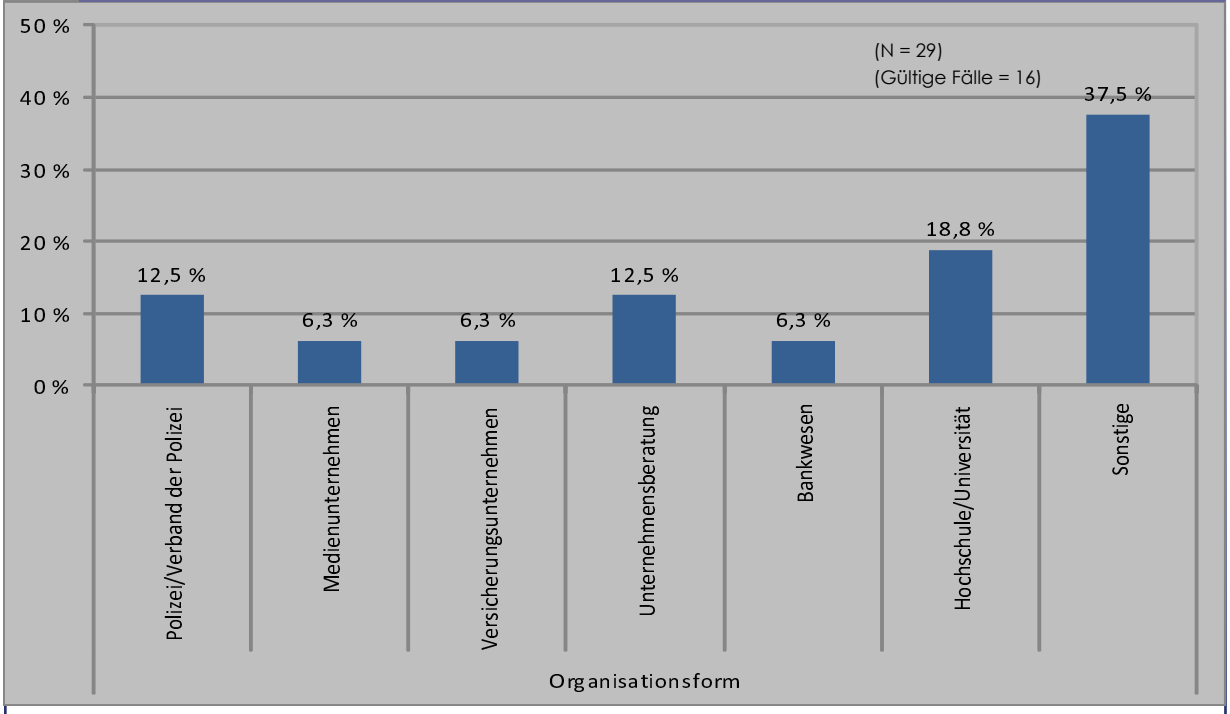
K20.

In welchem der folgenden Bereiche sind Sie beschäftigt?

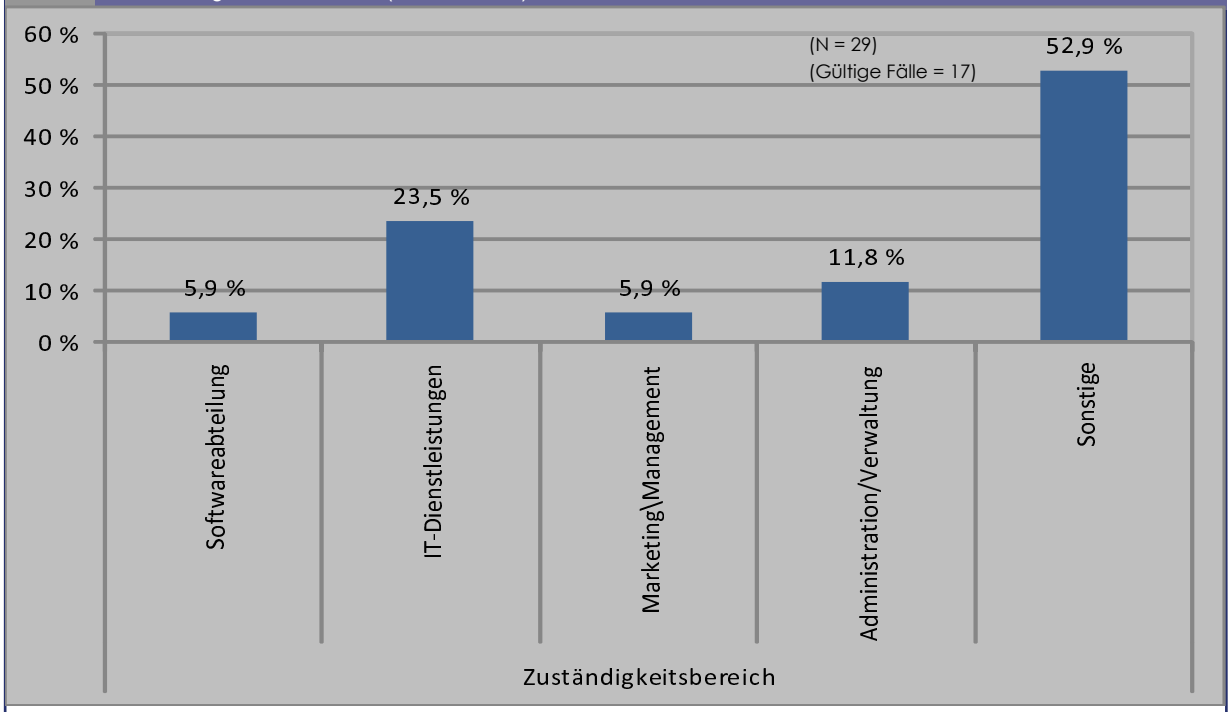
- □ Administration/Verwaltung
- □ Controlling
- □ Internet/E-Commerce
- □ IT-Dienstleistungen
- □ Marketing/Management
- □ Softwareabteilung
- □ Sonstige

Als Arbeitsbereich der Befragten überwiegen die "IT-Dienstleistungen" (23,5 %). Die "Administration/Verwaltung" erreicht 11,8 %. "Softwareabteilungen" und das "Marketing/Management" sind zu 5,9 % vertreten. Die Kategorie "Sonstige" unterteilt sich in zwei Nennungen "IT-Sicherheit" und je einer Nennung in den Bereichen: "Beratung", "Forschung/Lehre", "Frühwarnsystem", "Information Security" und "IuK-Forensik/TKÜ".

K19 Organisationsformen (in Prozent)



K20 Zuständigkeitsbereich (in Prozent)



K21.

Haben Sie in Ihrer Organisation Fach- und/oder Personalverantwortung?

- □ Personalverantwortung
- □ Fachverantwortung
- □ Fach- und Personalverantwortung
- □ Keine Fach- oder Personalverantwortung

Personalverantwortung ist den Befragten mit 5,9 % und Fachverantwortung mit 35,5 % übertragen. Weitere 47,1 % geben an sowohl Fach- als auch Personalverantwortung innezuhaben. Entsprechend geben 11,8 % an in keinem der genannten Verantwortungsbereiche tätig zu sein.

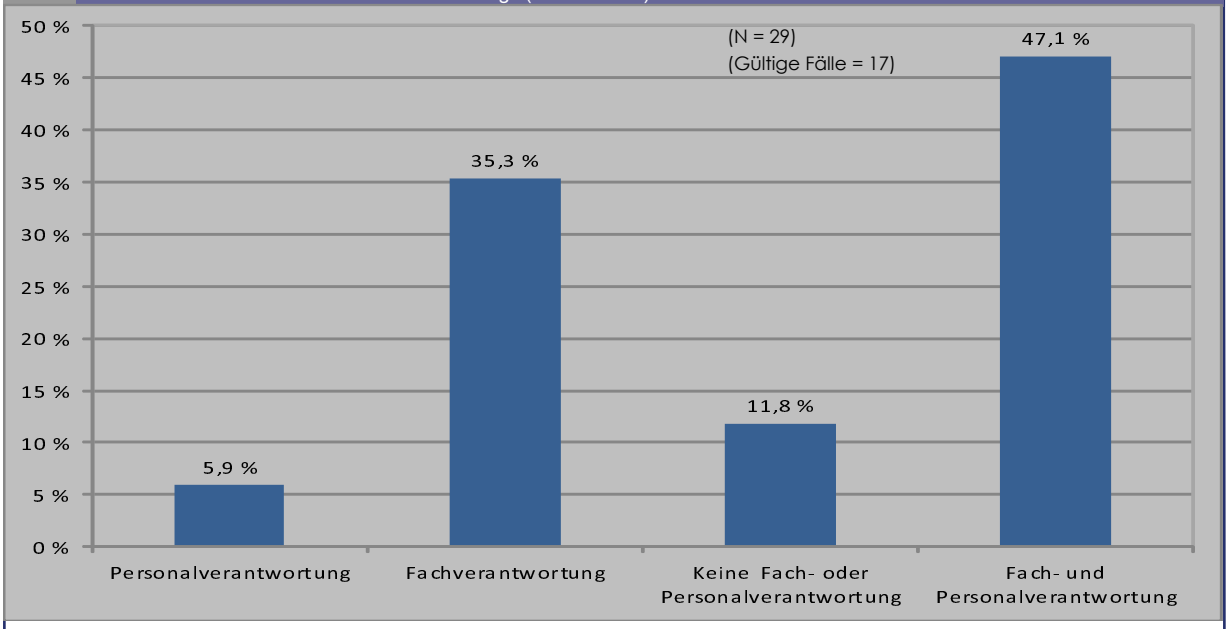
K22.

Wie viele MitarbeiterInnen gibt es schätzungsweise in Ihrer gesamten Organisation?

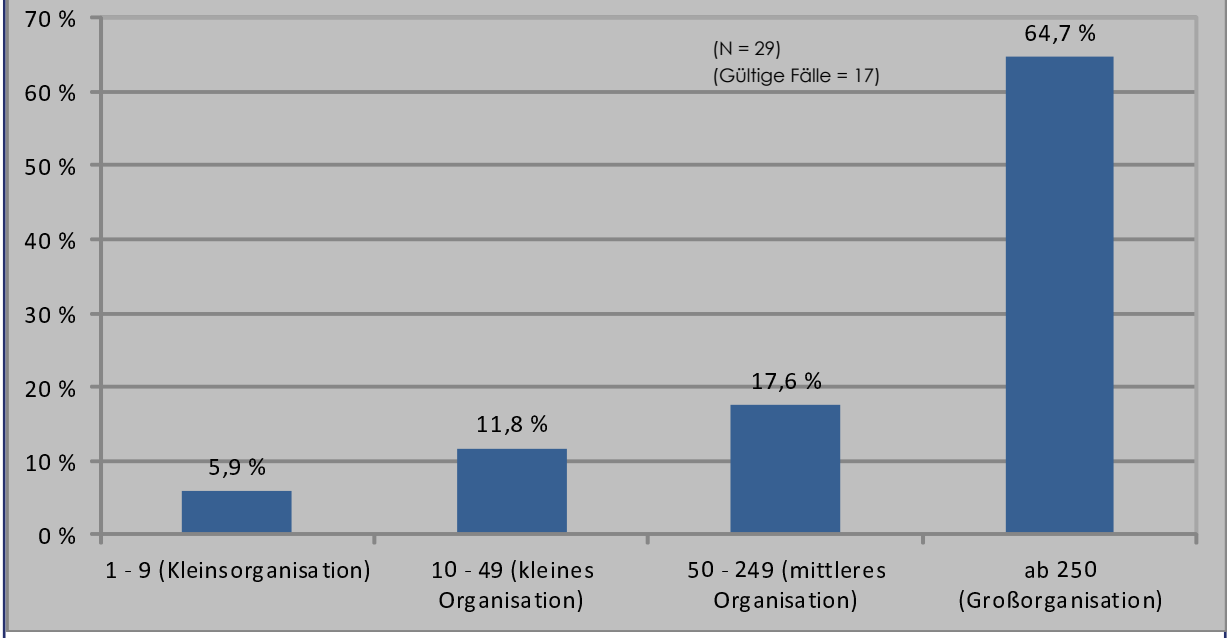
- □ 1 - 9 (Kleinstorganisation)
- □ 10 - 49 (kleine Organisation)
- □ 50 - 259 (mittlere Organisation)
- □ ab 250 (Großorganisation)
- □ weiß ich nicht

Bezüglich der Mitarbeiterzahl in den Organisationen gilt: Es überwiegen die Großorganisationen mit mehr als 250 Mitarbeitern (64,7 %). Mittlere Organisationen sind mit 17,6 % vertreten. Kleine Organisationen sowie Kleinstorganisationen erreichen mit 11,8 % beziehungsweise 5,9 % die niedrigsten Werte in der Umfrage.

K21 Fach- und/oder Personalverantwortung (in Prozent)



K22 Anzahl Mitarbeiter (in Prozent)



5. Zentrale Ergebnisse und Schlussfolgerungen

Das Spektrum der **"IT-Aus- und Weiterbildungen" (K1 - K4)** verdeutlicht einerseits, dass Beschäftigte in den befragten Organisationen sowohl staatlich geprüfte IT-Aus- und Weiterbildungen (IT-Ausbildung zu 60,0 %, Operative Professionals zu 60,0 % Strategische Professionals zu 55,0 %, IT-Spezialisten nach ISO 17024 zu 40,0 %), als auch zahlreiche IT-Weiterbildungszertifikate - insbesondere von ITIL (55,6 %) und Cisco Systems Inc. (44,4 %) - absolviert haben. Andererseits zeigt sich, dass es augenfällige Informationslücken („weiß nicht") über die Verteilung und Ausprägung der IT-Aus- und Weiterbildungen (20,0 % - 35,0 %) sowie der Weiterbildungszertifikate (27,8 % - 61,1 %) in den Organisationen gibt. In Bezug auf das Marktpotenzial im Bereich Cyber-Sicherheit kann festgehalten werden, dass ca. 75,0 % der befragten Organisationen über einen oder mehrere Mitarbeiter im Bereich Cyber-Sicherheit verfügen.

Alleine den Wirtschaftsbereich "Information und Kommunikation" betrachtet (129.303 Unternehmen in Deutschland. Quelle: Statistisches Bundesamt (2013): Unternehmensregister. Wiesbaden): Unter der Voraussetzung, dass jedes dieser Unternehmen über mindestens eine halbe Stelle für einen Cyber-Sicherheitsbeauftragen verfügt, kann ein Marktpotenzial im deutschen Weiterbildungsbereich „Cyber-Sicherheit" von rund 60.000 Personen angenommen werden.

Anknüpfend an die vorherigen Kennzahlen geht der nachfolgende Abschnitt auf den **"Bedarf an Weiterbildung" (K5 - K8)** im Bereich der Cyber-Sicherheit in den befragten Organisationen ein. Dieser Bedarf wird sowohl hinsichtlich möglicher IT-Studiengänge als auch IT-Weiterbildungszertifikate gesehen. Im Hinblick auf eine akademische IT-Weiterbildung unterteilt sich der Bedarf auf Masterstudiengänge und IT-Zertifikate mit den Schwerpunkten auf den Inhalten: "Sicherheit & Kryptographie", "Rechnernetze und verteilte Systeme" sowie "Digitale Forensik".

In der Einzelbetrachtung wird als sinnvolle **"Ausgestaltung der Weiterbildung" (K9 - K11)**, berufsbegleitende Studiengänge im Umfang von drei bis vier Jahren und Seminare von maximal 3 Monaten favorisiert. In der Gesamtbetrachtung bevorzugen die befragten Experten mit 60,0 % das Seminar vor dem Studium (40,0 %). Neben der bereits erwähnten berufsbegleitenden Organisationsform (100 %) wird als unverzichtbares Gestaltungselement der Weiterbildung auch das E-Learningseminar (73,3 %) gezählt.

Eine durchaus unterschiedliche Antwortausprägung wurde in den Abschnitten **"Anrechnung" (K12 - K13)** und **"Ausgestaltung der Anrechnung" (K14 - K16)** deutlich. Der erstgenannte Abschnitt verdeutlicht, dass rund die Hälfte der Befragten vor dem Zeitpunkt der vorliegenden Studie keine Berührungspunkte mit der Frage nach einer "Anrechnung beruflicher Kompetenzen auf Hochschulstudiengänge" hatten. Nahezu 50 % der Befragten erachten diese jedoch als "sehr sinnvoll" oder "sinnvoll". Anrechnung ist aus Sicht der Befragten mit den Zielen der "Vermeidung von Ausbildungsdopplungen", dem Fachkräftemangel und dem Bedarf der Gestaltung qualifizierter, gezielter und differenzierter Weiterbildungsformen verbunden. Anrechnungspotenzial im Hinblick auf ein Studium im Bereich Cyber-Sicherheit

wird insbesondere den Zertifikaten des SCP und (ISC)², CA Technologies Security-Management, Checkpoint Systems Inc., GIAC sowie ISITS zugesprochen.

Abgeschlossen wurde die vorliegende Studie durch den Abschnitt **"Persönliche Daten" (K17 - K22)**. Hier zeigte sich folgendes Bild: Die Mehrheit der befragten Personen gehört einer Organisation an, dessen Hauptsitz innerhalb Deutschlands (82,4 %) liegt. Es überwiegen die Großorganisationen mit mehr als 250 Mitarbeitern (64,7 %). Die Befragten entstammen zu 81,2 % aus dem Bereich Wirtschaft und Verwaltung sowie außerhochschulische Forschung und zu 18,8 % aus dem Bereich Hochschule\Universität.

6. Anhang

K1

Häufigkeiten von IT- Aus und Weiterbildung				
		Antworten		Prozent der Fälle
		N	Prozent	
Gültig	staatl. geprüfte IT-Ausbildungen (ja)	12	16,0 %	60,0 %
	staatl. geprüfte IT-Ausbildungen (nein)	2	2,7 %	10,0 %
	staatl. geprüfte IT-Ausbildungen (weiß ich nicht)	5	6,7 %	25,0 %
	IT-Spezialisten (nach ISO 17024) (ja)	8	10,7 %	40,0 %
	IT-Spezialisten (nach ISO 17024) (nein)	3	4,0 %	15,0 %
	IT-Spezialisten (nach ISO 17024) (weiß ich nicht)	7	9,3 %	35,0 %
	Operative Professionals (ja)	12	16,0 %	60,0 %
	Operative Professionals (nein)	3	4,0 %	15,0 %
	Operative Professionals (weiß ich nicht)	5	6,7 %	25,0 %
	Strategische Professionals (ja)	11	14,7 %	55,0 %
	Strategische Professionals (nein)	3	4,0 %	15,0 %
	Strategische Professionals (weiß ich nicht)	4	5,3 %	20,0 %
Gesamt		**75**	**100,0 %**	**375,0 %**
a. Dichotomie-Gruppe tabellarisch dargestellt bei Wert 1.				

K2

Häufigkeiten von Cyber-Sicherheit im Unternehmen/in der Organisation					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	1 - 3	5	17,2 %	23,8 %	23,8 %
	7 und mehr	11	37,9 %	52,4 %	76,2 %
	weiß ich nicht	3	10,3 %	14,3 %	90,5 %
	keine	2	6,9 %	9,5 %	100,0 %
	Gesamt	21	72,4 %	100,0 %	
Fehlend	-77	5	17,2 %		
	0	3	10,3 %		
	Gesamt	8	27,6 %		
Gesamt		**29**	**100,0 %**		

K3

		Antworten (N)			Prozent der Fälle			
	Häufigkeiten von Zertifikate	ja	nein	weiß ich nicht	ja	nein	weiß ich nicht	keine Angabe
Gültige	(ISC)² (International Information Systems Security Certification Consortium)	4	5	8	22,2 %	27,8 %	44,4 %	5,6 %
	CA Technologies Security-Management	2	7	8	11,1 %	38,9 %	44,4 %	5,6 %
	Checkpoint Systems Inc.	5	5	6	27,8 %	27,8 %	33,3 %	11,1 %
	Cisco Systems Inc.	8	3	7	44,4 %	16,7 %	38,9 %	0,0 %
	GIAC (Global Information Assurance Center)	2	5	10	11,1 %	27,8 %	55,6 %	5,6 %
	ISACA (Information Systems Audit and Control Association)	7	4	6	38,9 %	22,2 %	33,3 %	5,6 %
	ISITS (International School of IT Security)	1	5	11	5,6 %	27,8 %	61,1 %	5,6 %
	ITIL (IT Infrastructure Library)	10	3	5	55,6 %	16,7 %	27,8 %	0,0 %
	NetApp Inc. (Network Appliance Inc.)	4	4	8	22,2 %	22,2 %	44,4 %	11,1 %
	Red Hat	4	4	8	22,2 %	22,2 %	44,4 %	11,1 %
	SCP (Security Certified Program)	1	5	11	5,6 %	27,8 %	61,1 %	5,6 %
	SonicWALL Inc.	1	6	9	5,6 %	33,3 %	50,0 %	11,1 %
	Sourcefire Inc. (Network Security Solutions)	0	5	11	0,0 %	27,8 %	61,1 %	11,1 %
	TeleTrusT (Bundesverband IT-Sicherheit e.V.)	5	4	8	27,8 %	22,2 %	44,4 %	5,6 %
Gesamt		**54**	**65**	**116**	**300,0 %**	**361,1 %**	**644,4 %**	**94,4 %**

K4

Häufigkeiten von IT-(Security-)Zertifikate - Weitere

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	ACE, AMBCI, CISA, CISM, IEEE Certified Biometrics Professional (CBP), AccessData ACE, PSA etc.	1	3,4 %	3,4 %	86,2 %
	Google AdWords Spezialist	1	3,4 %	3,4 %	89,7 %
	ISSECO	1	3,4 %	3,4 %	93,1 %
	ISSECO Certified Professional for Secure Software Engineering Diverse Hersteller/Produktspezifische Zertitifizierungen, die hier m.E. aber nichts zu suchen haben.	1	3,4 %	3,4 %	96,6 %
	LPIC 1-3, Novell	1	3,4 %	3,4 %	100,0 %
	Gesamt	**29**	**100,0 %**	**100,0 %**	

K5

Häufigkeiten von Bedarf

		Antworten		Prozent der Fälle
		N	Prozent	
Gültig	IT-Studiengang (ja)	12	30,0 %	60,0 %
	IT-Studiengang (nein)	5	12,5 %	25,0 %
	IT-Studiengang (weiß ich nicht)	3	7,5 %	15,0 %
	IT-Weiterbildungszertifikat (ja)	13	32,5 %	65,0 %
	IT-Weiterbildungszertifikat (nein)	2	5,0 %	10,0 %
	IT-Weiterbildungszertifikat (weiß ich nicht)	5	12,5 %	25,0 %
Gesamt		**40**	**100,0 %**	**200,0 %**

a. Dichotomie-Gruppe tabellarisch dargestellt bei Wert 1.

K6

Häufigkeiten von Bedarf Weiterbildung - offen

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	fundierte Qualifikation bzgl. des technologischen Fortschritts - IT-/Forensik-Grundlagen für nicht Beamte/Tarifbeschäftigte, die keine IT-Ausbildung oder Studium haben. - Anerkennung als IT-/Forensik-Sachverständige	1	3,4 %	3,4 %	3,4 %
	Bedeutung des Themas	1	3,4 %	3,4 %	96,6 %
	Da aus unserer Sicht nur über derartige Angebote eine notwendige Fachtiefe erreicht werden kann.	1	3,4 %	3,4 %	100,0 %
	Gesamt	**29**	**100,0 %**	**100,0 %**	

K7

Häufigkeiten von Form Weiterbildung					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Masterstudium	7	24,1 %	46,7 %	46,7 %
	IT-Zertifikate	8	27,6 %	53,3 %	100,0 %
	Gesamt	15	51,7 %	100,0 %	
Fehlend	-77	14	48,3 %		
Gesamt		**29**	**100,0 %**		

K8

Häufigkeiten von Inhalte				
		Antworten		Prozent der Fälle
		N	Prozent	
Gültig	IT-Governance/ IT-Compliance	10	9,4 %	71,4 %
	IT-Revision	8	7,5 %	57,1 %
	IT-Risikomanagement	10	9,4 %	71,4 %
	Informationsmanagement	5	4,7 %	35,7 %
	IT gestützte Geschäftspro-zesse (ERP-Systeme)	3	2,8 %	21,4 %
	Strafprozessrecht/ eDiscovery	8	7,5 %	57,1 %
	Knowledge Discovery	1	0,9 %	7,1 %
	Datenmanagement/ Datenarchivierung	10	9,4 %	71,4 %
	Rechnernetze und verteilte Systeme	12	11,3 %	85,7 %
	Softwareengineering/ Qualitätsmanagement	11	10,4 %	78,6 %
	Computerlinguistik	2	1,9 %	14,3 %
	Digitale Forensik	12	11,3 %	85,7 %
	Sicherheit & Kryptographie	14	13,2 %	100,0 %
Gesamt		**106**	**100,0 %**	**757,1 %**
a. Dichotomie-Gruppe tabellarisch dargestellt bei Wert 1.				

K9

Häufigkeiten von Organistion Weiterbildung				
		Antworten		Prozent der Fälle
		N	Prozent	
Gültig	Präsenzseminare	4	8,7 %	26,7 %
	E-Learningseminare	11	23,9 %	73,3 %
	Blended Learning	6	13,0 %	40,0 %
	In Teilzeit	7	15,2 %	46,7 %
	In Vollzeit	3	6,5 %	20,0 %
	Berufsbegleitend	15	32,6 %	100,0 %
Gesamt		**46**	**100,0 %**	**306,7 %**
a. Dichotomie-Gruppe tabellarisch dargestellt bei Wert 1.				

K10

Häufigkeiten von Umfang Weiterbildung					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	1 - 2 Jahre (Studium)	2	6,9 %	13,3 %	13,3 %
	3 - 4 Jahre (Studium)	4	13,8 %	26,7 %	40,0 %
	Seminare bis maximal 3 Monate (Zertifikate)	4	13,8 %	26,7 %	66,7 %
	Seminare bis maximal 6 Monate (Zertifikate)	3	10,3 %	20,0 %	86,7 %
	Seminare bis maximal 1 Jahr (Zertifikate)	2	6,9 %	13,3 %	100,0 %
	Gesamt	15	51,7 %	100,0 %	
Fehlend	-77	14	48,3 %		
Gesamt		**29**	**100,0 %**		

K11

Häufigkeiten von ausgezeichnete IT-Ausbildung - Weiteres					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	- Forum / Plattform für den Austausch der Teilnehmer/-innen - gutes Lernmaterial für das Selbststudium	1	3,4 %	3,4 %	3,4 %
	-66	14	48,3 %	48,3 %	51,7 %
	-99	11	37,9 %	37,9 %	89,7 %
	Eine praxisnahe Qualifizierung anhand realer Beispiele sollte vermittelt werden	1	3,4 %	3,4 %	93,1 %
	Internationale Anerkennung	1	3,4 %	3,4 %	96,5 %
	Praxisbezug, hoher Level	1	3,4 %	3,4 %	100,0 %
	Gesamt	**29**	**100,0 %**	**100,0 %**	

K12

Häufigkeiten von Beschäftigung mit Anrechnung beruflicher Kompetenzen					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	ja	10	34,5 %	52,6 %	52,6 %
	nein	9	31,0 %	47,4 %	100,0 %
	Gesamt	19	65,5 %	100,0 %	
Fehlend	-77	10	34,5 %		
Gesamt		**29**	**100,0 %**		

K13

Häufigkeiten von Anrechnung beruflicher Kompetenzen sinnvoll					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	sehr sinnvoll	3	10,3 %	15,8 %	15,8 %
	sinnvoll	6	20,7 %	31,6 %	47,4 %
	ich bin unentschlossen	3	10,3 %	15,8 %	63,2 %
	nicht im Bereich IT sinnvoll	2	6,9 %	10,5 %	73,7 %
	völlig ausgeschlossen	3	10,3 %	15,8 %	89,5 %
	ich habe keine Meinung zum Thema	2	6,9 %	10,5 %	100,0 %
	Gesamt	19	65,5 %	100,0 %	
Fehlend	-77	10	34,5 %		
Gesamt		**29**	**100,0 %**		

K14

Häufigkeiten von Ziel der Anrechnung beruflicher Kompetenzen					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Vermeidung von Ausbildungsdopplungen	3	10,3 %	37,5 %	37,5 %
	Differenzierte Ausbildungen	2	6,9 %	25,0 %	62,5 %
	Fachkräftemangelabbau	2	6,9 %	25,0 %	87,5 %
	Keines der genannten	1	3,4 %	12,5 %	100,0 %
	Gesamt	8	27,6 %	100,0 %	
Fehlend	-77	20	69,0 %		
	0	1	3,4 %		
	Gesamt	21	72,4 %		
Gesamt		**29**	**100,0 %**		

K15

Häufigkeiten von Ziel Anrechnung - offen					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	- gezielte und qualifizierte Weiterbildung - Mangel geeigneter Seminarangebote im Fachbereih der Forensik	1	3,4 %	3,4 %	3,4 %
	Keine Geschenke: Anrechnung von Hochschulleistungen ok, Anrechn ung von beruflichen Leistungen schwierig ggf. mit Prüfung verbunden	1	3,4 %	3,4 %	100,0 %
	Gesamt	**29**	**100,0 %**	**100,0 %**	

K16

Häufigkeiten von Anrechnungspotenzial Zertifikate	niedriges Potenzial	<-----	--------	------->	hohes Potenzial	weiß ich nicht
	Anzahl	Anzahl	Anzahl	Anzahl	Anzahl	Anzahl
(ISC)² (International Information Systems Security Certification Consortium)	2	0	2	2	2	0
CA Technologies Security-Management	2	0	1	0	4	1
Checkpoint Systems Inc.	2	0	1	1	3	1
Cisco Systems Inc.	3	0	1	1	2	1
GIAC (Global Information Assurance Center)	0	2	1	0	4	0
ISACA (nformation Systems Audit and Control Association)	1	2	1	2	1	0
ISITS (International School of IT Security)	0	1	2	1	3	0
ITIL (IT Infrastructure Library)	1	4	1	1	1	0
NetApp Inc. (Network Appliance Inc.)	2	0	2	0	2	1
Red Hat	3	1	1	0	1	1
SCP (Security Certified Program)	1	1	0	1	5	0
SonicWALL Inc.	1	0	2	0	3	1
Sourcefire Inc. (Network Security Solutions)	1	0	1	1	2	2
TeleTrusT (Bundesverband IT-Sicherheit e.V.)	0	1	3	1	2	0
Gesamt	**19**	**12**	**19**	**11**	**35**	**8**

K17

Häufigkeiten von Sitz des Unternehmens bzw. Organisation					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Deutschland	14	48,3 %	82,4 %	82,4 %
	Österreich/Schweiz	2	6,9 %	11,8 %	94,1 %
	USA	1	3,4 %	5,9 %	100,0 %
	Gesamt	17	58,6 %	100,0 %	
Fehlend	-77	11	37,9 %		
	0	1	3,4 %		
	Gesamt	12	41,4 %		
Gesamt		**29**	**100%**		

K18

Häufigkeiten von Deutschland: Sitz des Unternehmens bzw. Organisation Deutschland					
		Häufigkeit	Prozent	Gültige	Kumulierte Prozente
Gültig	Bayern, Baden-Württemberg	8	27,6 %	50,0 %	50,0 %
	Hessen, Rheinland-Pfalz, Saarland, Nordrhein-Westfalen	7	24,1 %	43,8 %	93,8 %
	Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt	1	3,4 %	6,3 %	100,0 %
	Gesamt	16	55,2 %	100,0 %	
Fehlend	-77	11	37,9 %		
	0	2	6,9 %		
	Gesamt	13	44,8 %		
Gesamt		**29**	**100,0 %**		

K19

Häufigkeiten von Organisationsform					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Polizei/Verband der Polizei	2	6,9 %	12,5 %	12,5 %
	Medienunternehmen	1	3,4 %	6,3 %	18,8 %
	Versicherungsunternehmen	1	3,4 %	6,3 %	25,0 %
	Unternehmensberatung	2	6,9 %	12,5 %	37,5 %
	Bankwesen	1	3,4 %	6,3 %	43,8 %
	Hochschule/Universität	3	10,3 %	18,8 %	62,5 %
	Sonstige	6	20,7 %	37,5 %	100,0 %
	Gesamt	16	55,2 %	100,0 %	
Fehlend	-77	11	37,9 %		
	0	2	6,9 %		
	Gesamt	13	44,8 %		
Gesamt		**29**	**100,0 %**		

Häufigkeiten von Organisationsform - Sonstige		
		Häufigkeit
Gültig	Forschungseinrichtung	33,3 %
	Industrie	33,3 %
	Wirtschaftsunternehmen	33,3 %
	Gesamt	**100 %**

K20

Häufigkeiten von Zuständigkeitsbereich					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Softwareabteilung	1	3,4 %	5,9 %	5,9 %
	IT-Dienstleistungen	4	13,8 %	23,5 %	29,4 %
	Marketing\Management	1	3,4 %	5,9 %	35,3 %
	Administration/Verwal-tung	2	6,9 %	11,8 %	47,1 %
	Sonstige	9	31,0 %	52,9 %	100,0 %
	Gesamt	17	58,6 %	100,0 %	
Fehlend	-77	11	37,9 %		
	0	1	3,4 %		
	Gesamt	12	41,4 %		
Gesamt		**29**	**100,0 %**		

Häufigkeiten von Sonstige		
		Häufigkeit
Gültig	Beratung	14,3 %
	Forschung, Lehre	14,3 %
	Frühwarnsystem	14,3 %
	Informatin Security	14,3 %
	IT-Sicherheit	28,6 %
	IuK-Forensik / TKÜ	14,3 %
	Gesamt	**100,0 %**

K21

Häufigkeiten von Fach- und/oder Personalverantwortung					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Personalverantwortung	1	3,4 %	5,9 %	5,9 %
	Fachverantwortung	6	20,7 %	35,3 %	41,2 %
	Keine Fach- oder Personalverantwortung	2	6,9 %	11,8 %	52,9 %
	Fach- und Personalverantwortung	8	27,6 %	47,1 %	100,0 %
	Gesamt	17	58,6 %	100,0 %	
Fehlend	-77	11	37,9 %		
	0	1	3,4 %		
	Gesamt	12	41,4 %		
Gesamt		**29**	**100,0 %**		

K22

Häufigkeiten von Anzahl MitarbeiterInnen					
		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	1 - 9 (Kleinsorganisation)	1	3,4 %	5,9 %	5,9 %
	10 - 49 (kleines Organisation)	2	6,9 %	11,8 %	17,6 %
	50 - 249 (mittleres Organisation)	3	10,3 %	17,6 %	35,3 %
	ab 250 (Großorganisation)	11	37,9 %	64,7 %	100,0 %
	Gesamt	17	58,6 %	100,0 %	
Fehlend	-77	11	37,9 %		
	0	1	3,4 %		
	Gesamt	12	41,4 %		
Gesamt		**29**	**100,0 %**		