Studie Informationssicherheit in Deutschland, Österreich und der Schweiz 2015

Philipp Reisinger – is131510@fhstp.ac.at

Inhalt

- Einführung
- Wichtigste Ergebnisse
- Ergebnisse Gesamt
- Ergebnisse länderspezifisch
- Hypothesen
- Weitere Informationen

/informatik & security /fh/// st.pölten

Überblick, **Ziele**, **Key Facts** und **Aufbau**

EINFÜHRUNG

Überblick

/informatik & security /fh/// st.pölten

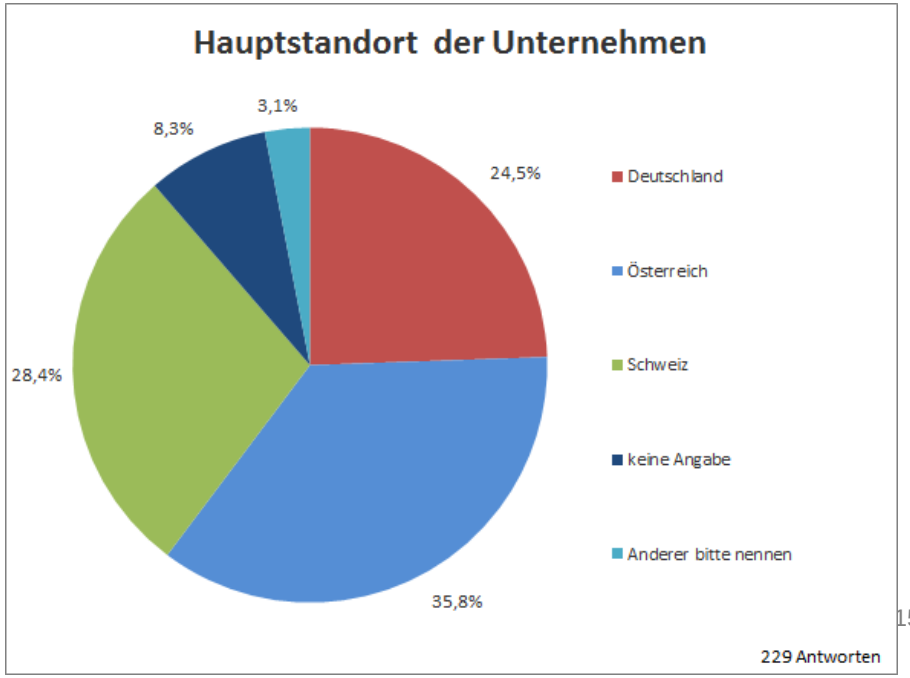
- **Studie** zum Thema **Informationssicherheit** in **Deutschland**, **Österreich** und der **Schweiz**
- **Einschränkung**
  - viele **Teilnehmer** mit **höherem Bewusstsein** und **Interesse** für das Thema der **Informationssicherheit** & **besser aufgestellt** als ein „**typisches durchschnittliches Unternehmen**“
  - **keine Anspruch** auf **Repräsentativität**
  - **Gesamtsituation** Informationssicherheit in Deutschland, Österreich und der Schweiz könnte „**anders**“ bzw. „**schlechter**“ sein, als hier nahegelegt wird
  - aktuelle **Informationssicherheitssituation** kann jedoch **zumindest** in Bezug auf die **teilnehmenden Unternehmen beschrieben werden**

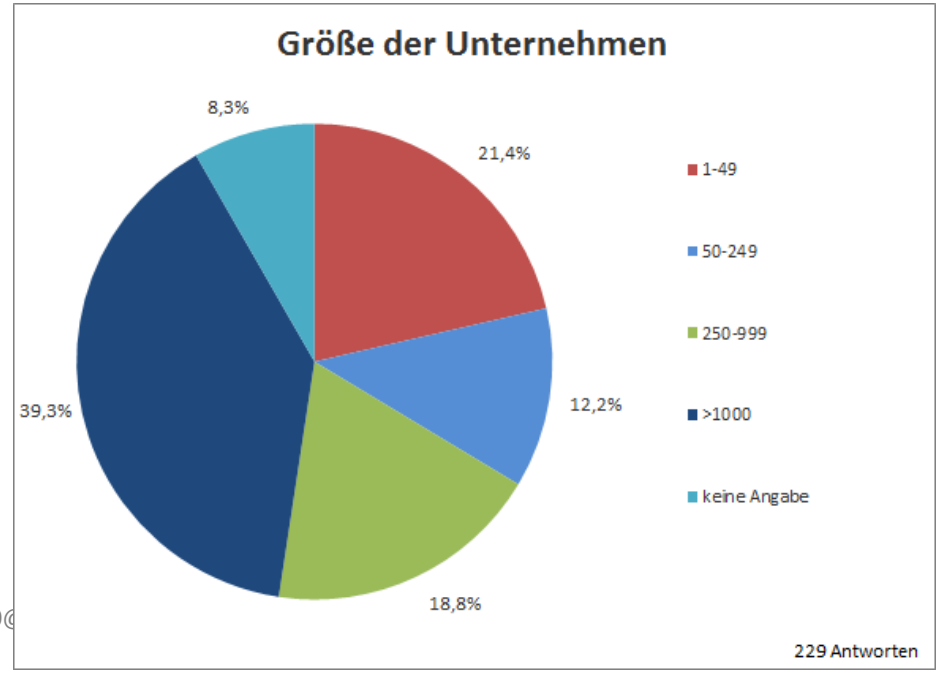
Ziele

- **Aktuelle Zahlen** zur Informationssicherheit
- **Bewusstsein** in Unternehmen in Bezug auf Informationssicherheit erheben
  - was ist deren **Stellenwert**
  - eigene Einschätzung der Unternehmen zu **Nutzung** und **Abhängigkeit** von IT und Daten
  - derzeitige **Situation** beschreiben
- **Technische** und **organisatorische Aufstellung** untersuchen
  - derzeit **umgesetzte Maßnahmen** (bzw. Tools, Systeme, Prozesse)
  - in **Planung** befindliche Maßnahmen
- Untersuchung diverser **Trendthemen**
  - APTs, NSA-Enthüllungen, Nutzung Open Source Software etc.

Key Facts und Aufbau

- Online Umfrage (surveymonkey.com)
- Ende Februar - Mai 2015
- 229 Teilnehmer
  - 56 Deutschland, 82 Österreich, 65 Schweiz, 19 k. A., 7 anderes Land





Key Facts und Aufbau

/informatik & security /fh/// st.pölten

- **5 Teilbereiche**
  I. **Wichtigkeit** der **Informationssicherheit**, **Abhängigkeit** von **IT** & **Informationen** bzw. Daten
  II. Gründe und Motivation für Informationssicherheit, Bedrohungen, Nutzung von Standards
  III. **Aktuelle Situation** im Unternehmen - Informationssicherheits-Policy, Richtlinien, Evaluierung der Informationssicherheit, Beratung, Vorfälle
  IV. „**Trendthemen**“ - mobile Geräte, Cloud & Outsourcing, Mitarbeiter-Awareness, Open Source Software, APT, NSA-Enthüllungen
  V. **Technische** und **organisatorische Aufstellung** der Unternehmen

/informatik & security /fh/// st.pölten

Allgemein wichtige Themen, **technische** und **organisatorische Maßnahmen**

WICHTIGSTE ERGEBNISSE

Wichtigste Ergebnisse

- **Informationssicherheit** für den Großteil der teilnehmenden Unternehmen von **großer bis sehr großer Bedeutung**
  - Für 35% ist Informationssicherheit „**sehr wichtig**“ und in allen wesentlichen Geschäftsprozessen ein definierter, integraler Bestandteil
  - 40% Informationssicherheit ein „**wichtiges**“ Thema, für welches eine dedizierte Rolle verantwortlich ist
- große Mehrheit ist sich der **Wichtigkeit** von korrekten **Daten und Informationen** sowie der **Abhängigkeit** von der **eigenen IT** bewusst
  - 89% der Unternehmen „**sehr stark**“ oder „**stark**“ von der eigenen **IT abhängig**, Ausfall von Kernsystemen für wenige Stunden oder einen Tag → Kerngeschäft würde stark negativ beeinträchtigt oder unmöglich gemacht

Wichtigste Ergebnisse

/informatik & security /fh/// st.pölten

- 89% der Unternehmen, im letzten Jahr von zumindest einem **Vorfall** im **Bereich der Informationssicherheit** betroffen
  - Malware (Viren, Trojaner, Spyware etc.) 54%, Spam 46%, Fahrlässigkeit von Mitarbeitern 28%, Hardware- oder Software-Fehler 28%, Stromausfälle 25%, (Spear)Phishing 21%
  - Hacking oder D(DOS) nur relativ wenige Unternehmen konfrontiert (9% bzw. 15%)
  - **nur 11%** im vergangenen Jahr von **keinen Vorfällen** betroffen
- **Gründe** für Informationssicherheit
  - **Gesetzliche Vorgaben/Compliance** 80%, **Vermeidung** von (Geld/Image)**Verlusten** durch Sicherheitsvorfälle bzw. Datenpannen 71%, Vorbeugung von Datenverlusten/Verfälschung 69%, **starke Abhängigkei**t von eigener IT in gewissen Geschäftsprozessen

Wichtigste Ergebnisse

/informatik & security /fh/// st.pölten

- Open Source Software
  - lediglich 12% der Unternehmen **keine Nutzung, ein einziges** Unternehmen **keine Nutzung aufgrund** von **Sicherheitsbedenken**
  - **Mehrheit** von 58% der Unternehmen setzten Open Source Software ein, jedoch **ohne** eine **(Sicherheits-)Überprüfung** dieser durchzuführen.
  - knappe **ein Viertel** nutzt Open Source Software und traf dabei **Maßnahmen** wie Durchführung von Code Reviews oder Recherche zu Auditergebnissen, Sicherheitsanalysen und dem Entwicklerkreis, um deren **Sicherheit, Qualität** und **Vertrauenswürdigkeit zu überprüfen**
  - **Achtung**: 12% keine Nutzung relativ hoch (div OSS Bibliotheken, auch in kommerziellen Produkten eingesetzt. Ev. keine Bewusstsein?)
  - **Achtung:** 25% Überprüfung relativ hoch. Nur exemplarische Liste. Wahrscheinlich nicht alle Maßnahmen getroffen.

Wichtigste Ergebnisse

/informatik & security /fh/// st.pölten

- APTs - Advanced Persistent Threats
  - knapp **mehr als die Hälfte (56%)** waren im letzten Jahr **nicht Ziel** eines komplexen, fortgeschrittenen, direkt auf sie gezielten IT-Angriffs
  - **25%** konnten auf diese Frage nur mit „**weiß nicht**" antworten
  - 5% zumindest **Verdacht** bezüglich des Auftretens eines APTs
  - Lediglich ca. **12%** erklärten, dass sie im vergangenen Jahr Ziel eines APTs waren, wobei nur bei einer **Minderheit** durch diesen auch **tatsächlich ein Schaden** entstand (9% erfolgreich abgewehrt, 3% Schaden entstanden)
  - **Achtung**: APTs **komplex**, **schwer** zu **identifizieren** bzw. **nachzuweisen.** Knapp **ein Drittel Unsicherheit** bzw. **Unwissenheit** bezüglich des Auftretens eines APT (26% „weiß nicht“ + 6% „Verdacht“).

Wichtigste Ergebnisse

- NSA-Enthüllungen
  - für knapp 40% der Unternehmen **kein Thema**
  - für 37% der Unternehmen ein Thema und eine **wachsende Beachtung** des Themas der **Informationssicherheit**
  - 17% zwar ein Thema, jedoch wurden **keine gezielten Maßnahmen** ergriffen
  - **Maßnahmen:** verstärkter Einsatz von **Verschlüsselung** 16%, Achtsamkeit - im Fall von **Cloud oder Outsourcing** wird verstärkt auf **heimische/europäische Anbieter** gesetzt 16%, Planung zur verstärkten **Beschaffung** von IT Made in Austria/Germany/Switzerland bzw. Europe 9%.
  - auf diese Enthüllungen folgende Erhöhung des IT-Sicherheitsbudgets wurde lediglich von 2% der Unternehmen genannt

Wichtigste Ergebnisse

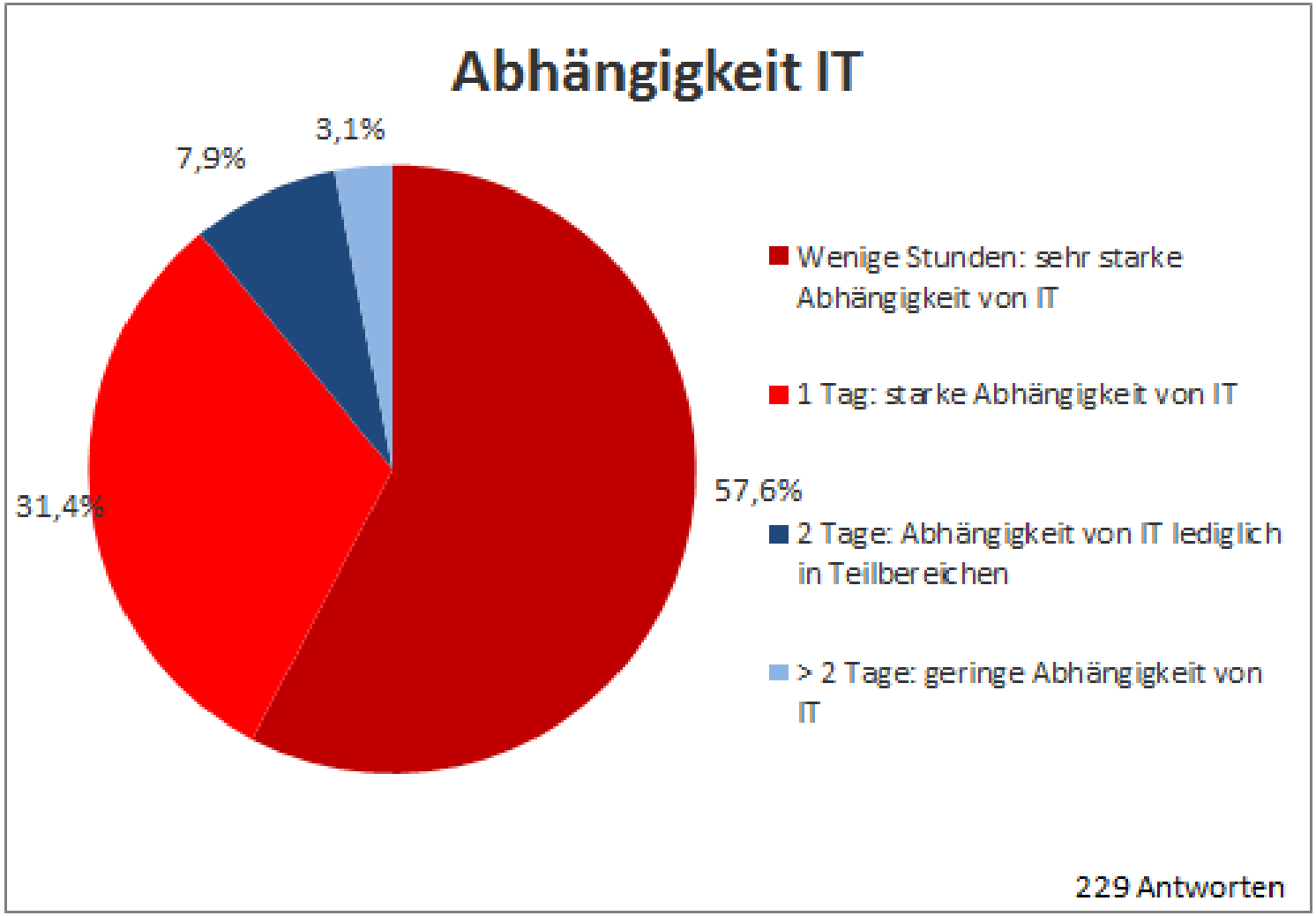
- **Grundlegende technische** und **organisatorische Maßnahmen** wie
  - Firewalls, Virenschutz, Backupsoftware, Spamschutz sowie Medien und Datenvernichtung oder Patch- und Updatemanagement **beinahe durchgängig** vorhanden
- **Weiterreichende Maßnahmen gespaltenes Bild** mit teilweise schnell sinkendem Implementierungsgrad
  - IDS/IPS, Layer 2 Netzwerksicherheit, PKI, Web Content Filtering, Vulnerability Management, Change Management, Identitäts- und Zugriffsmanagement
- Verschiedene **komplexe und aufwändige Maßnahmen** wie
  - DLP, SIEM, Versicherung gegen Cyber-Angriffe, Betrieb eines IKS inklusive IT-Kontrollen oder firmeneigenes CERT sind nur bei einer **Minderheit der Unternehmen** umgesetzt.

/informatik & security /fh/// st.pölten

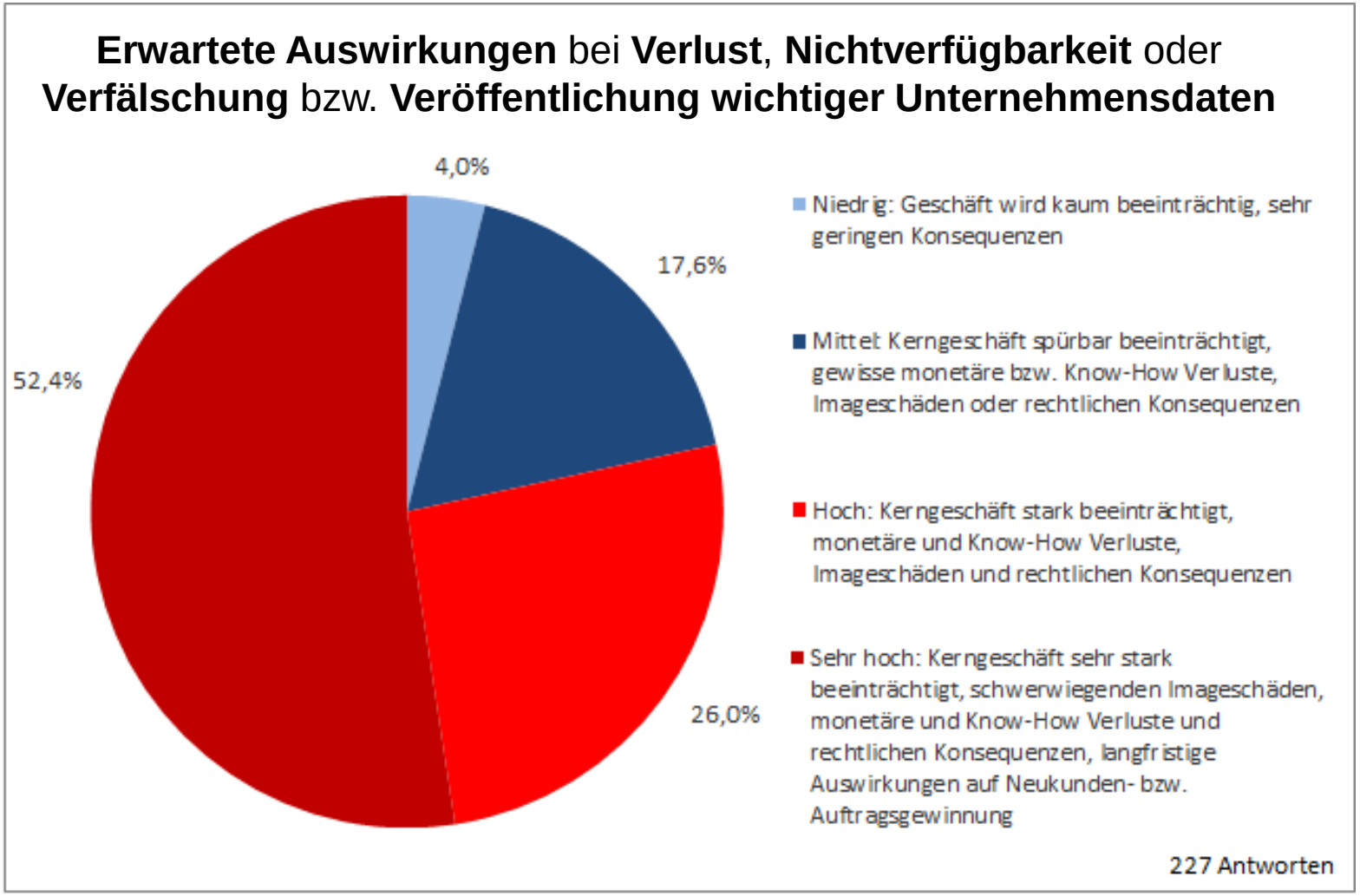
Wichtigkeit der **Informationssicherheit**, **Abhängigkeit** von **IT** & **Informationen** bzw. Daten

ERGEBNISSE GESAMT I

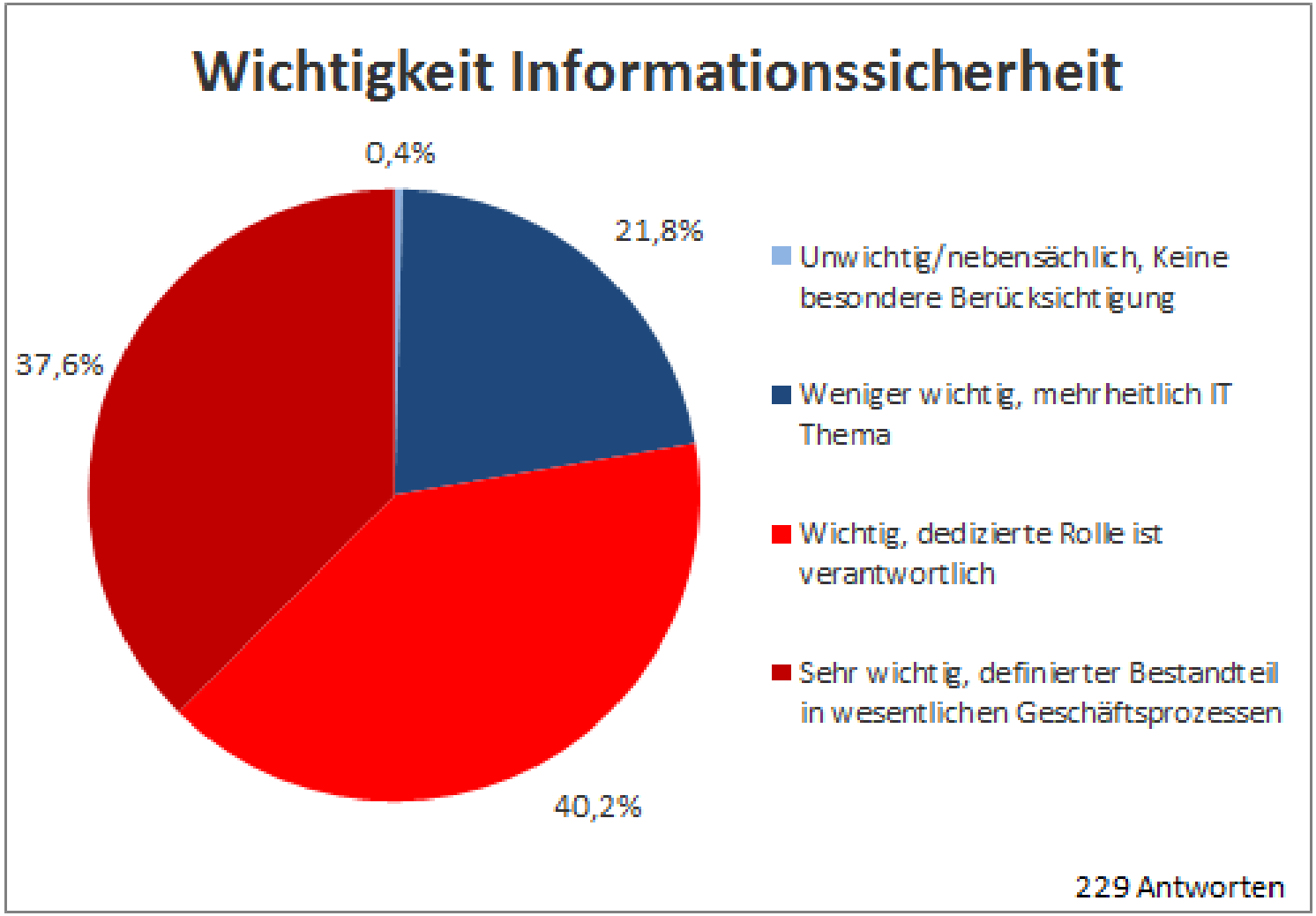
Ergebnisse Gesamt I



Ergebnisse Gesamt I



Ergebnisse Gesamt I

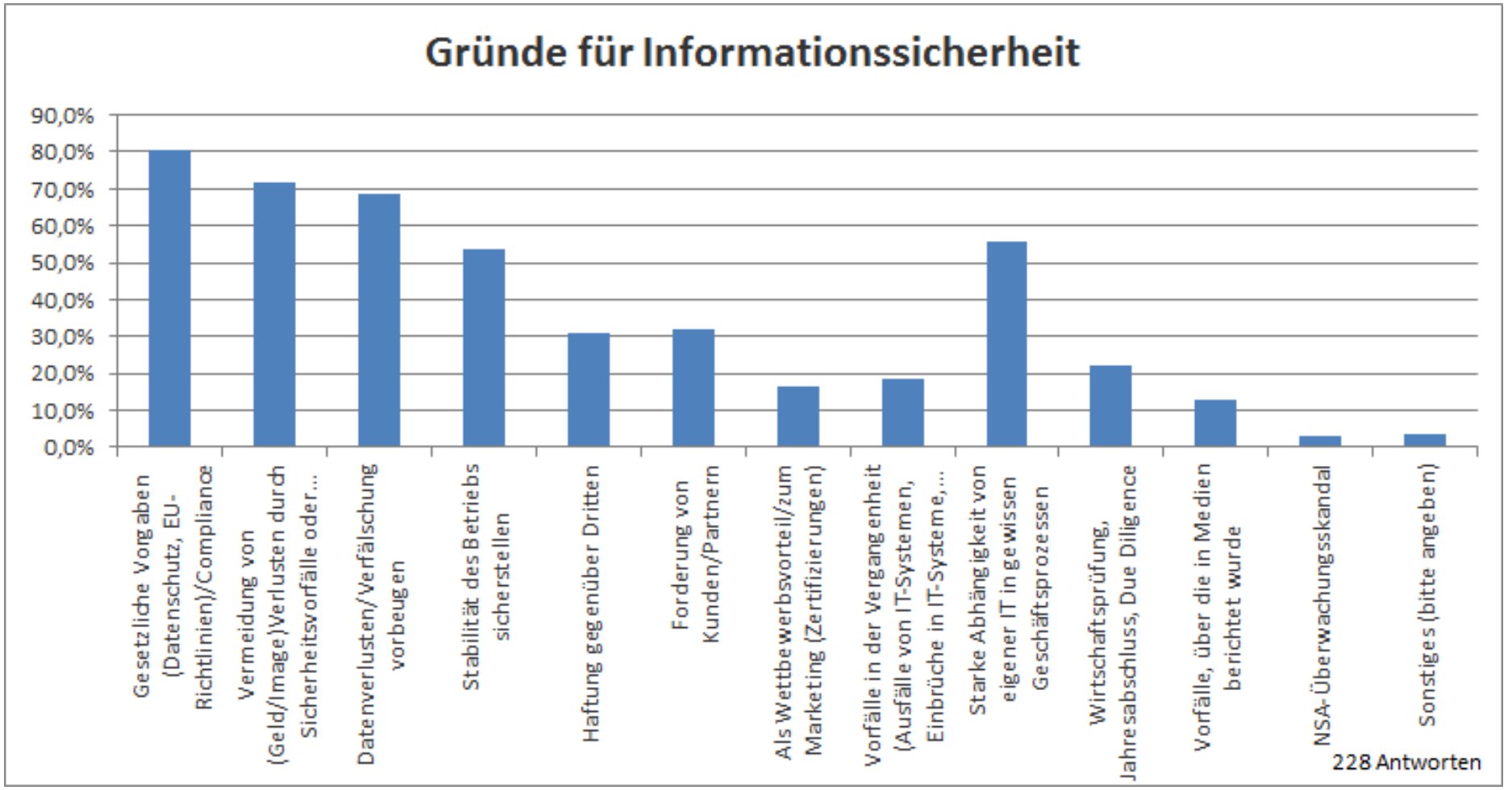


/informatik & security /fh/// st.pölten

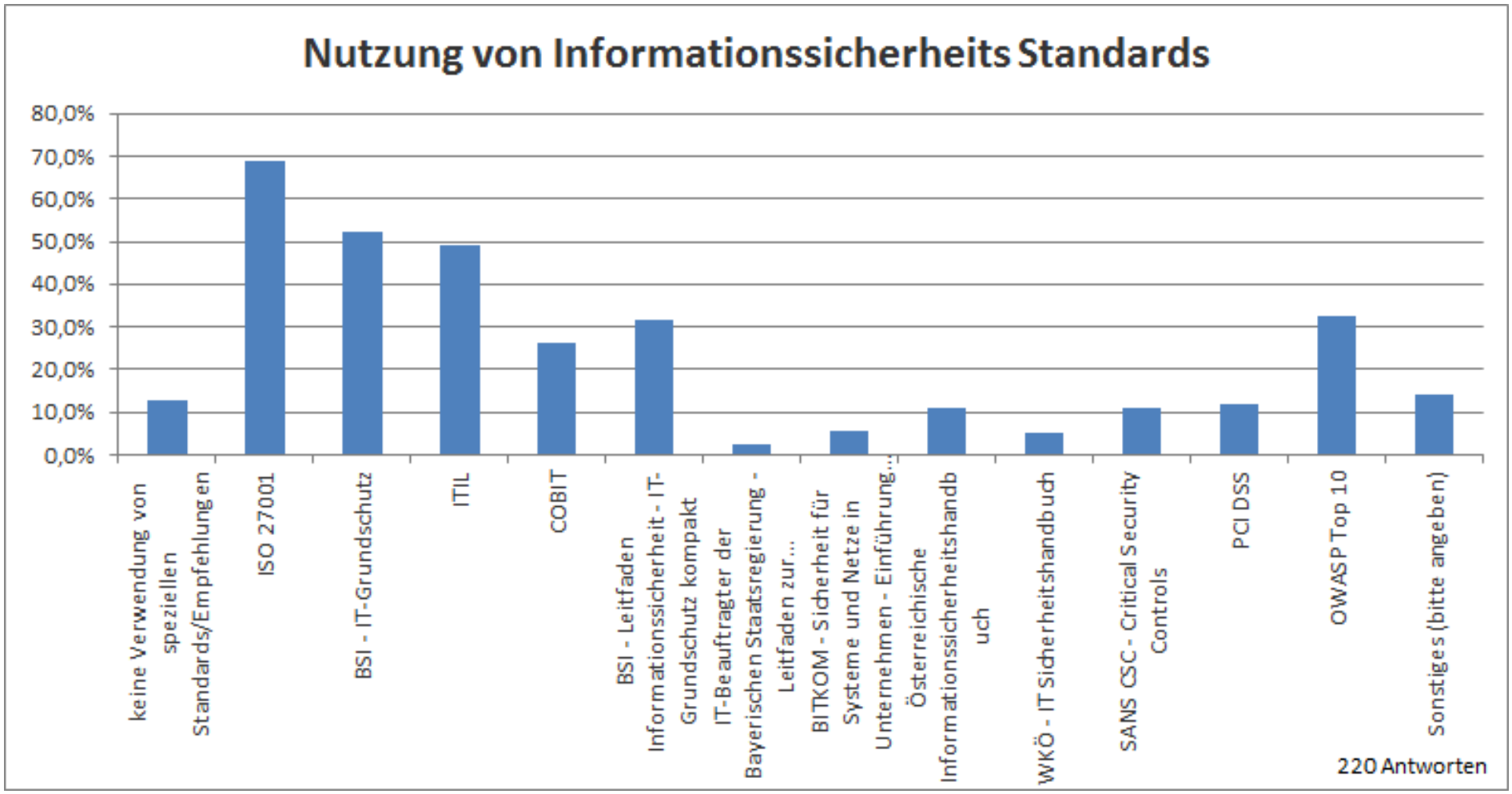
Gründe und **Motivation** für **Informationssicherheit, Bedrohungen, Nutzung** von **Standards**

ERGEBNISSE GESAMT II

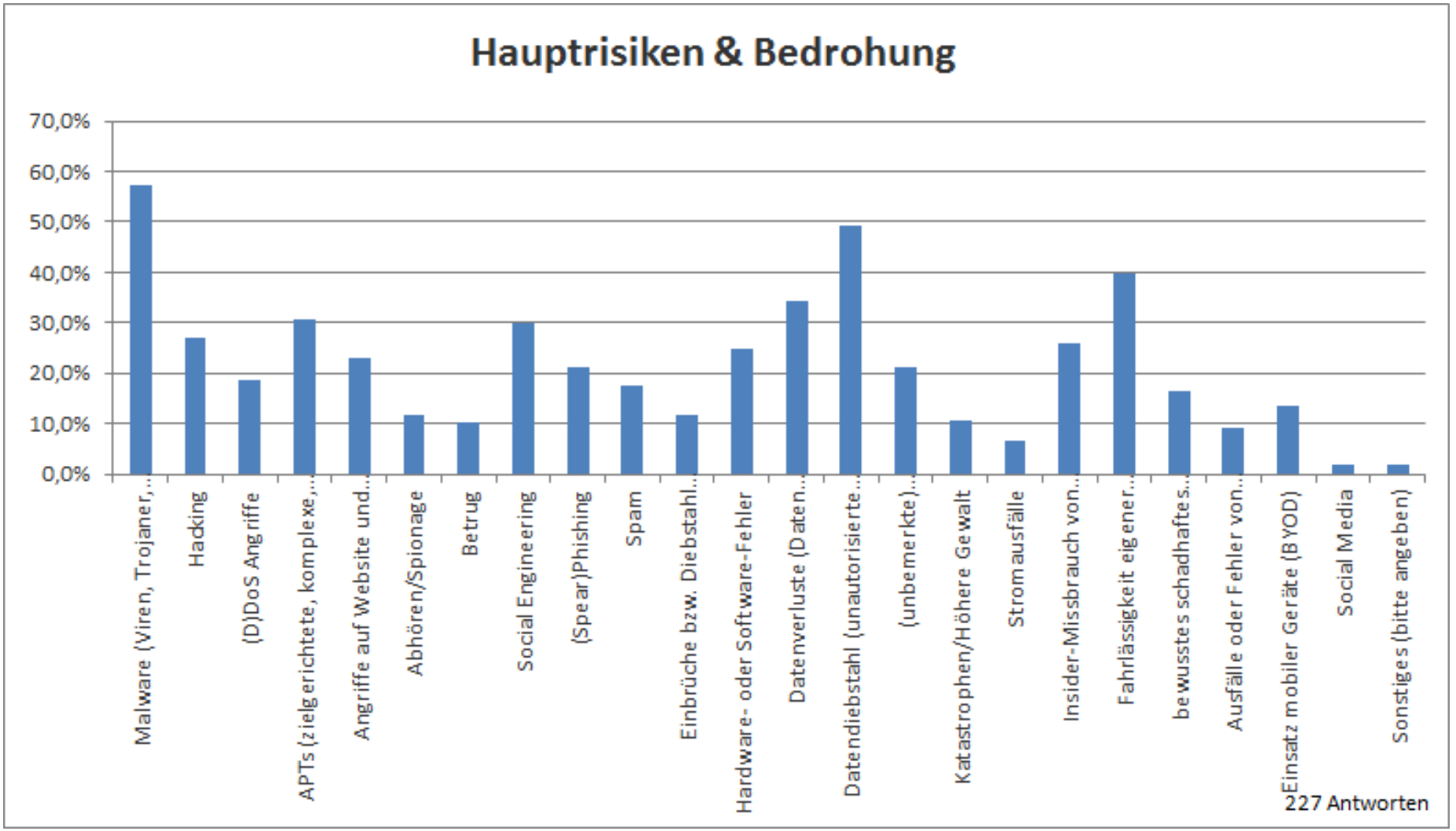
Ergebnisse Gesamt II



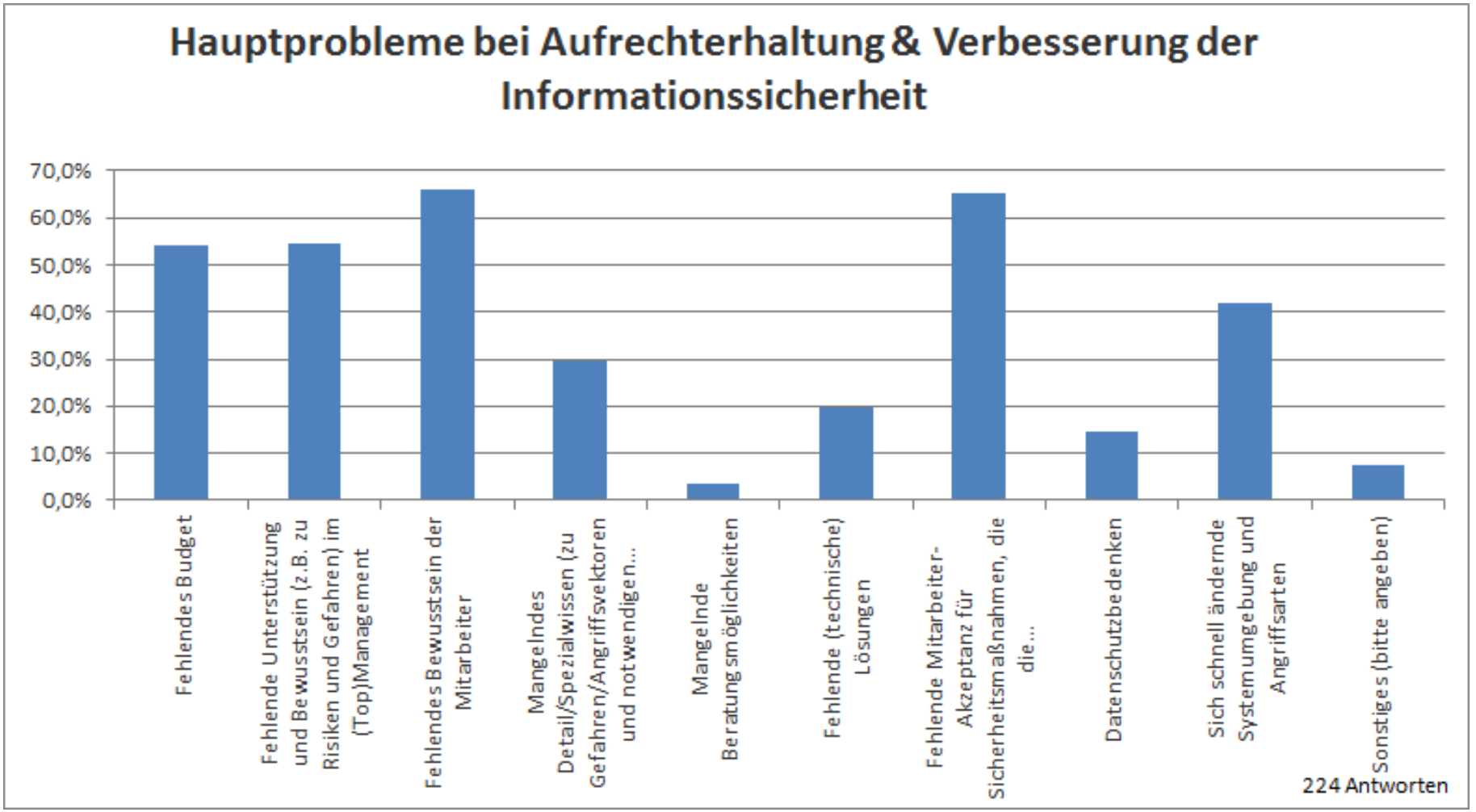
Ergebnisse Gesamt II



Ergebnisse Gesamt II



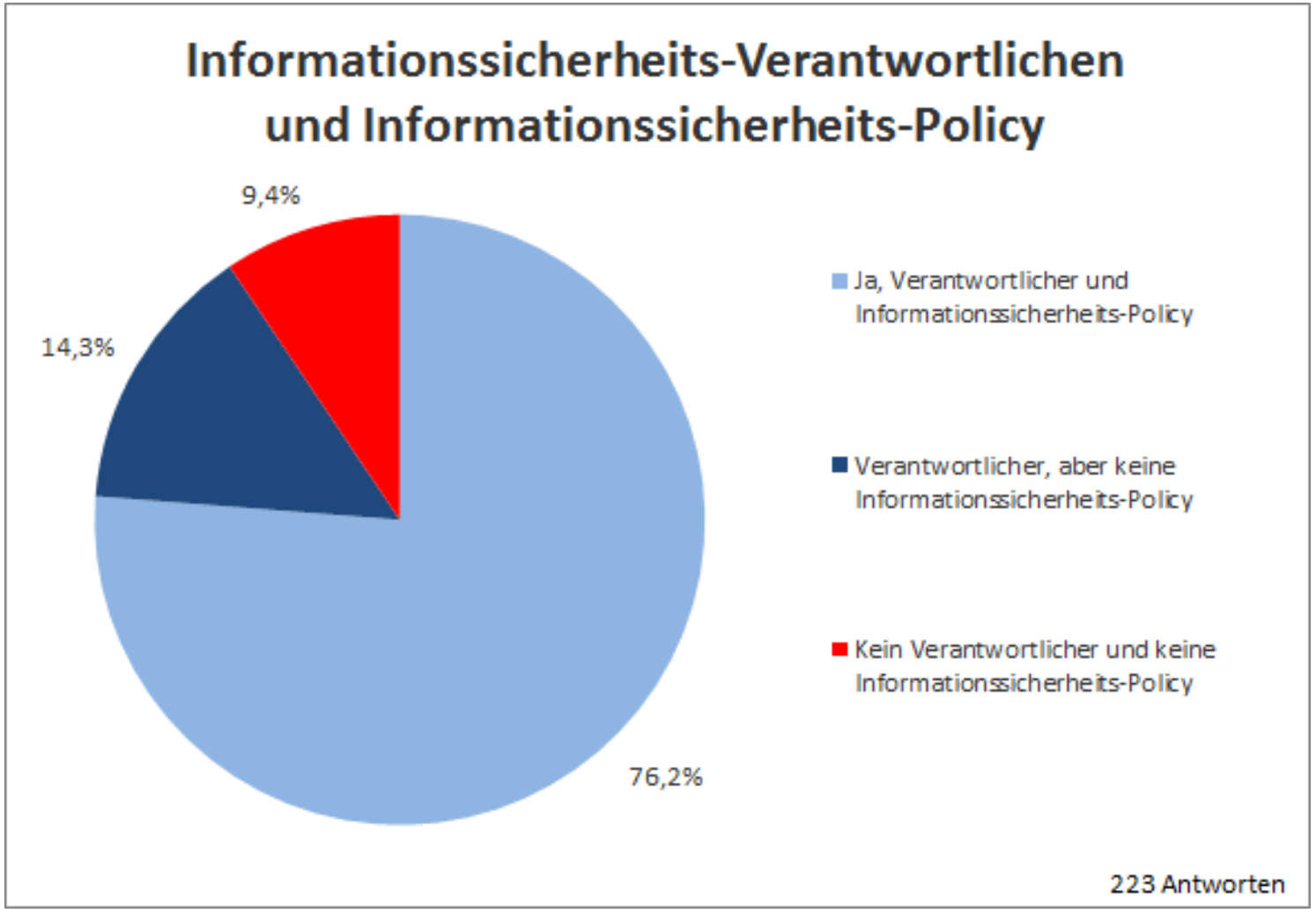
Ergebnisse Gesamt II



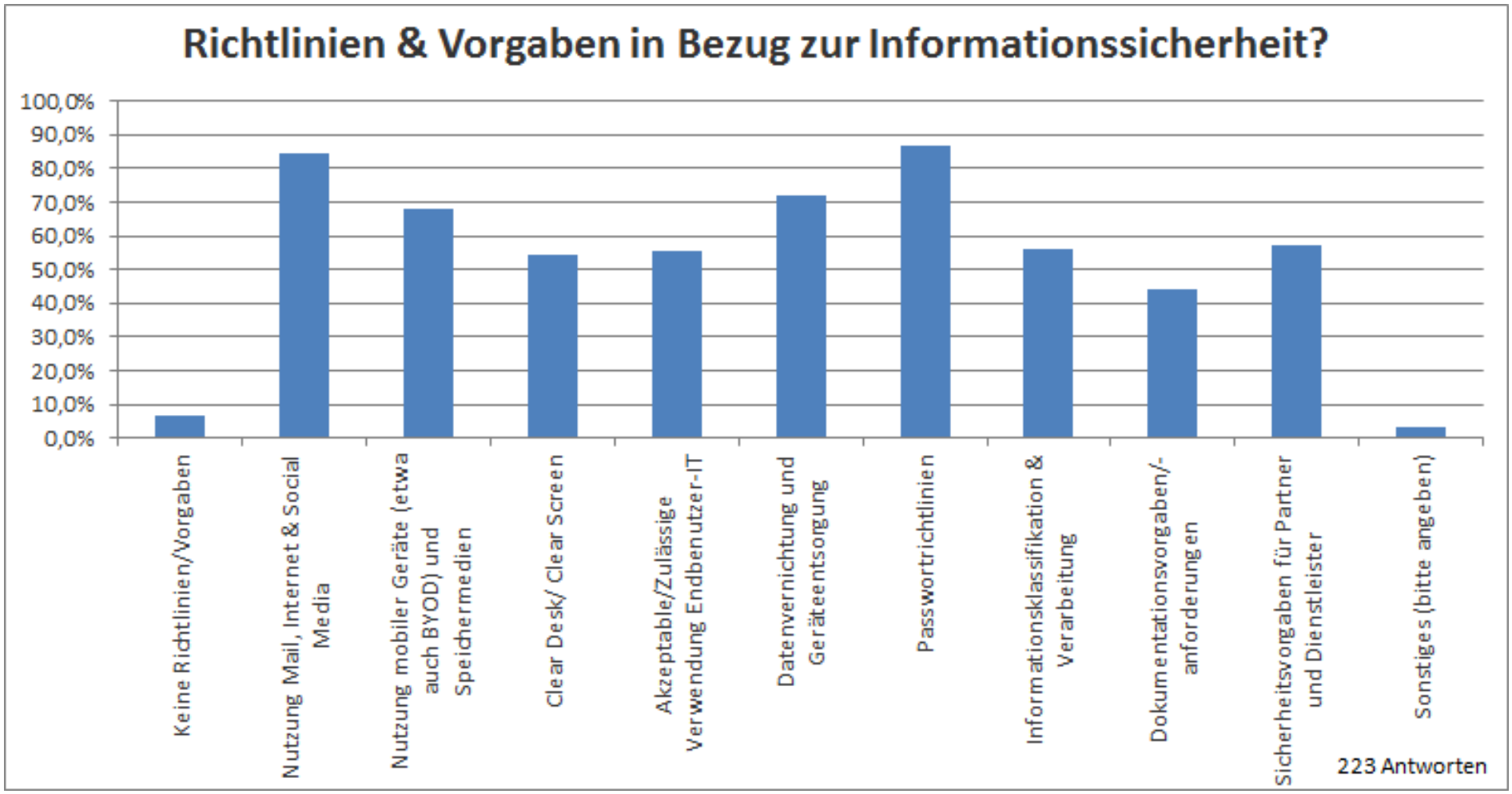
Aktuelle Situation im Unternehmen - Informationssicherheits-Policy, Richtlinien, Evaluierung der Informationssicherheit, Beratung, Vorfälle

ERGEBNISSE GESAMT III

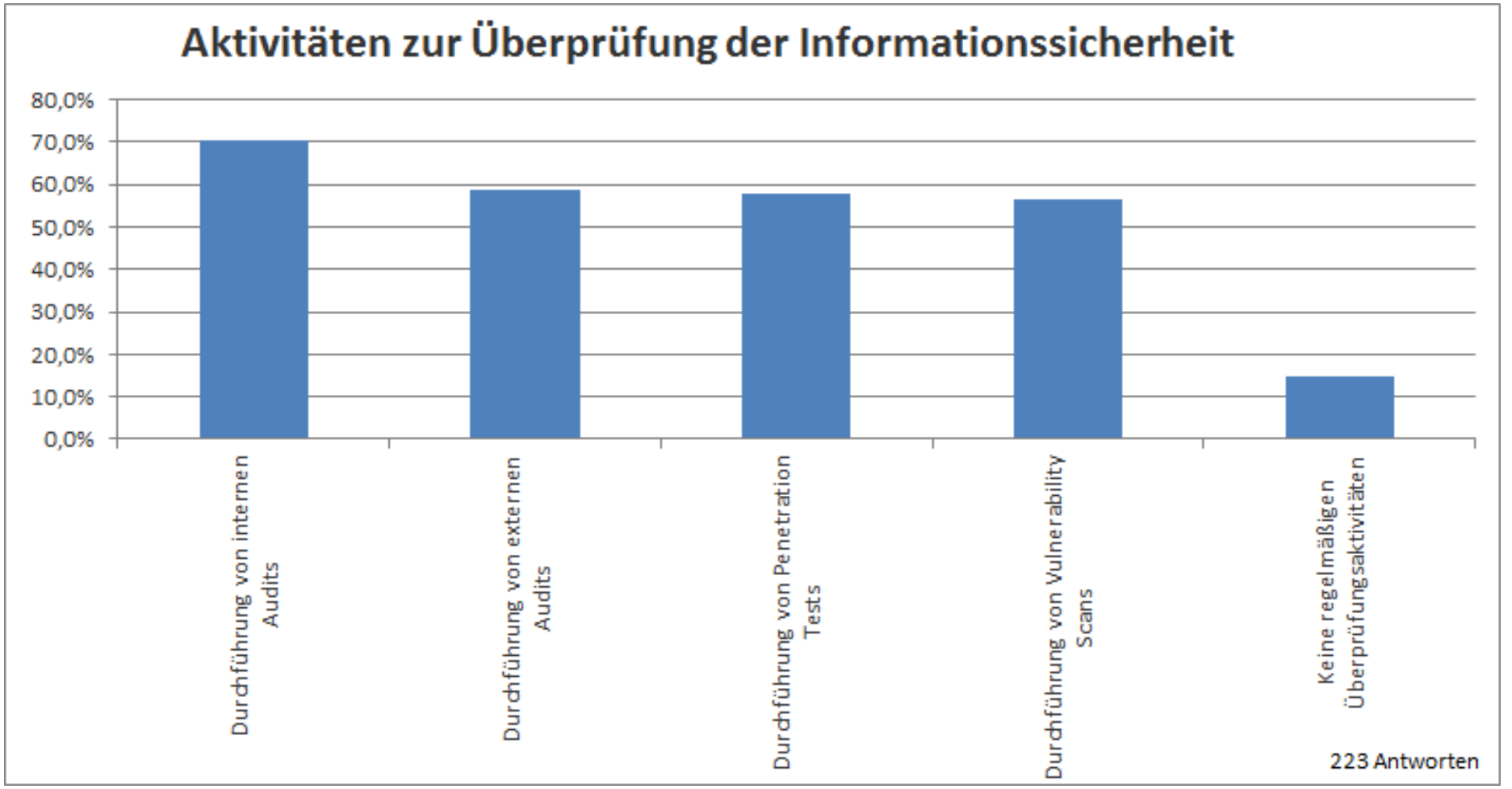
Ergebnisse Gesamt III



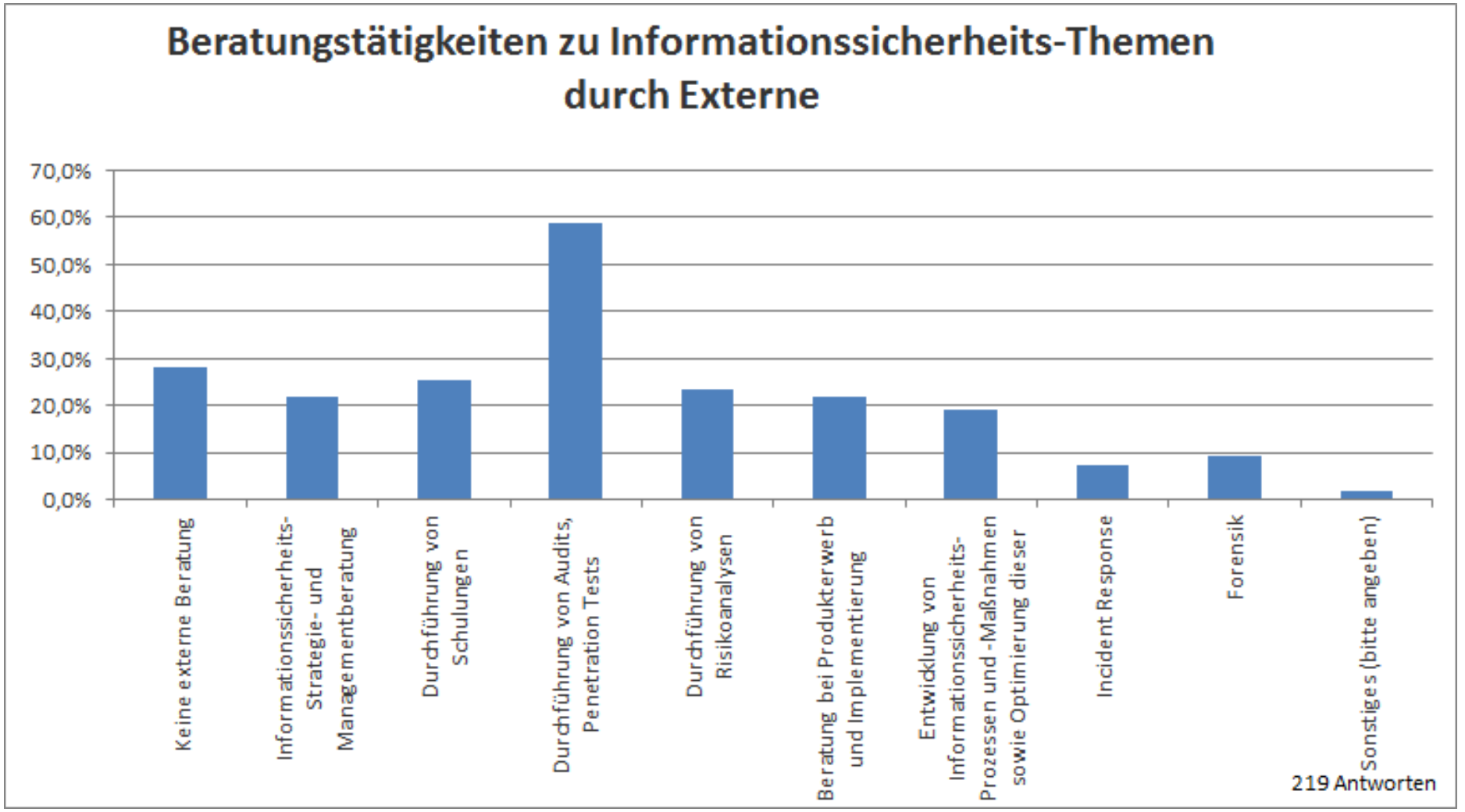
Ergebnisse Gesamt III



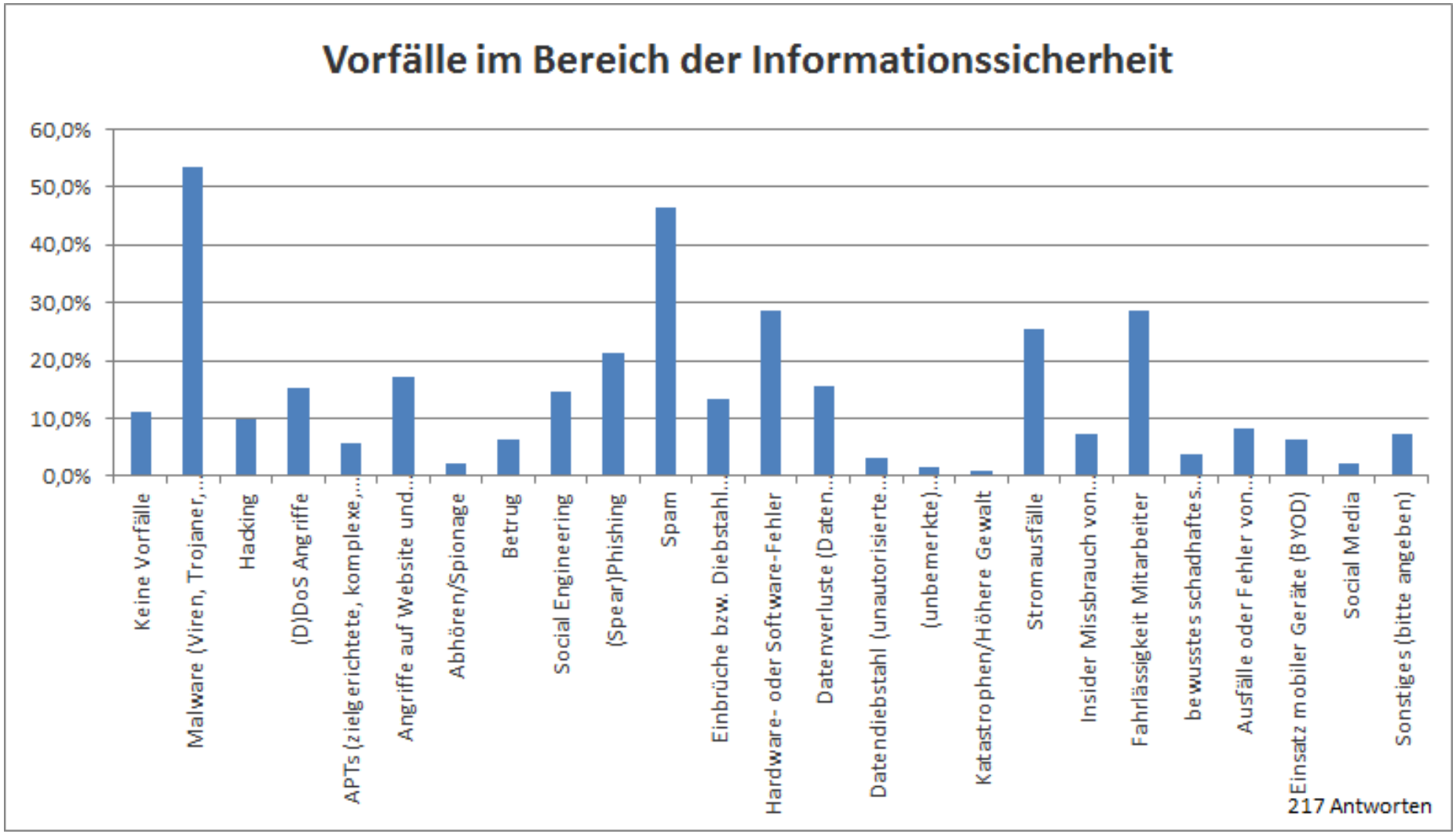
Ergebnisse Gesamt III



Ergebnisse Gesamt III



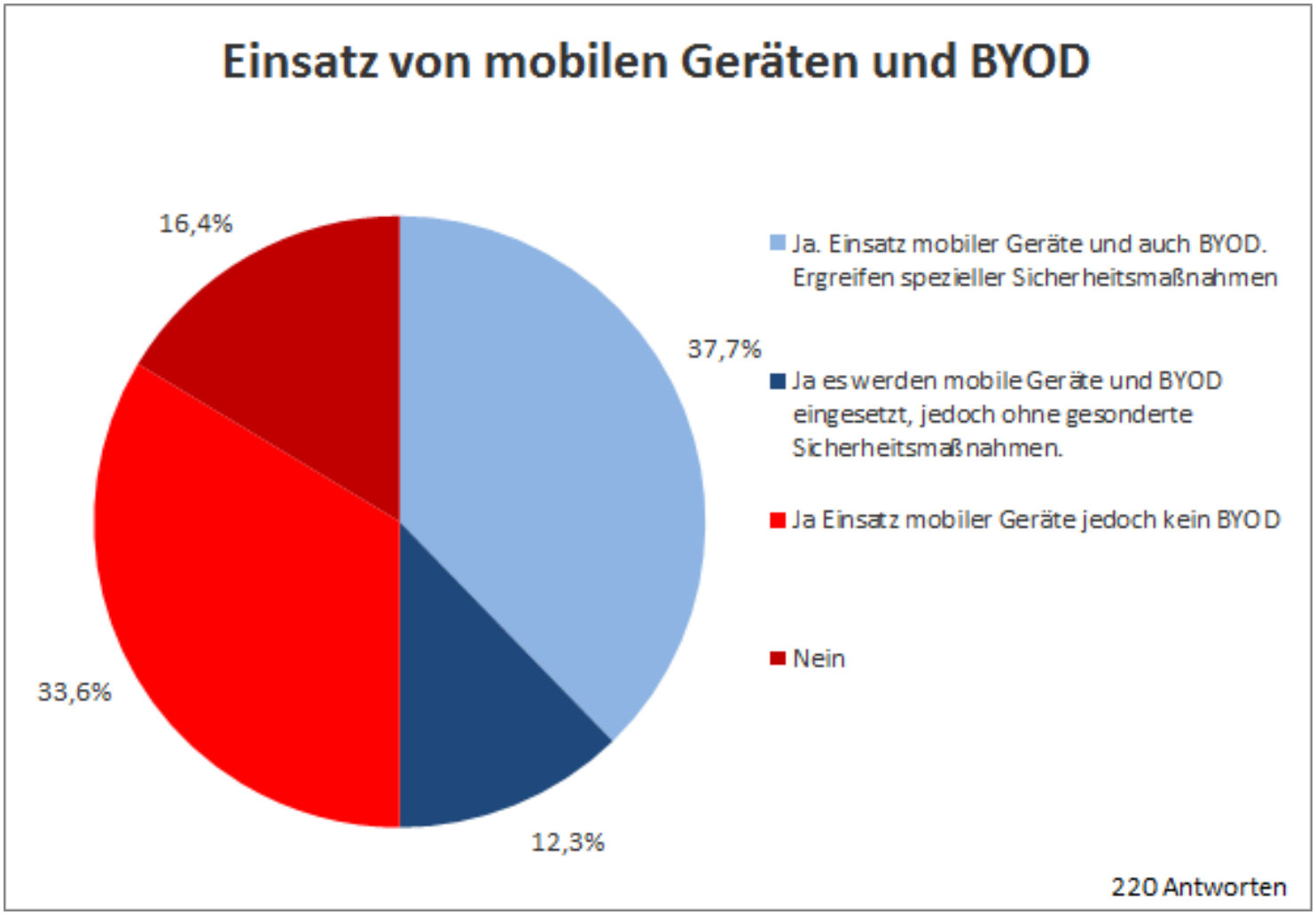
Ergebnisse Gesamt III



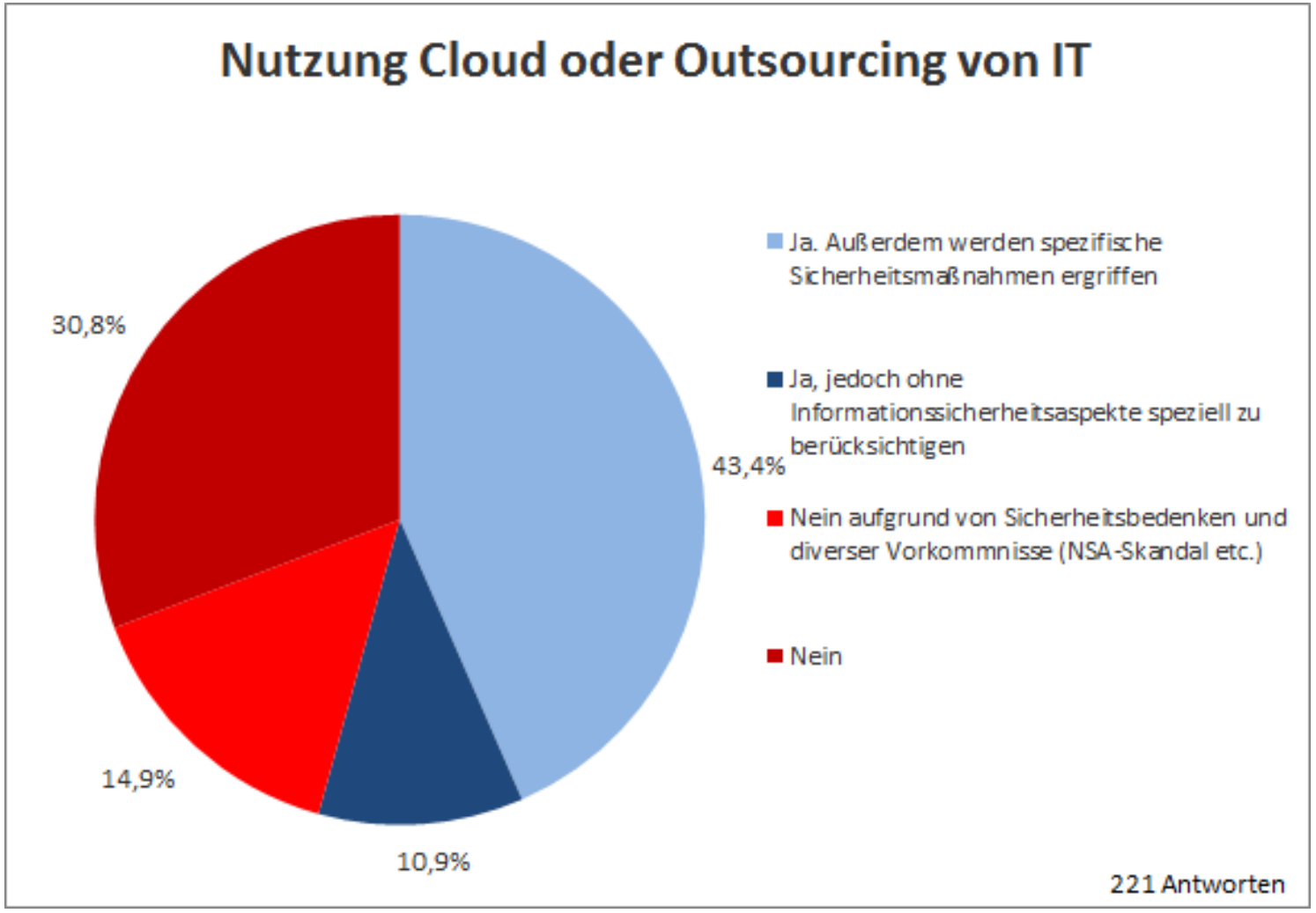
„Trendthemen“ - mobile Geräte, Cloud & Outsourcing, Mitarbeiter-Awareness, Open Source Software, APT, NSA-Enthüllungen

ERGEBNISSE GESAMT IV

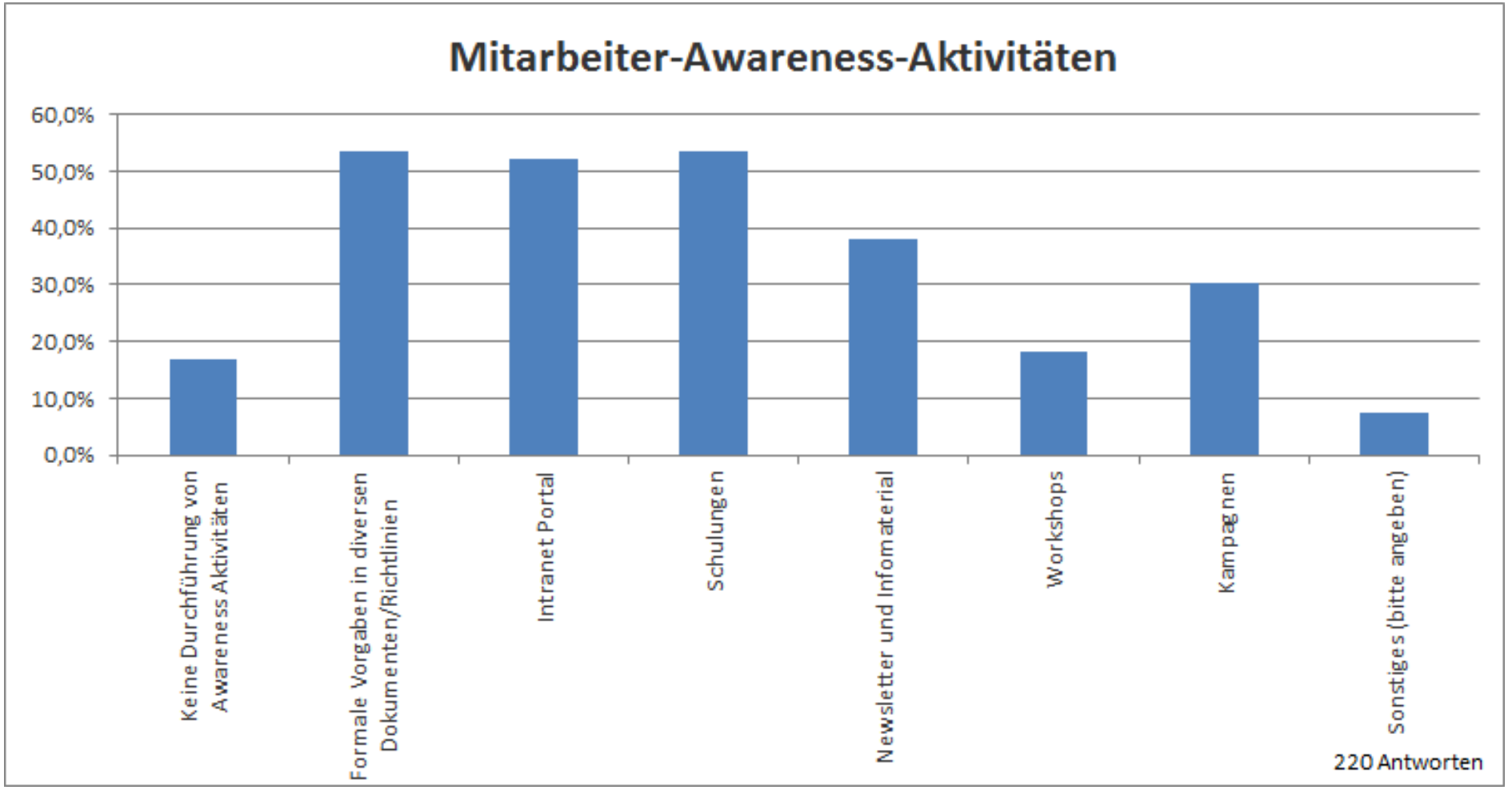
Ergebnisse Gesamt IV



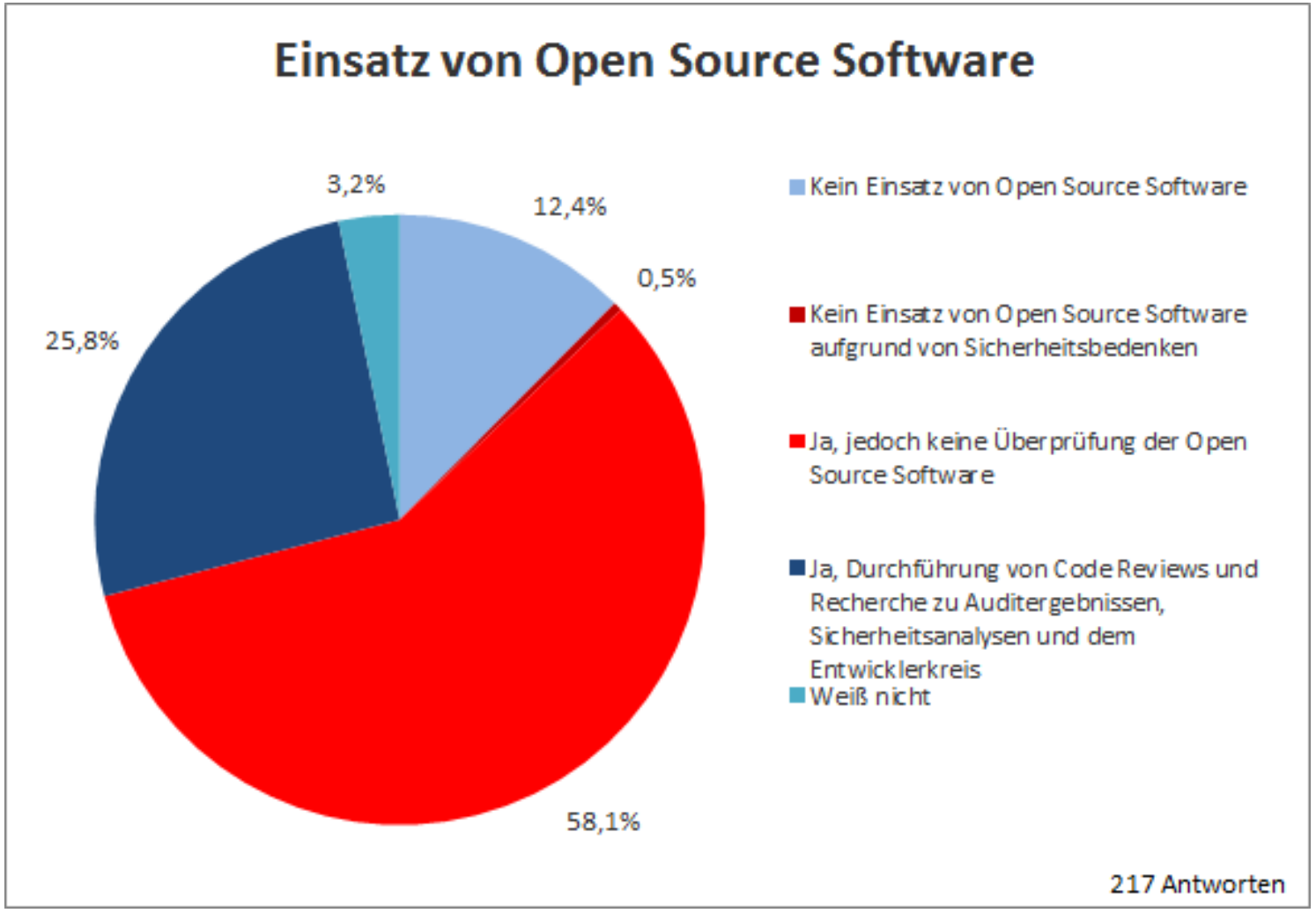
Ergebnisse Gesamt IV



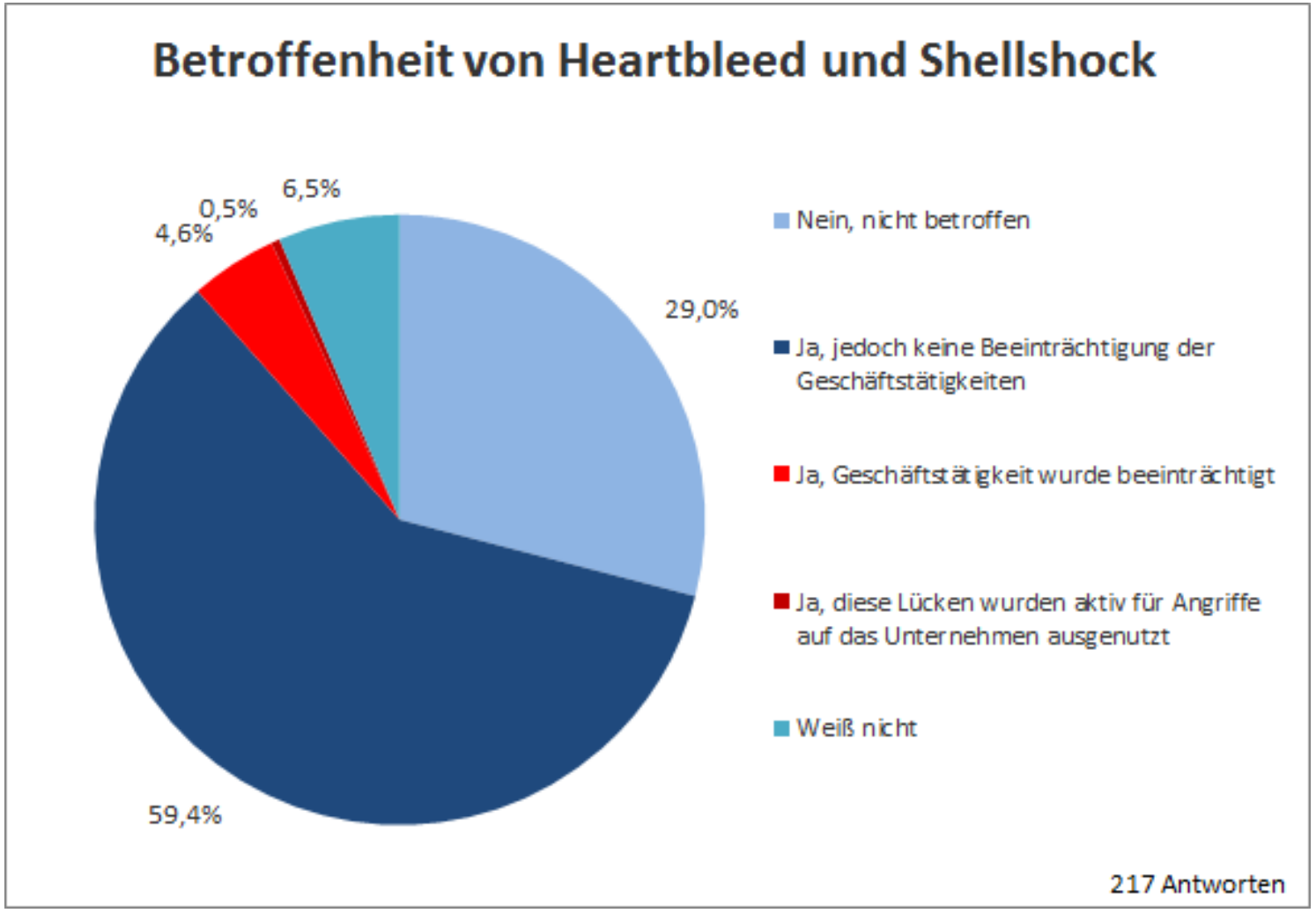
Ergebnisse Gesamt IV



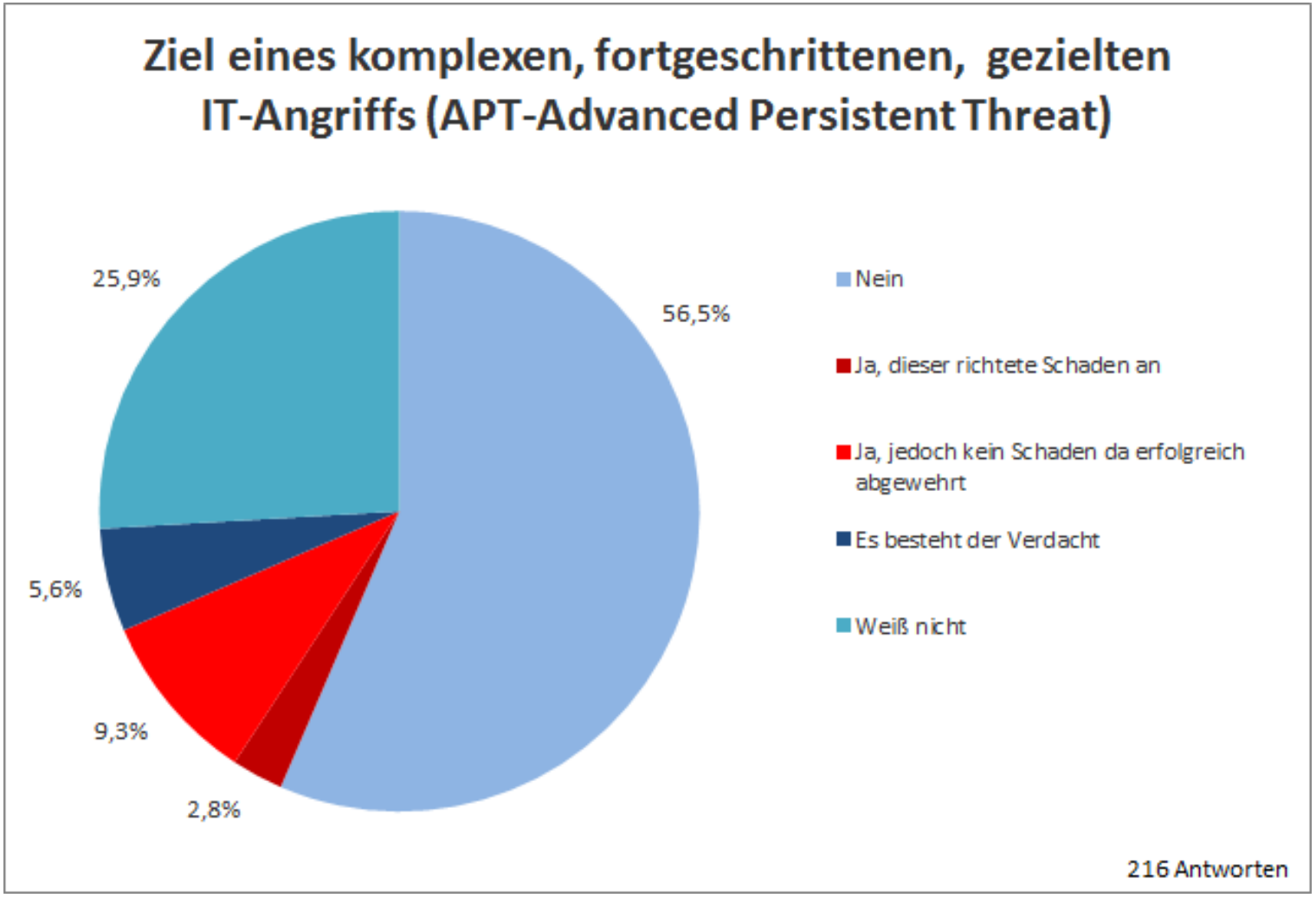
Ergebnisse Gesamt IV



Ergebnisse Gesamt IV

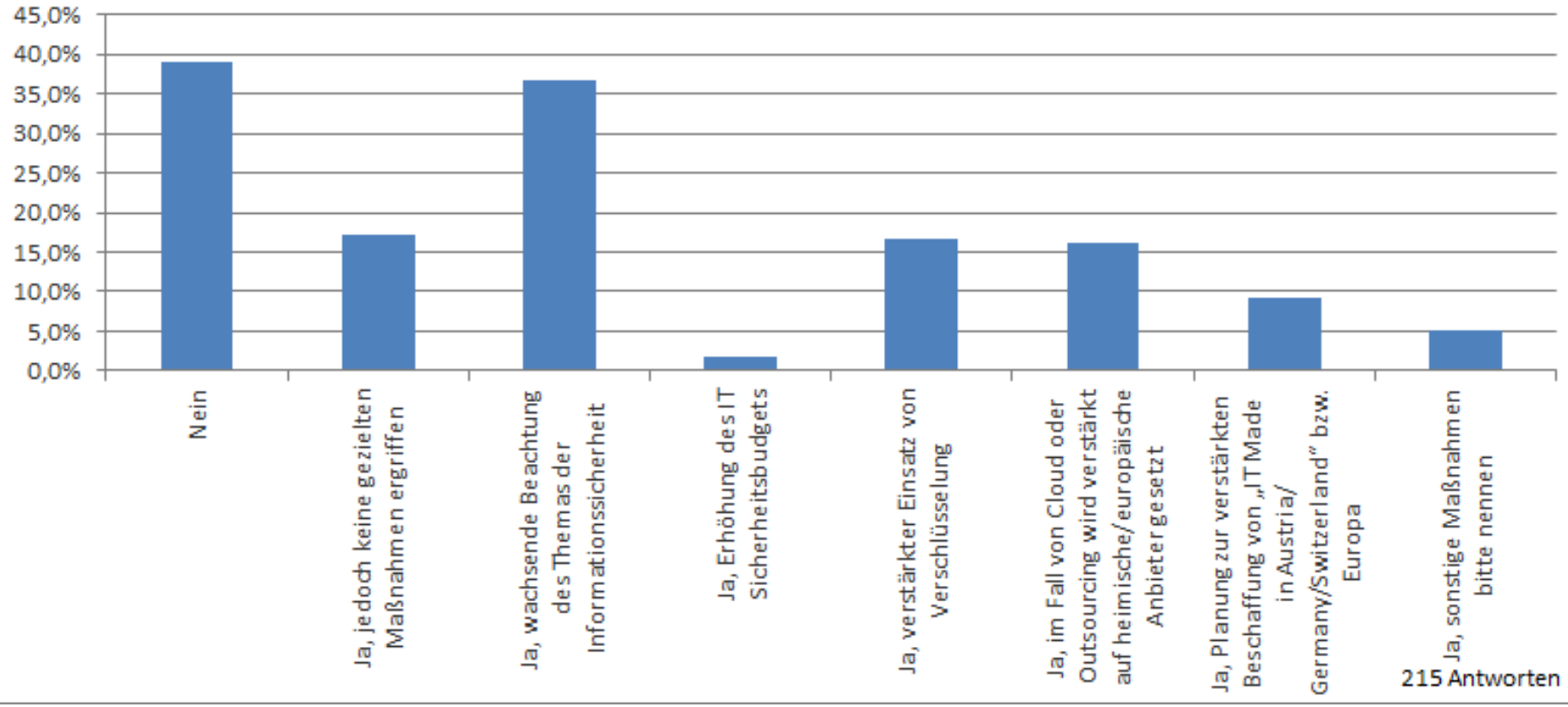


Ergebnisse Gesamt IV



Ergebnisse Gesamt IV

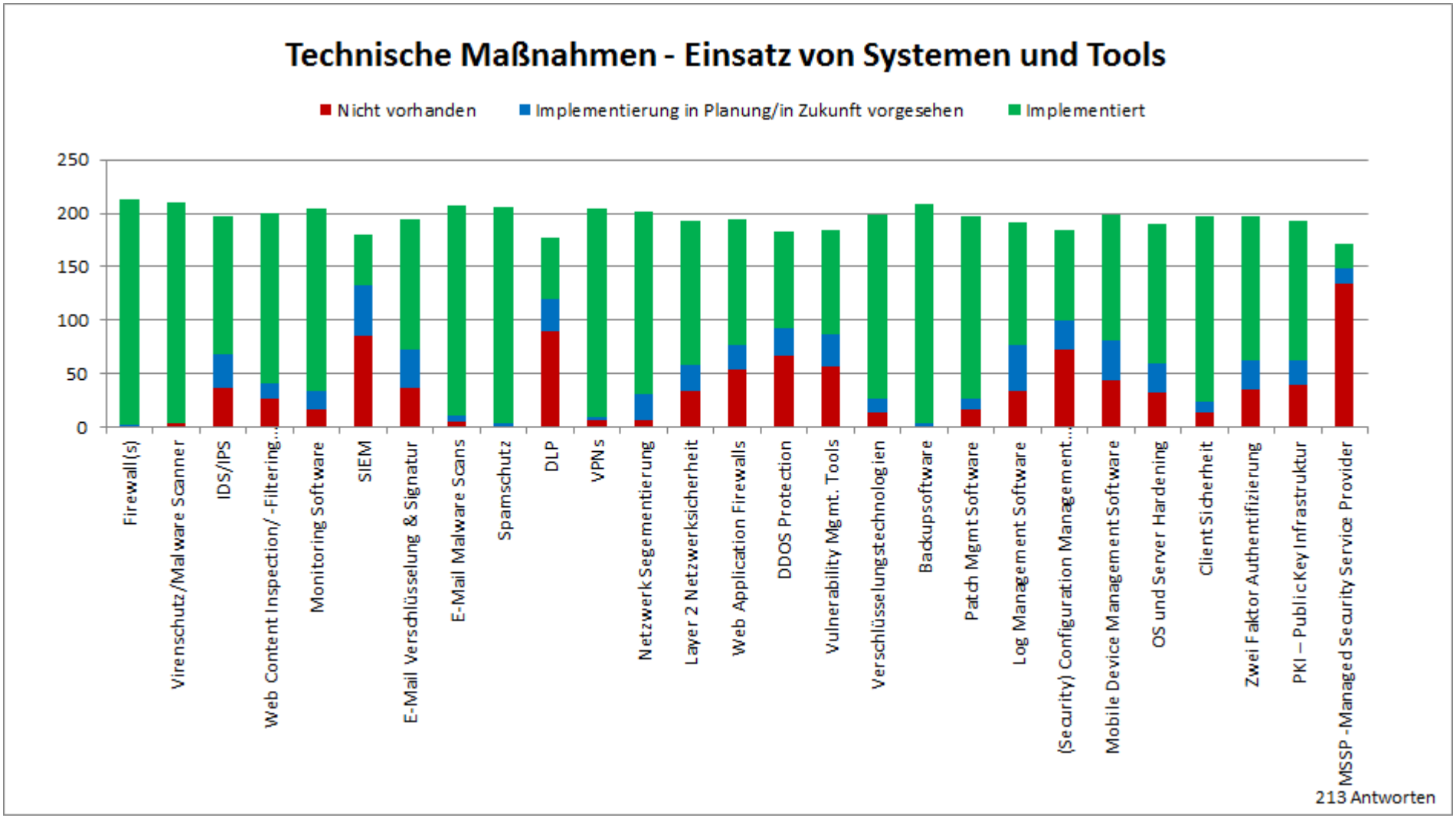
Waren die **NSA-Enthüllungen** bezüglich Überwachung und Spionage ein **Thema** bzw. haben Sie darauffolgend **spezielle Sicherheitsmaßnahmen ergriffen**?



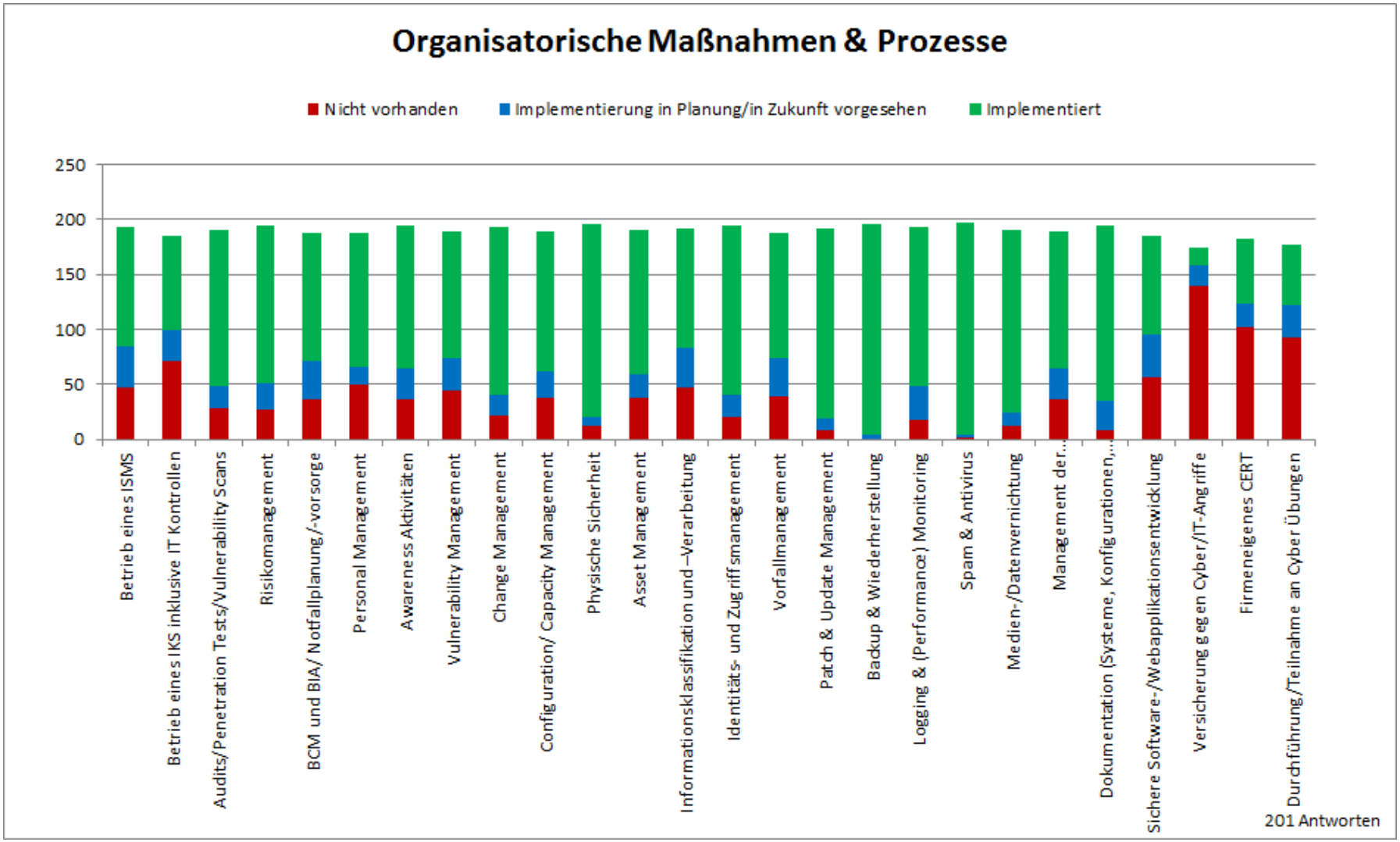
Technische und **organisatorische Aufstellung** der Unternehmen

ERGEBNISSE GESAMT V

Ergebnisse Gesamt V



Ergebnisse Gesamt V

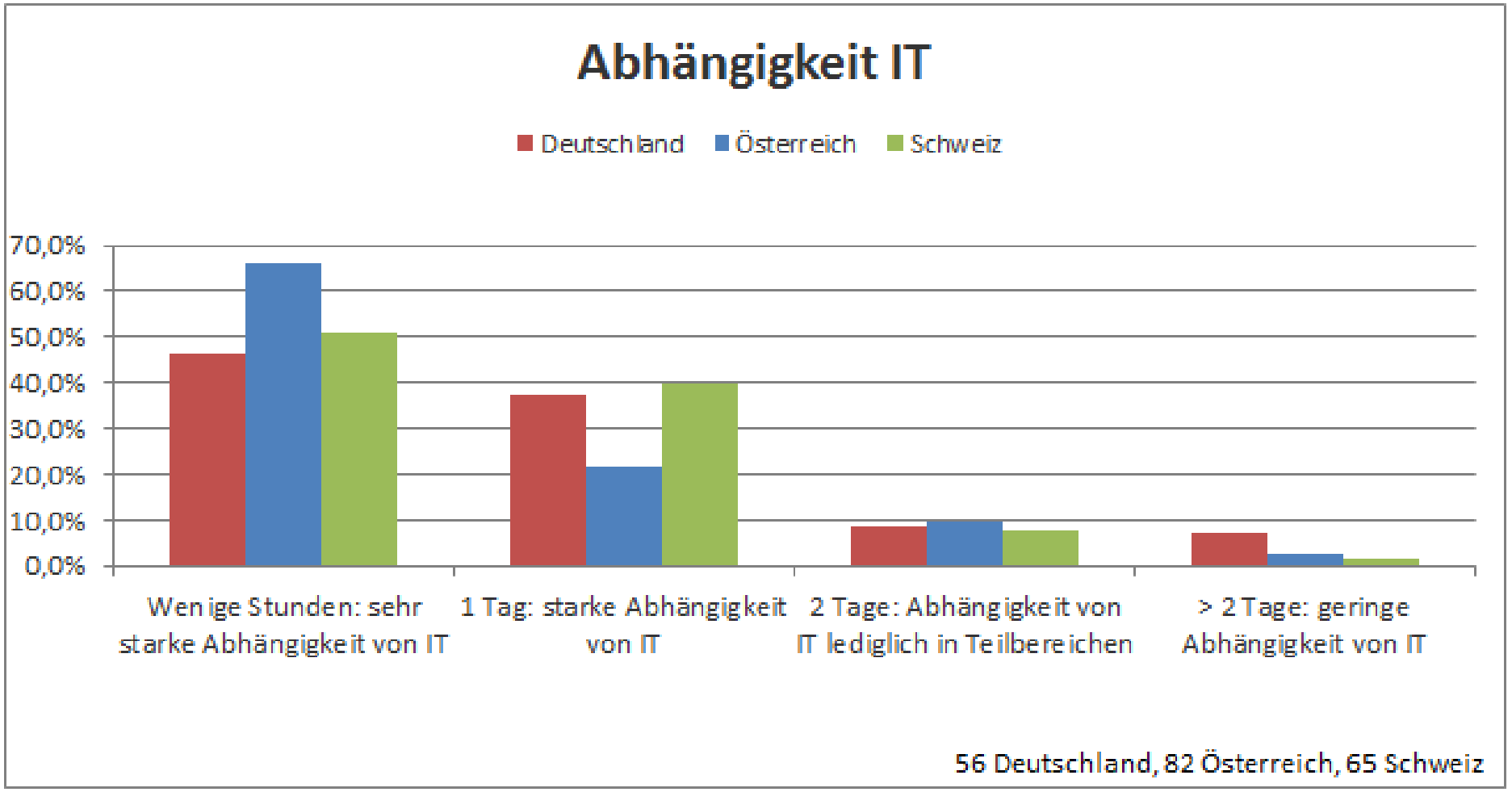


/informatik & security /fh/// st.pölten

Wichtigkeit der **Informationssicherheit**, **Abhängigkeit** von **IT** & **Informationen** bzw. Daten

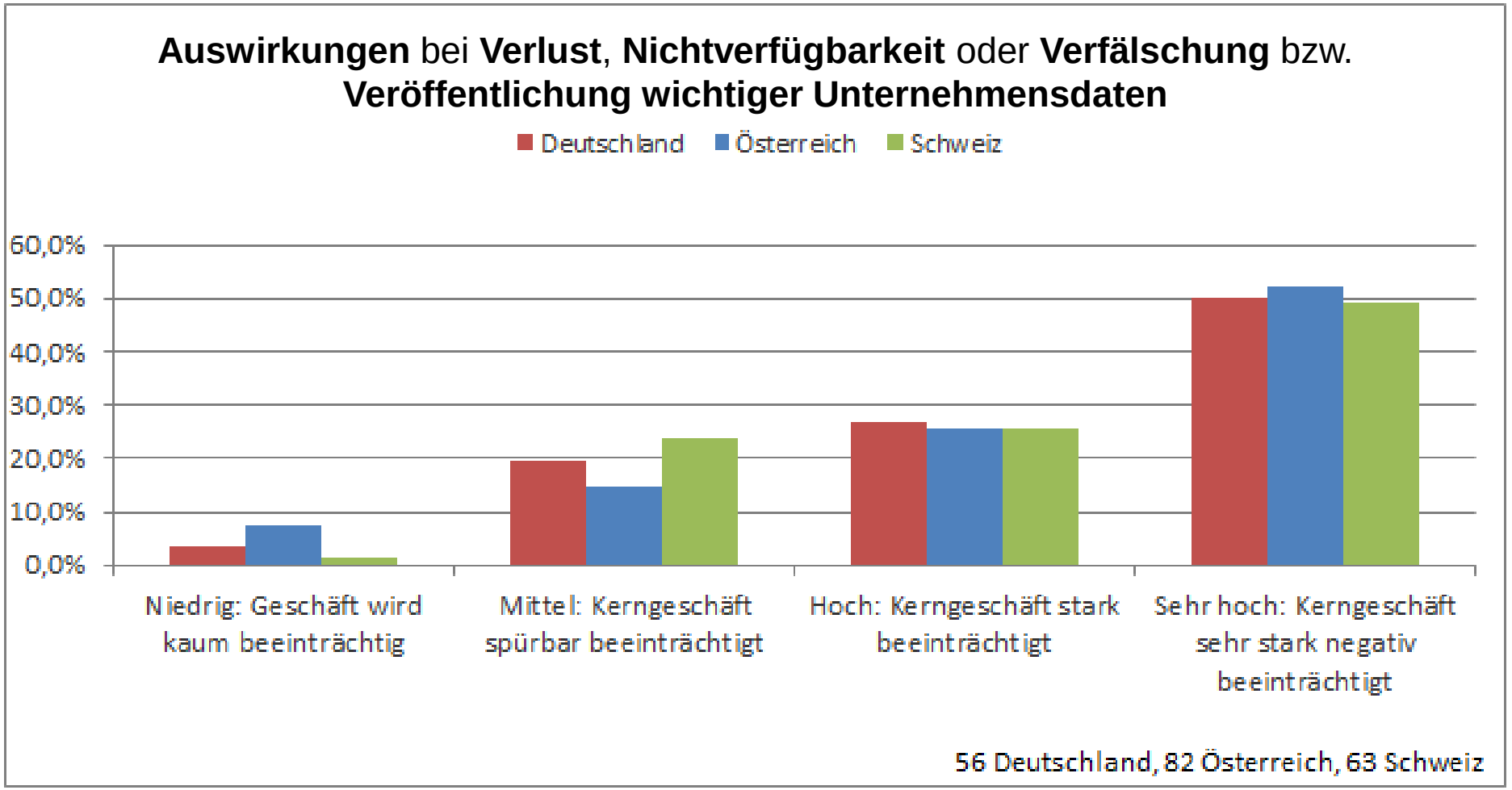
ERGEBNISSE LÄNDERSPEZIFISCH I

Ergebnisse länderspezifisch I

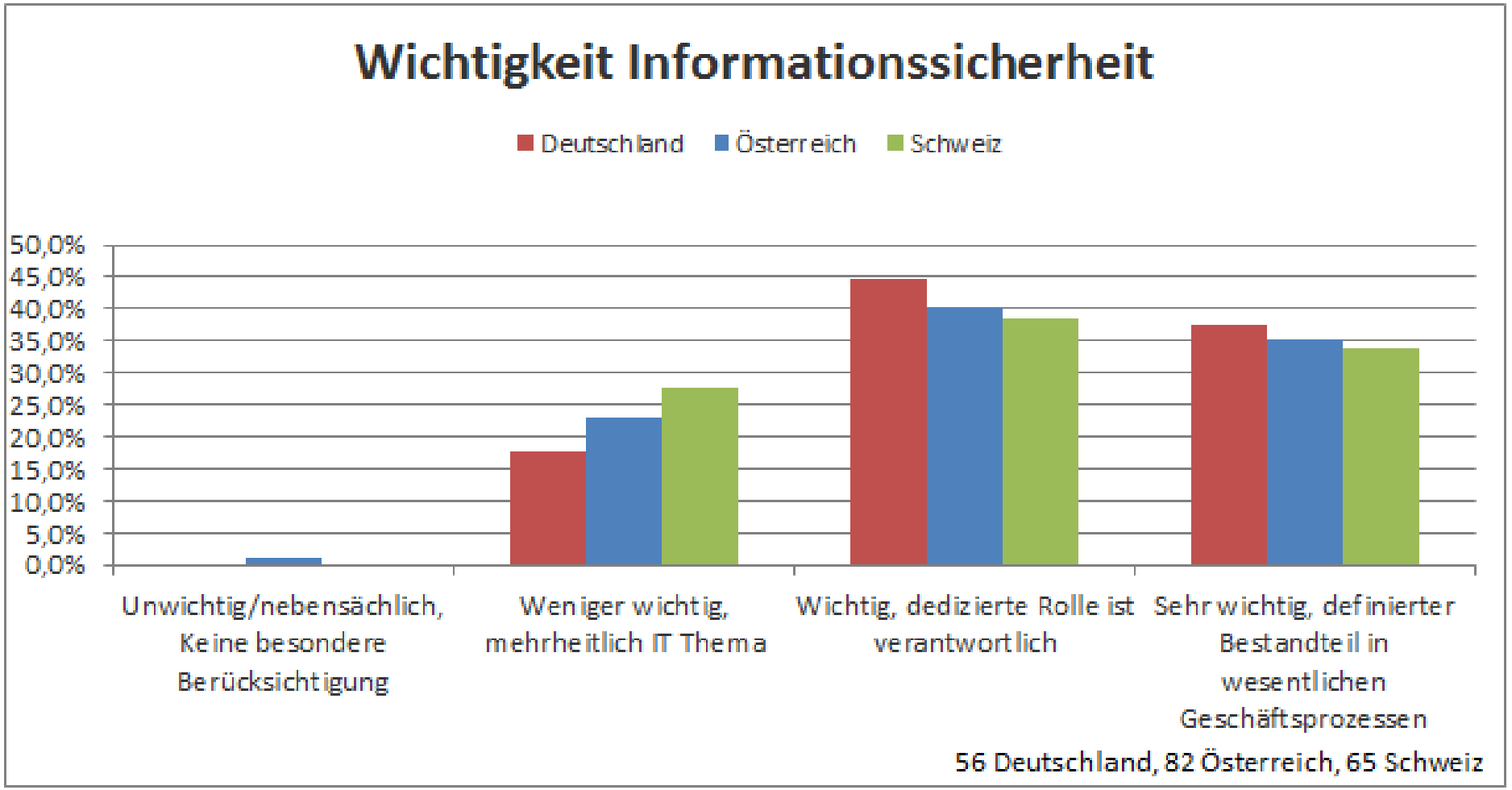


Ergebnisse länderspezifisch I

/informatik & security /fh/// st.pölten



Ergebnisse länderspezifisch I

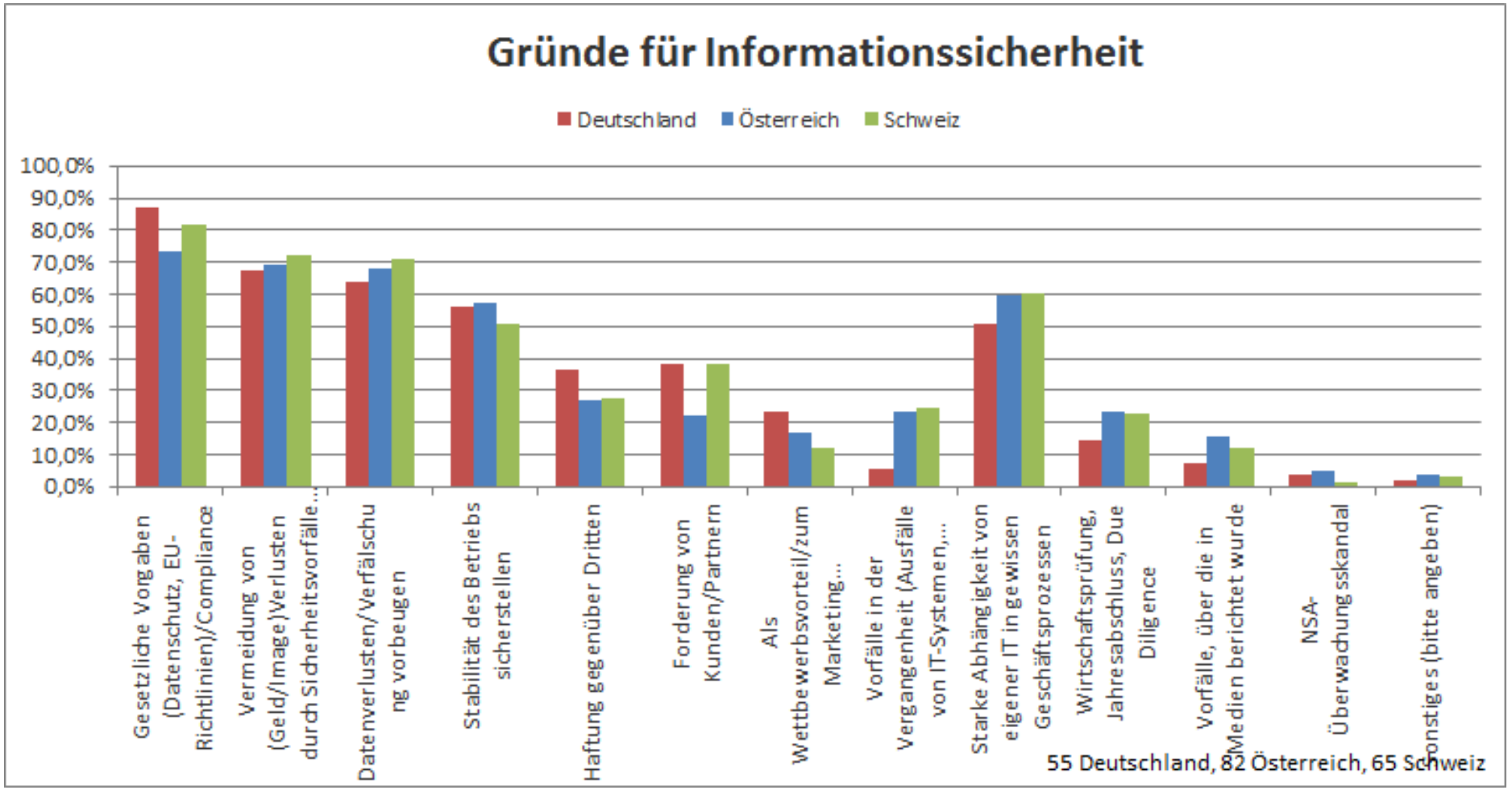


/informatik & security /fh/// st.pölten

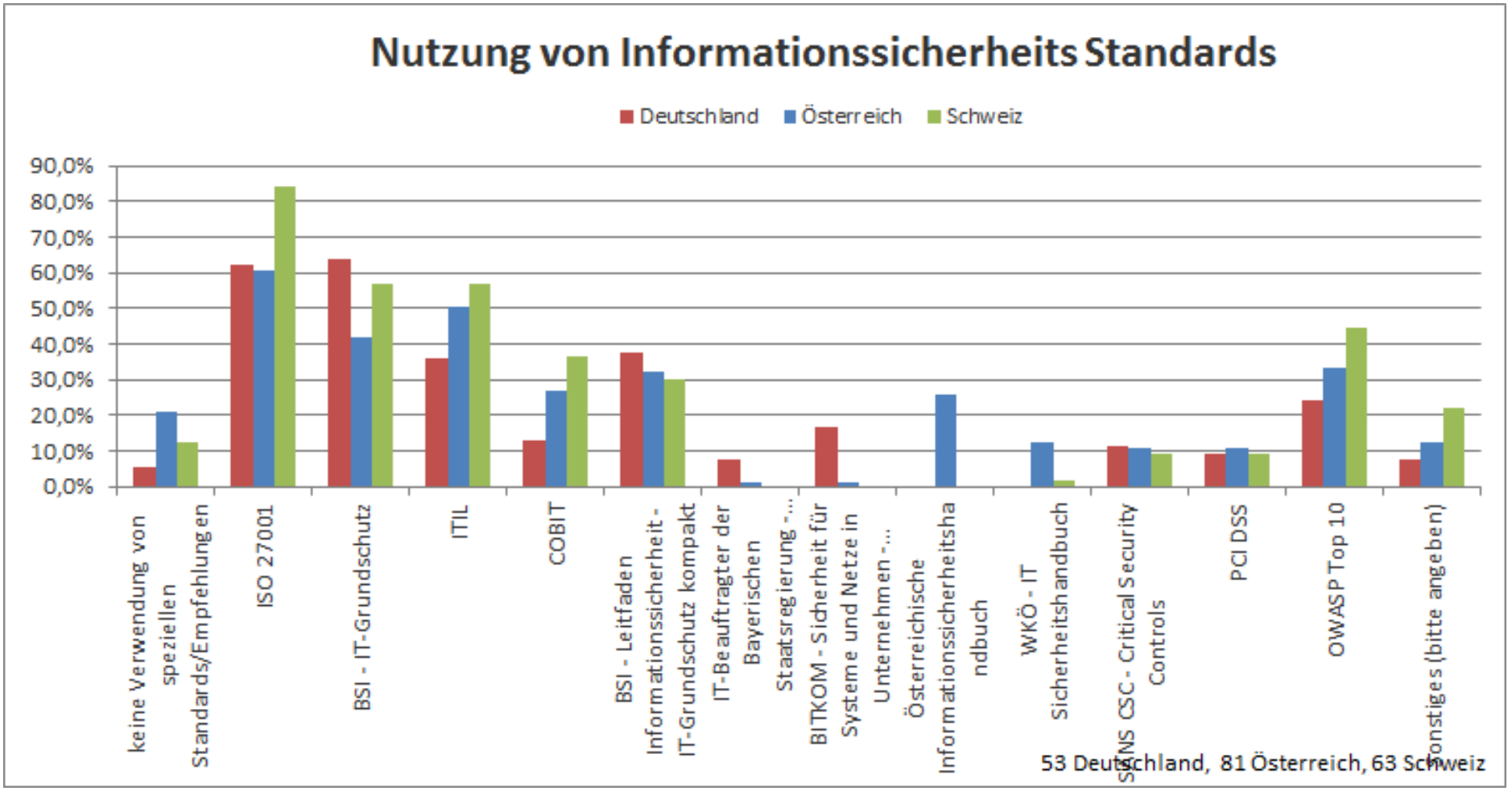
Gründe und Motivation für Informationssicherheit, Bedrohungen, Nutzung von Standards

ERGEBNISSE LÄNDERSPEZIFISCH II

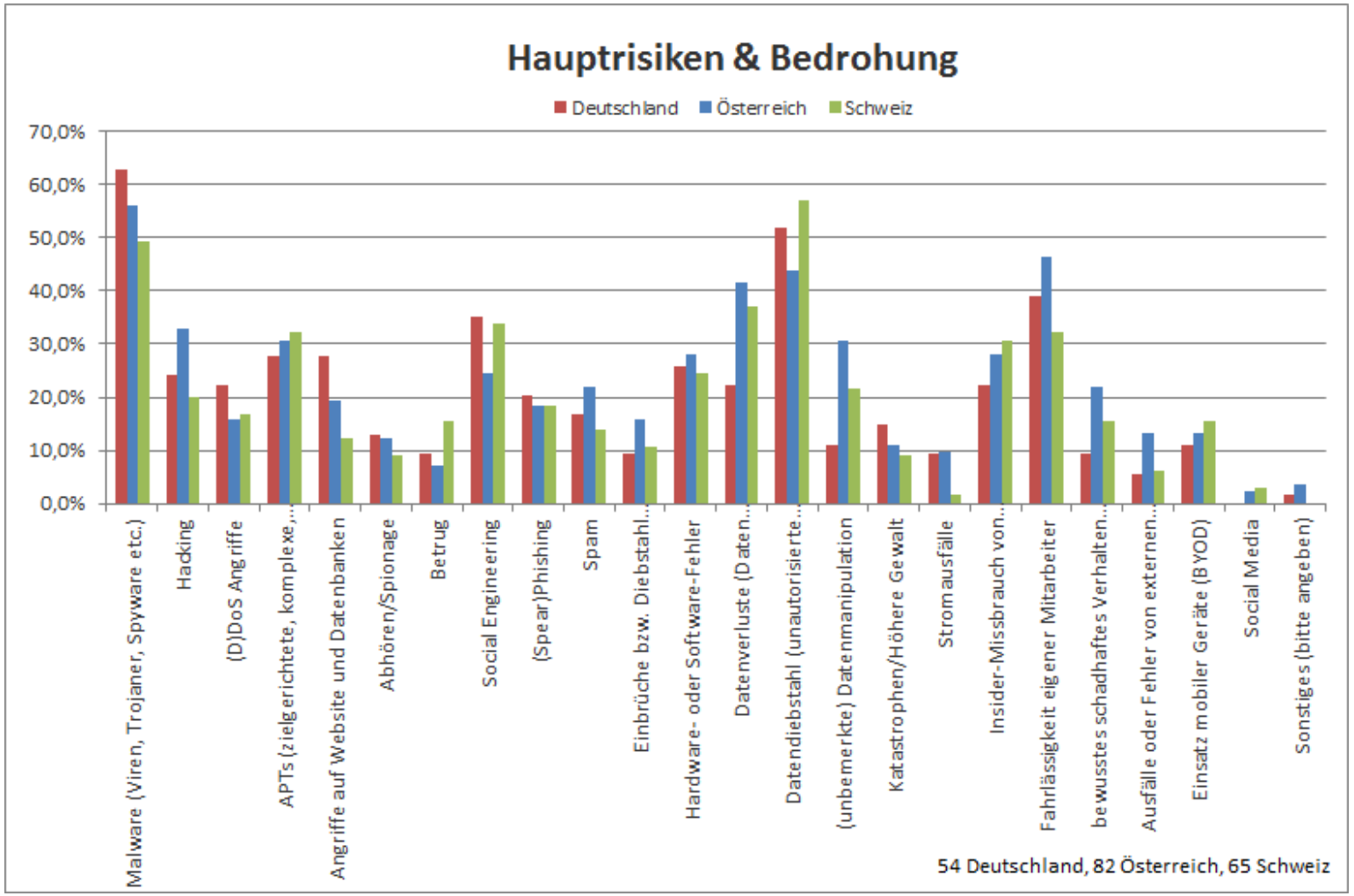
Ergebnisse länderspezifisch II



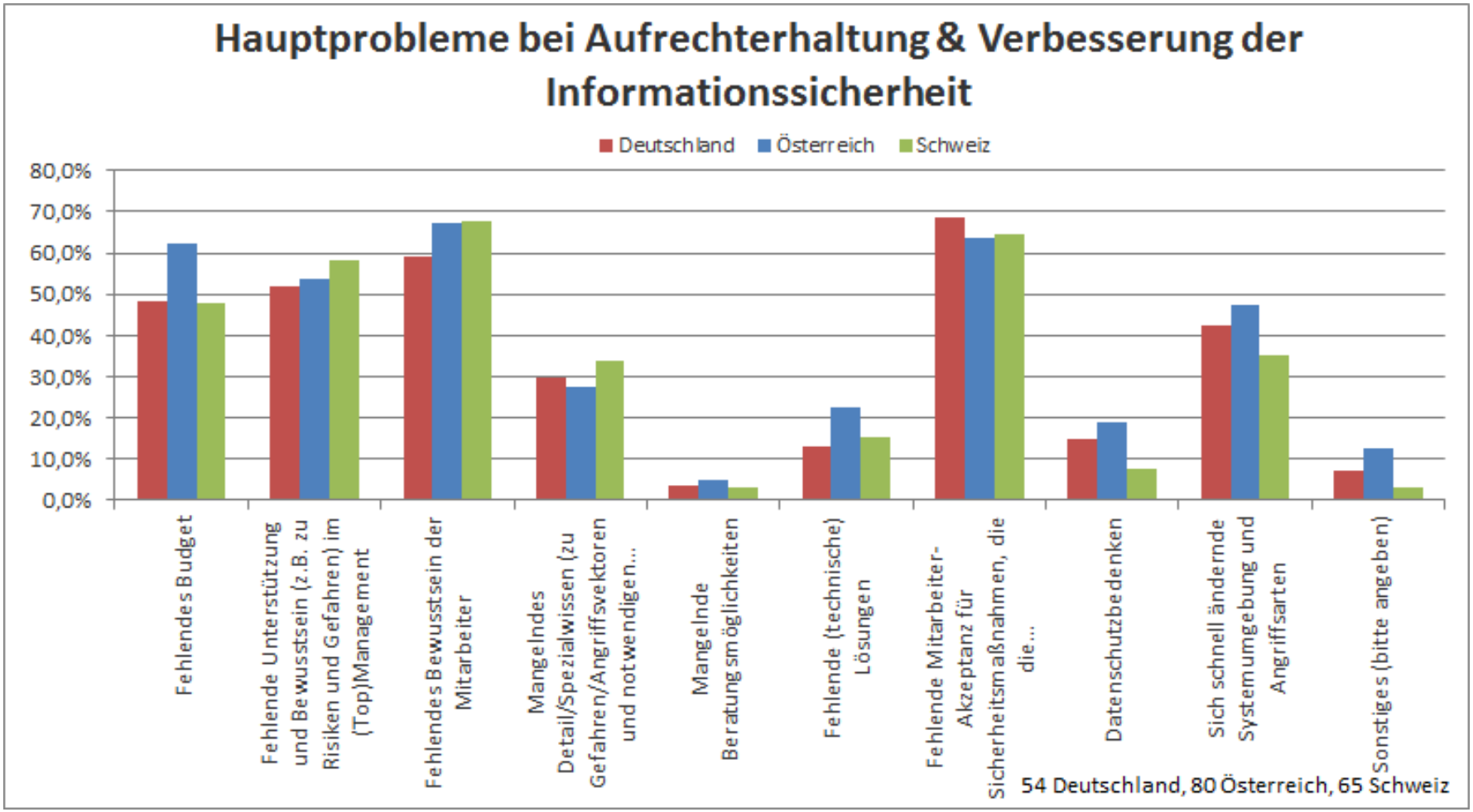
Ergebnisse länderspezifisch II



Ergebnisse länderspezifisch II



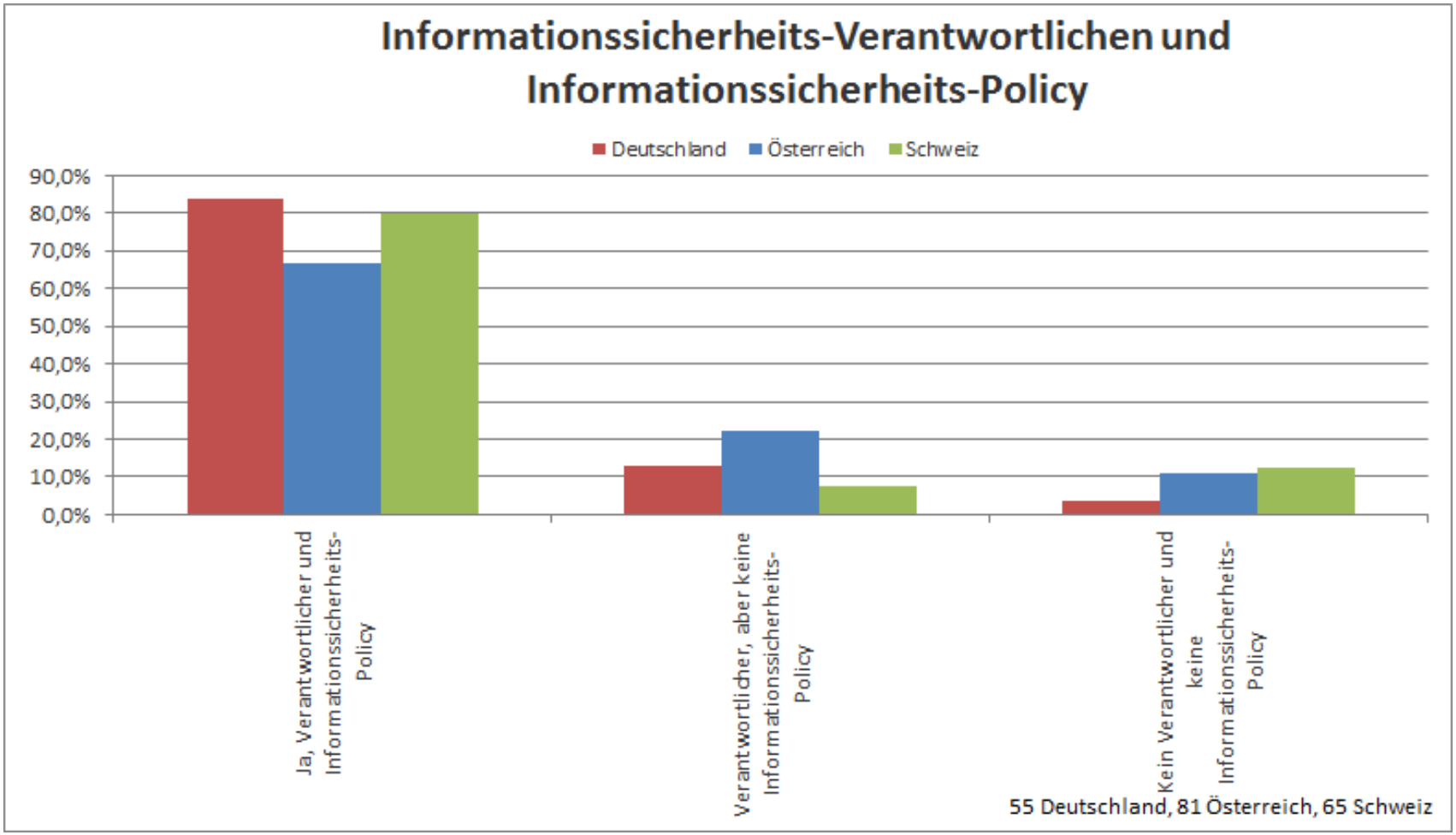
Ergebnisse länderspezifisch II



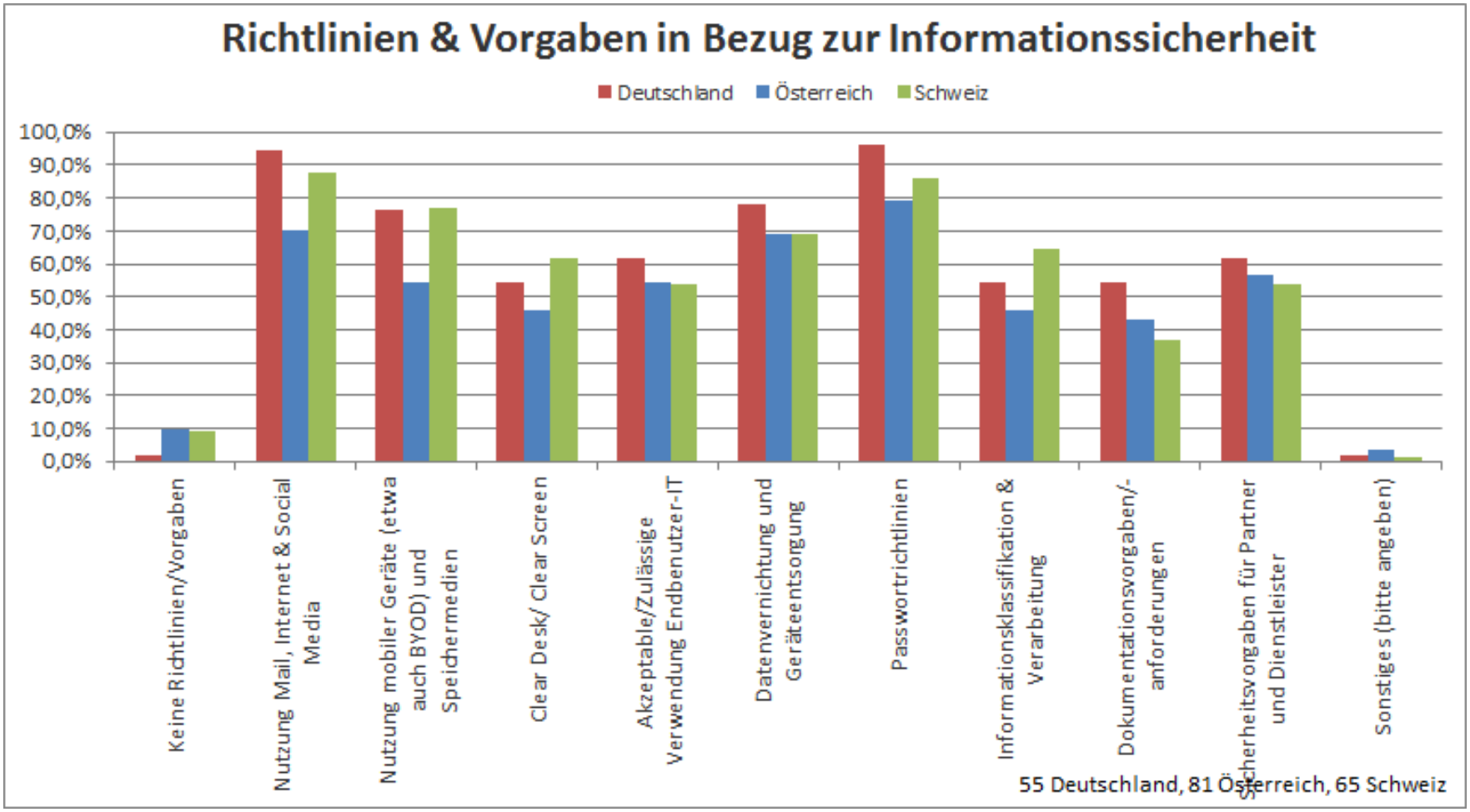
Aktuelle Situation im Unternehmen - Informationssicherheits-Policy, Richtlinien, Evaluierung der Informationssicherheit, Beratung, Vorfälle

ERGEBNISSE LÄNDERSPEZIFISCH III

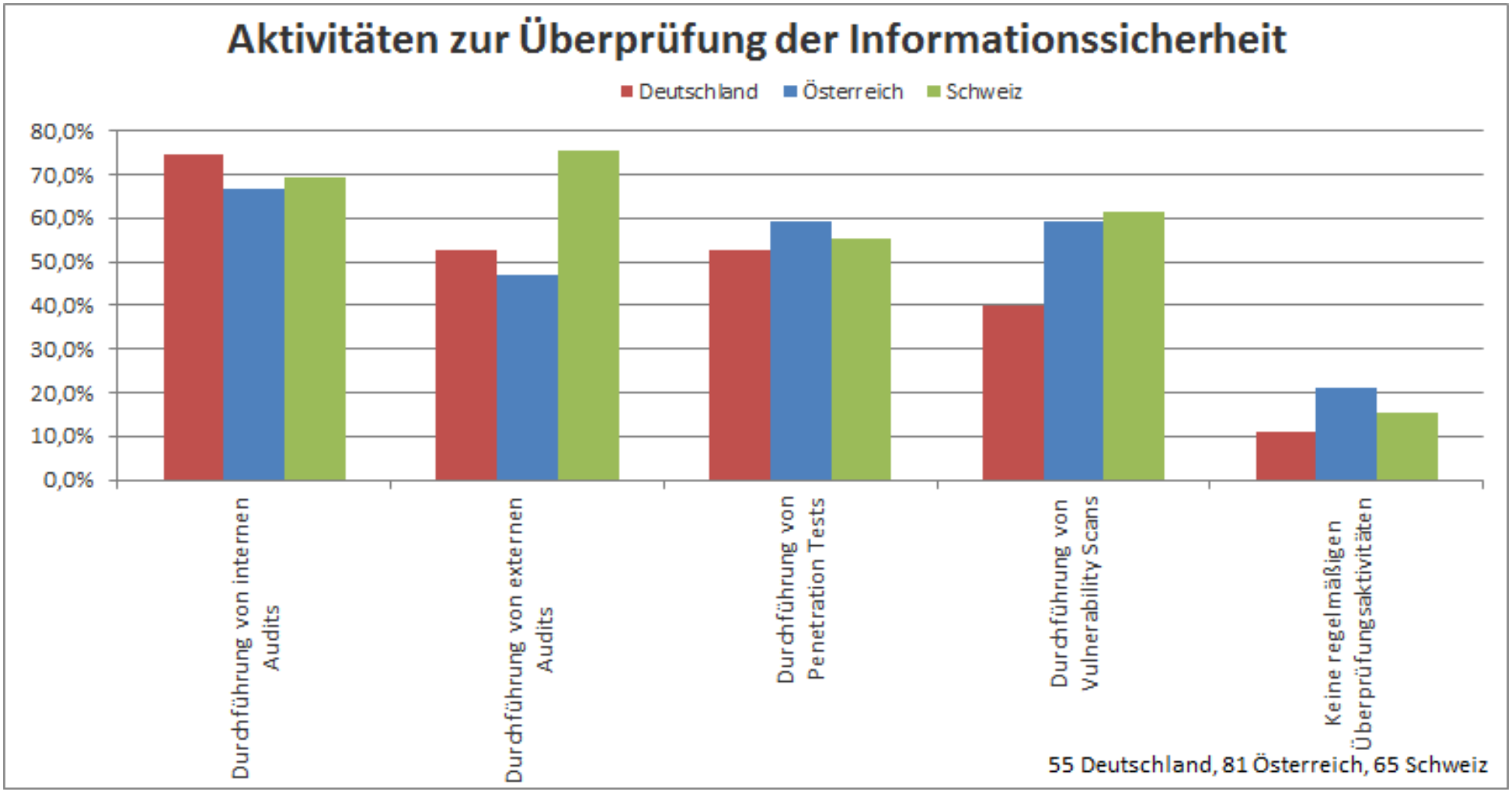
Ergebnisse länderspezifisch III



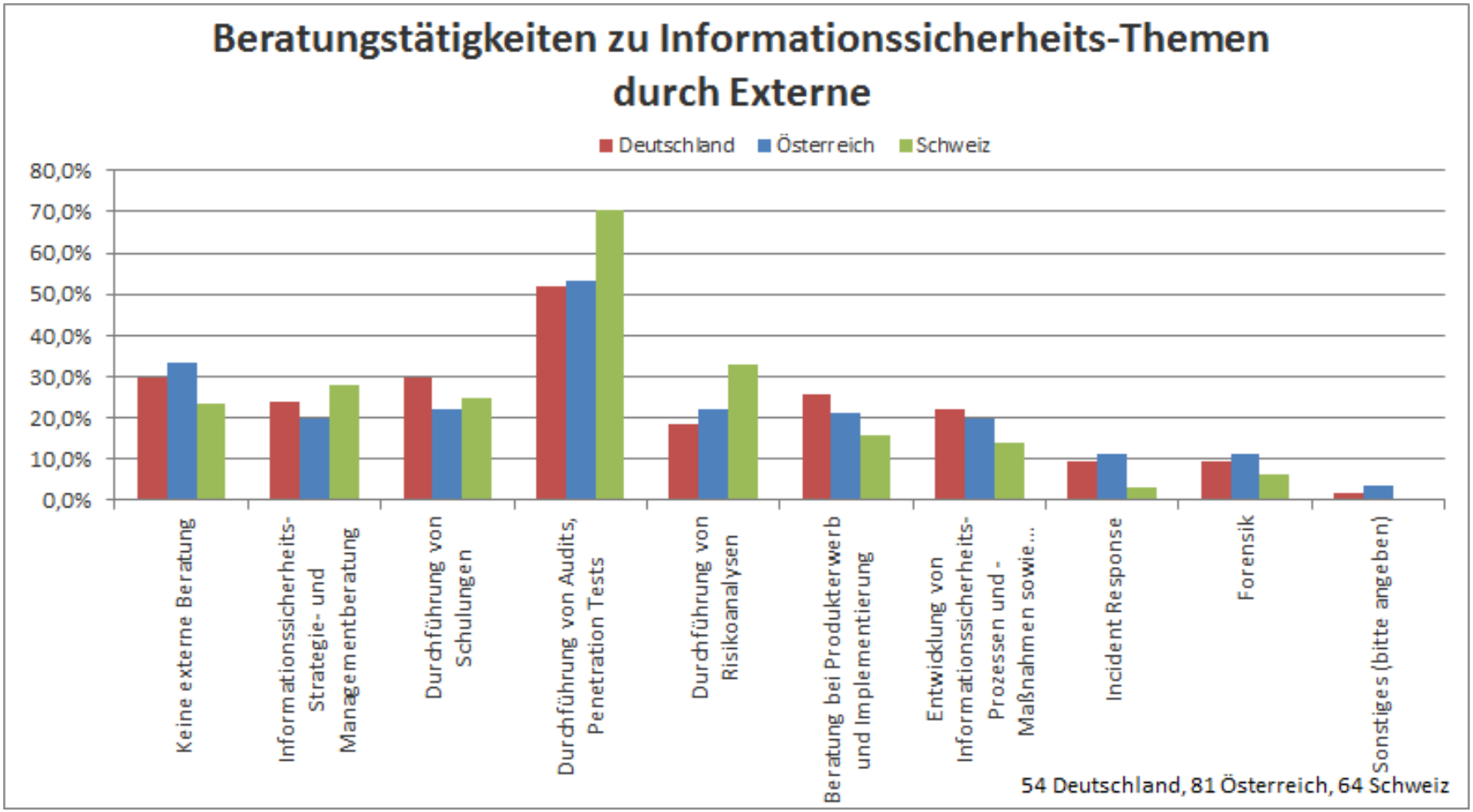
Ergebnisse länderspezifisch III



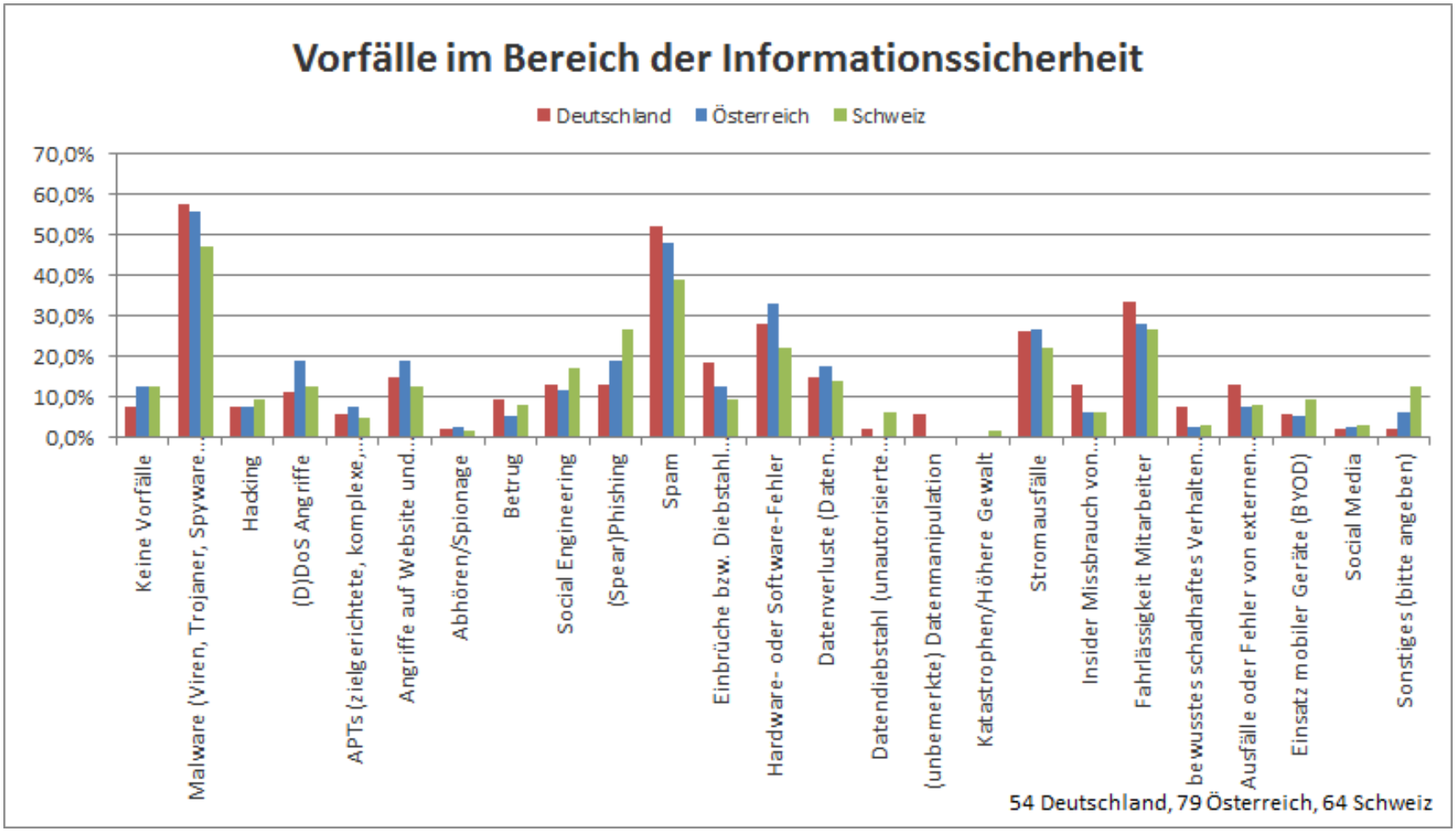
Ergebnisse länderspezifisch III



Ergebnisse länderspezifisch III



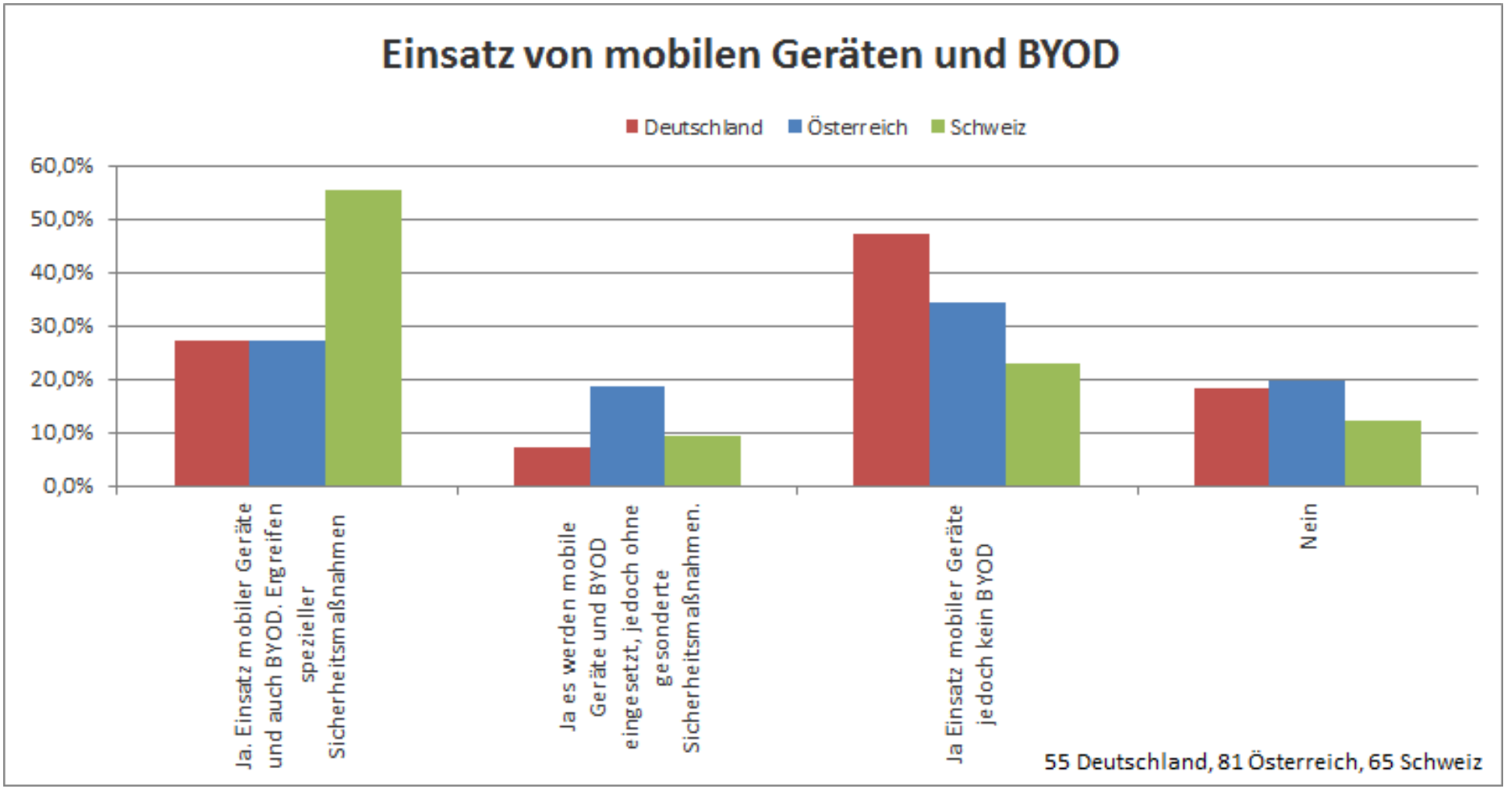
Ergebnisse länderspezifisch III



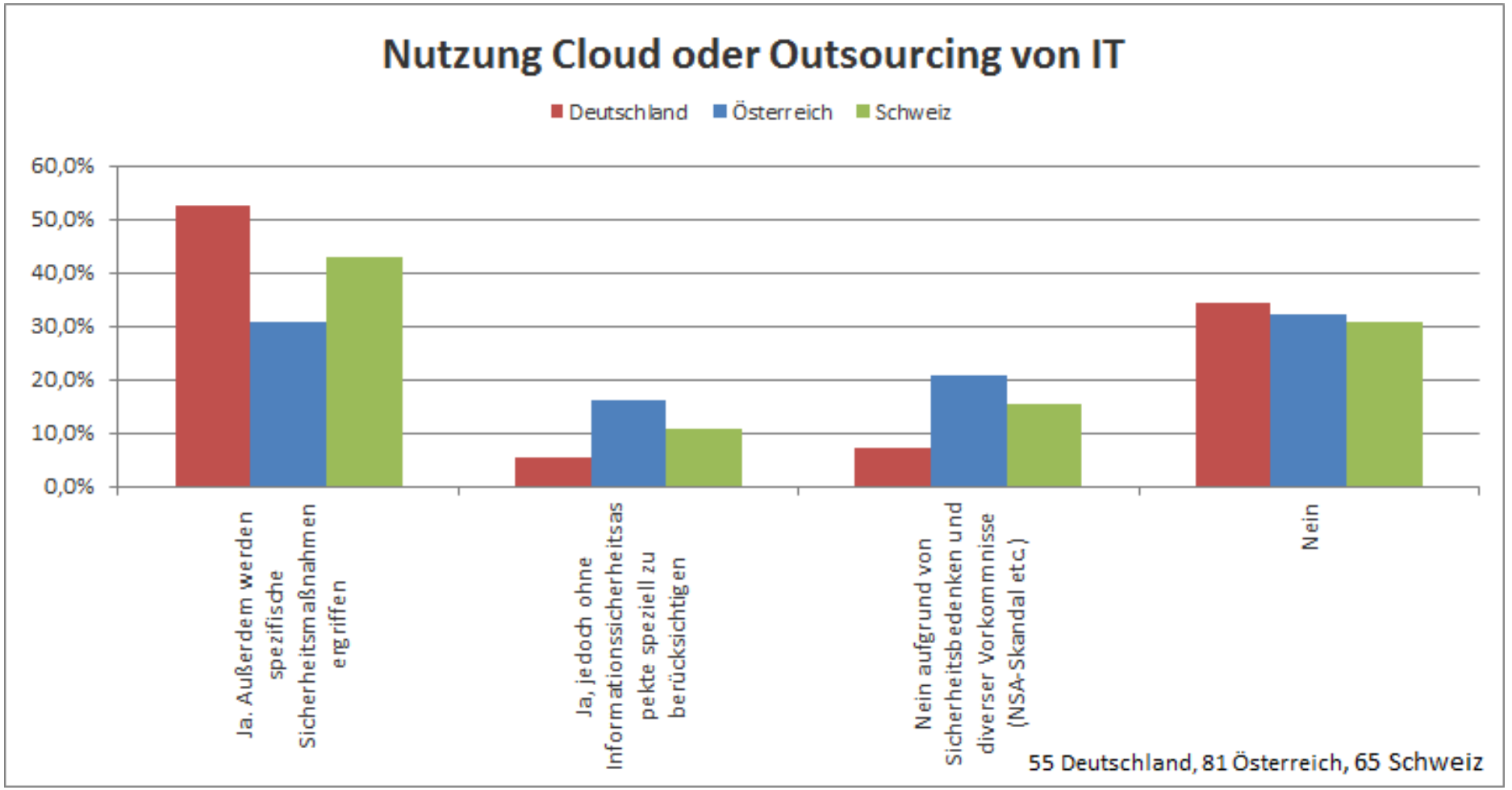
„Trendthemen“ - mobile Geräte, Cloud & Outsourcing, Mitarbeiter-Awareness, Open Source Software, APT, NSA-Enthüllungen

ERGEBNISSE LÄNDERSPEZIFISCH IV

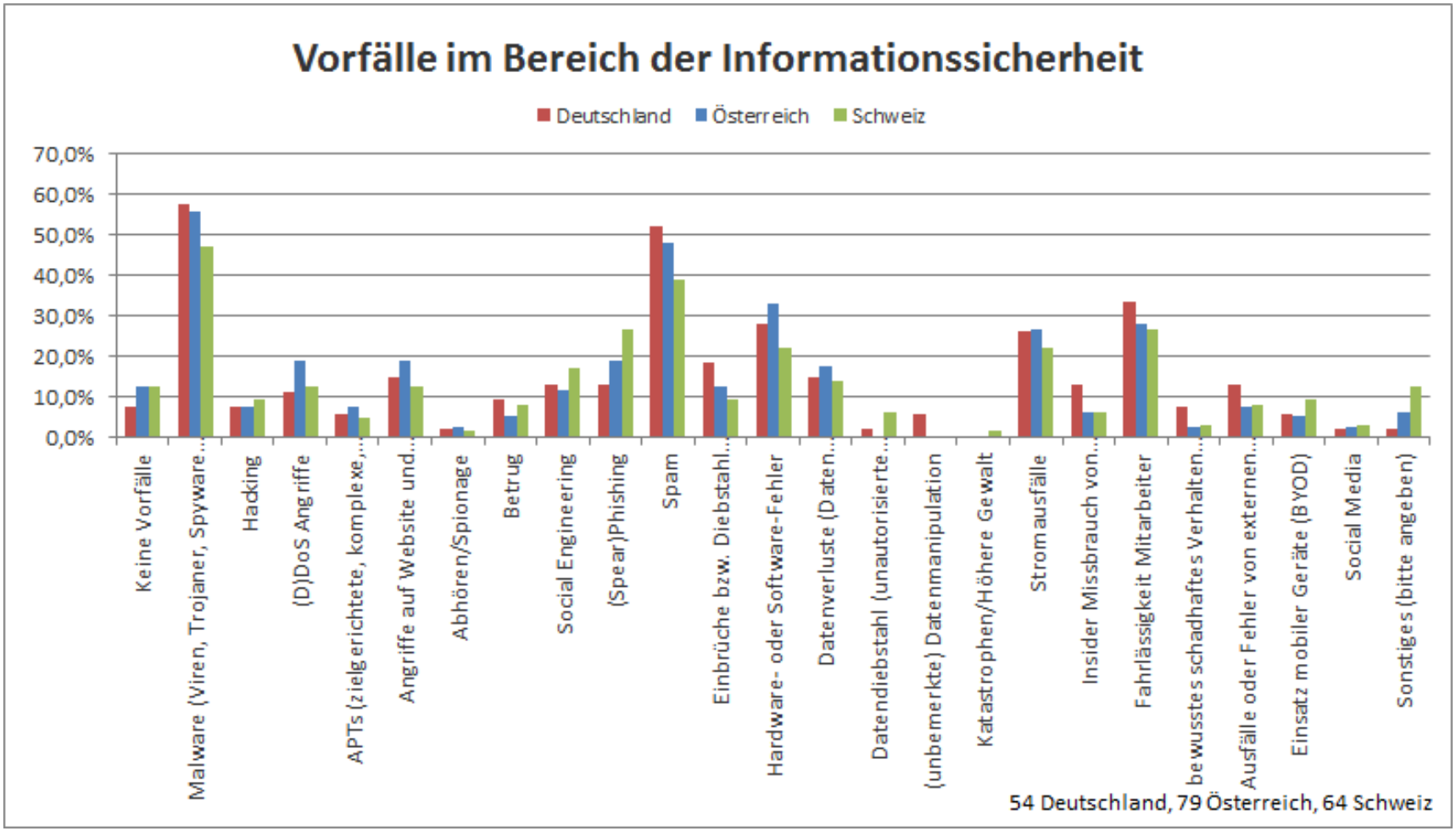
Ergebnisse länderspezifisch IV



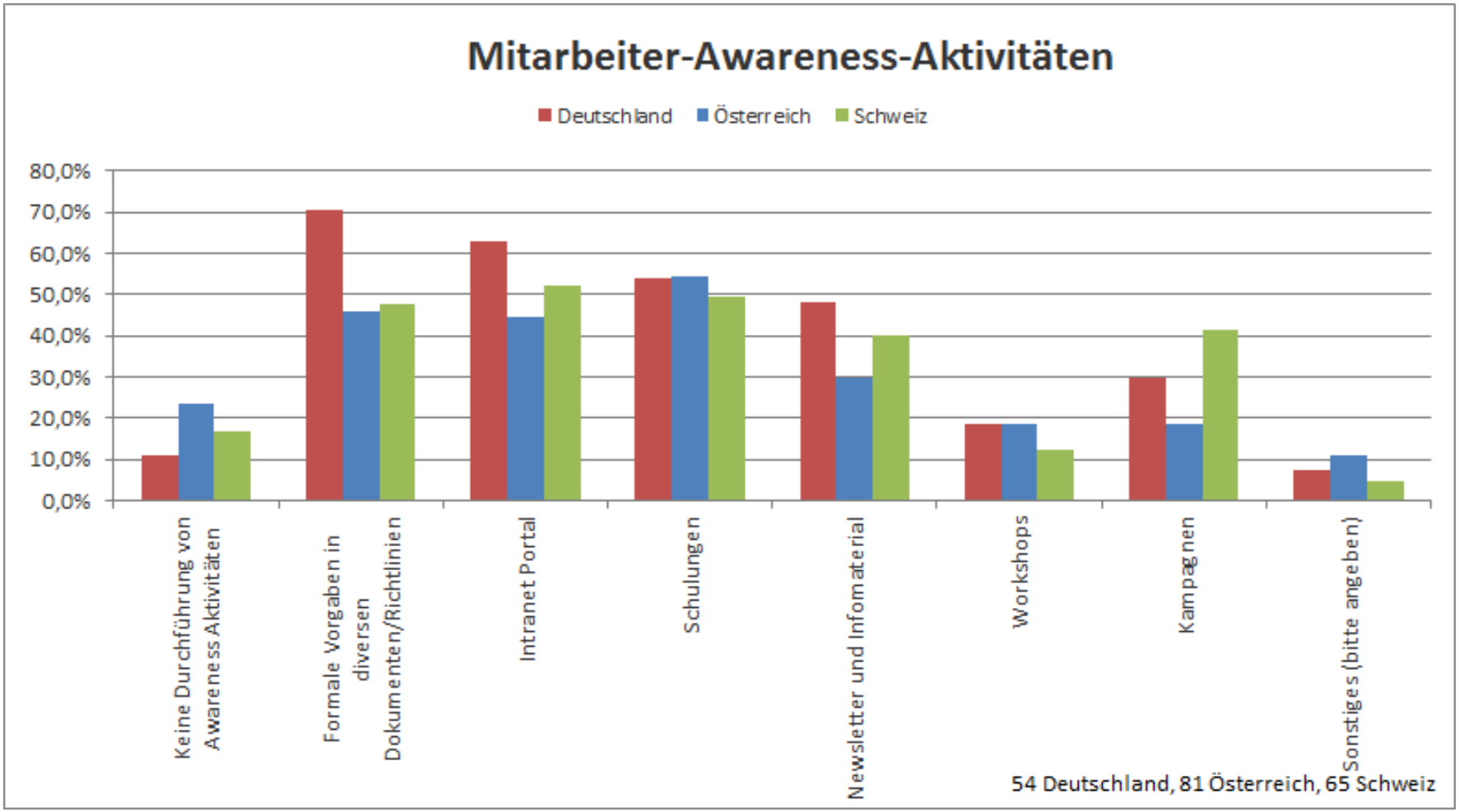
Ergebnisse länderspezifisch IV



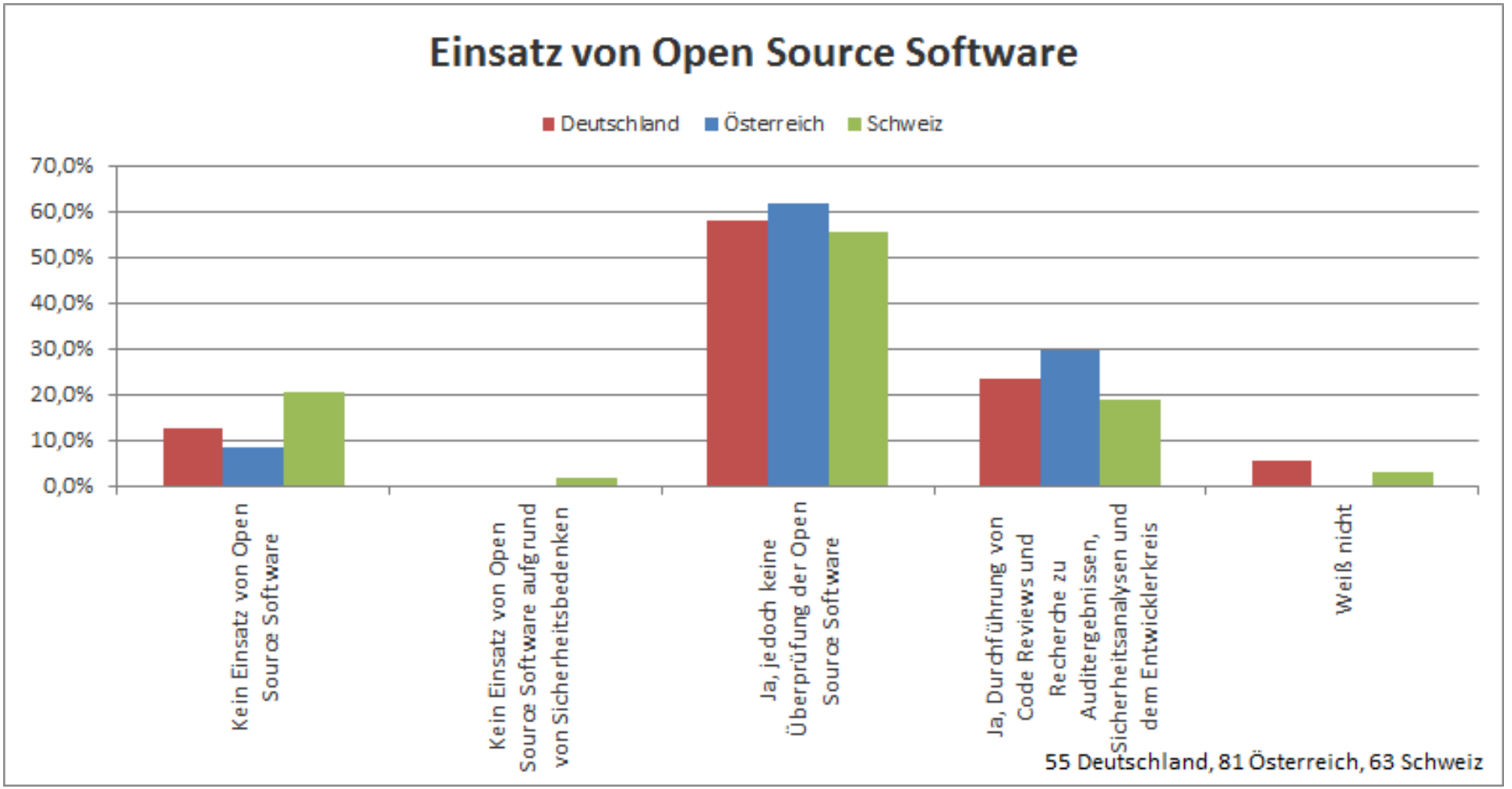
Ergebnisse länderspezifisch IV



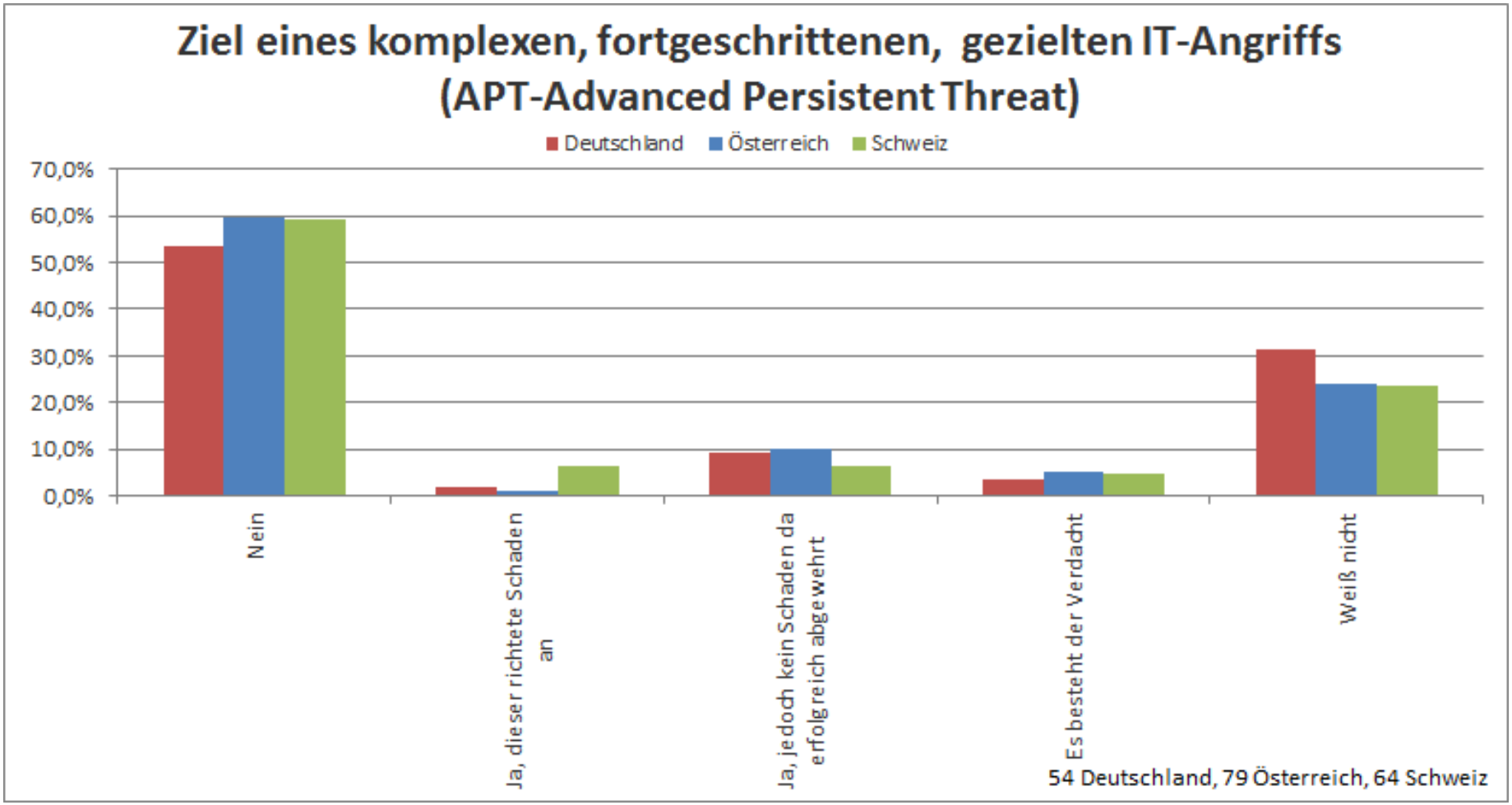
Ergebnisse länderspezifisch IV



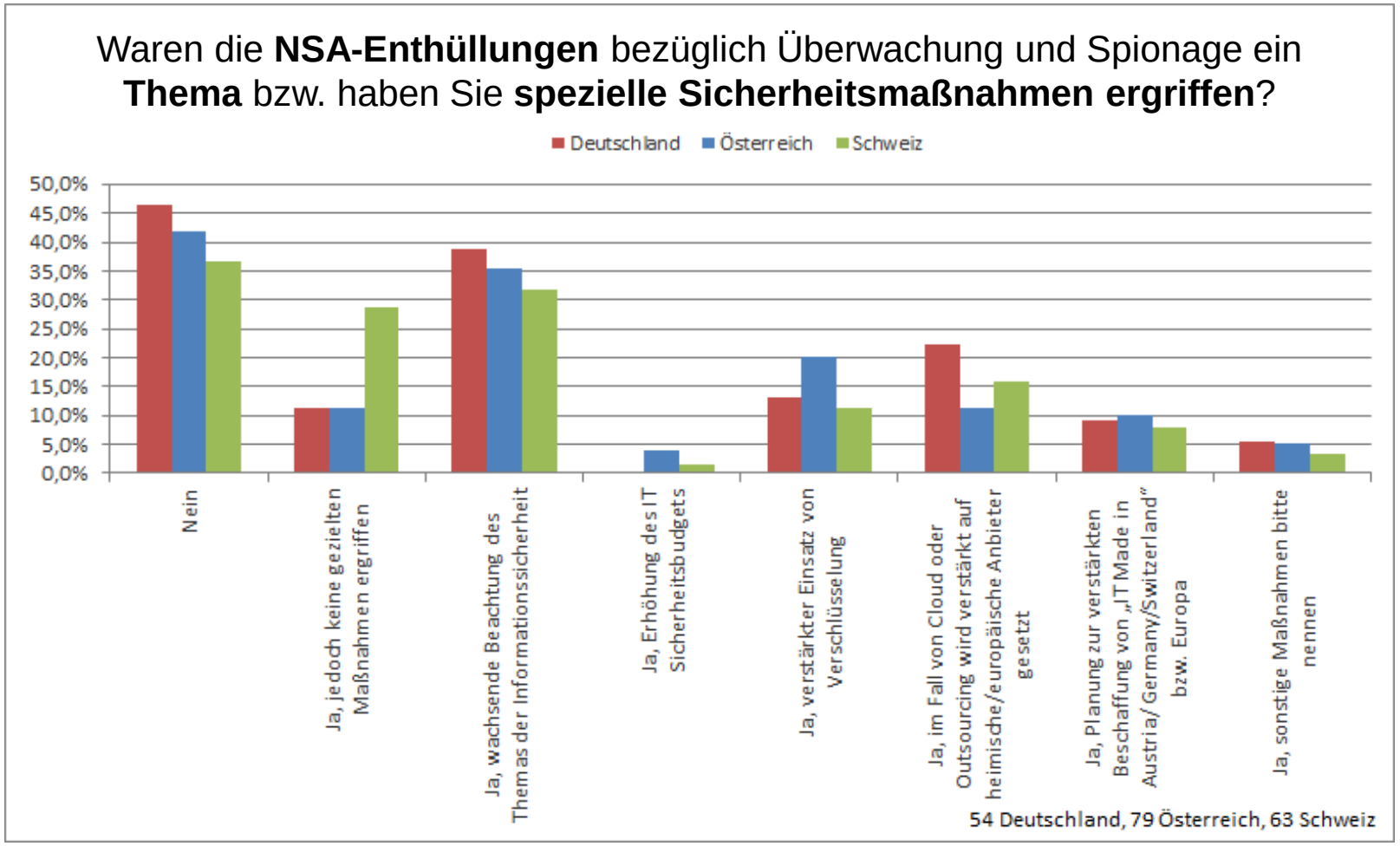
Ergebnisse länderspezifisch IV



Ergebnisse länderspezifisch IV



Ergebnisse länderspezifisch IV

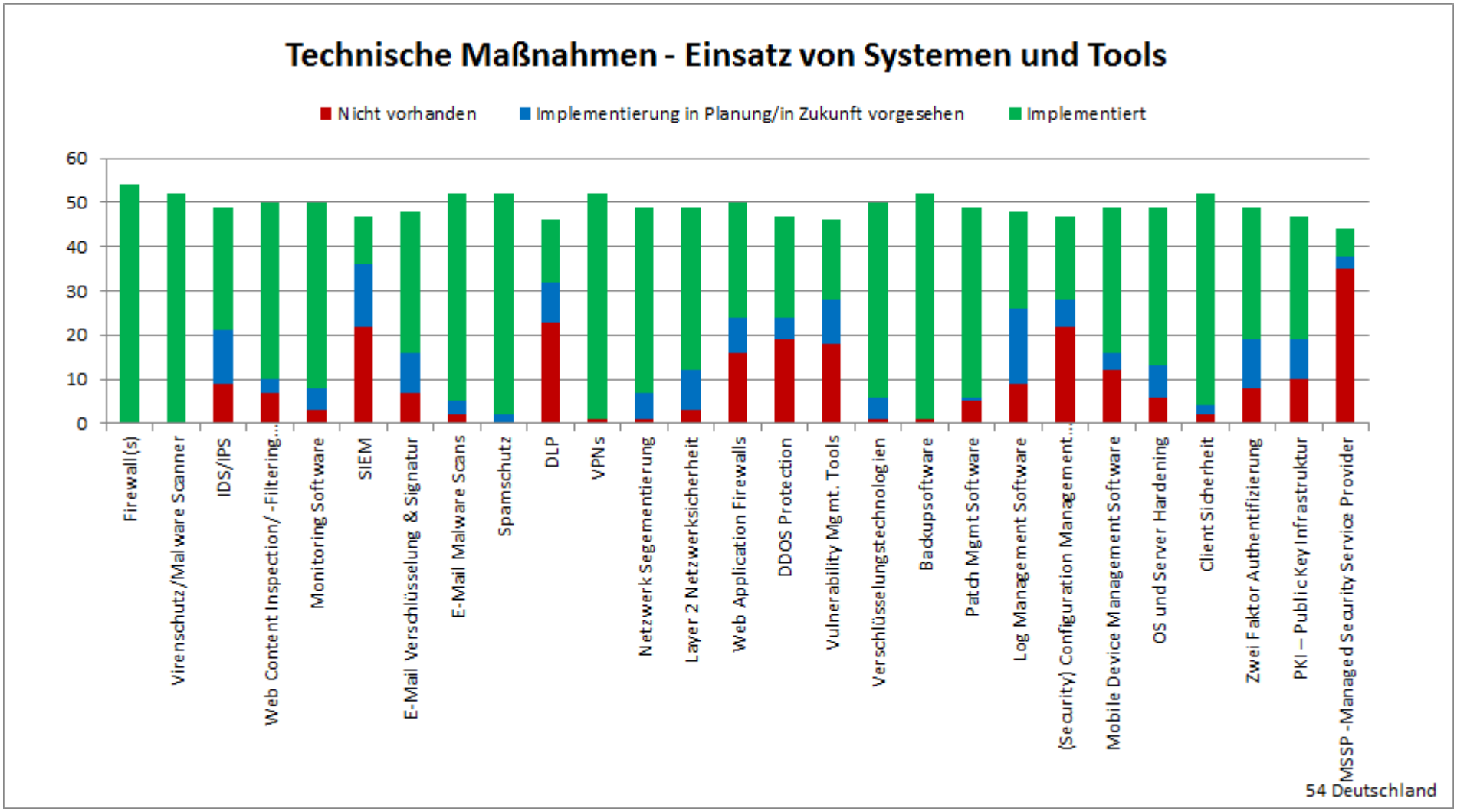


/informatik & security /fh/// st.pölten

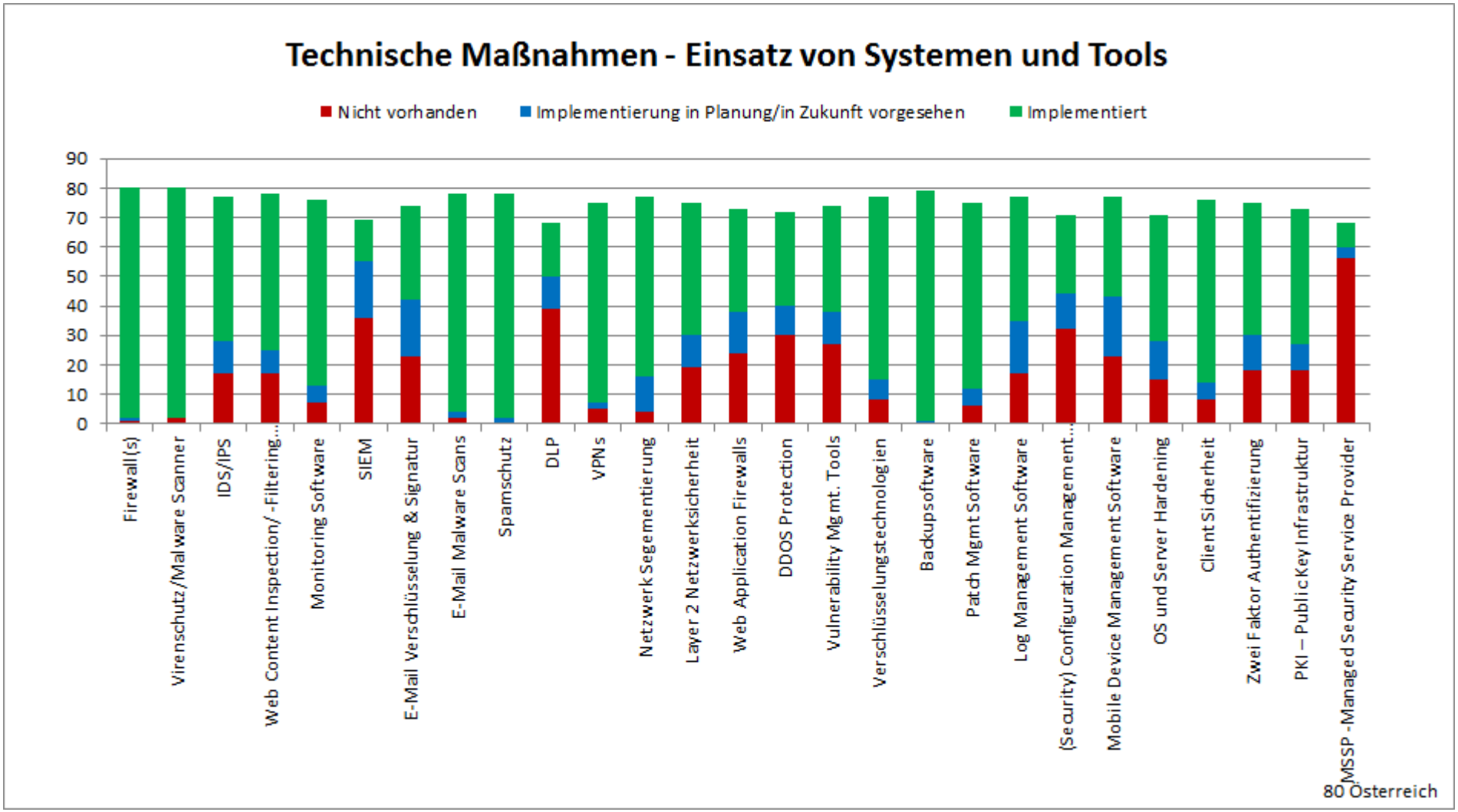
Technische und **organisatorische Aufstellung** der Unternehmen

ERGEBNISSE LÄNDERSPEZIFISCH V

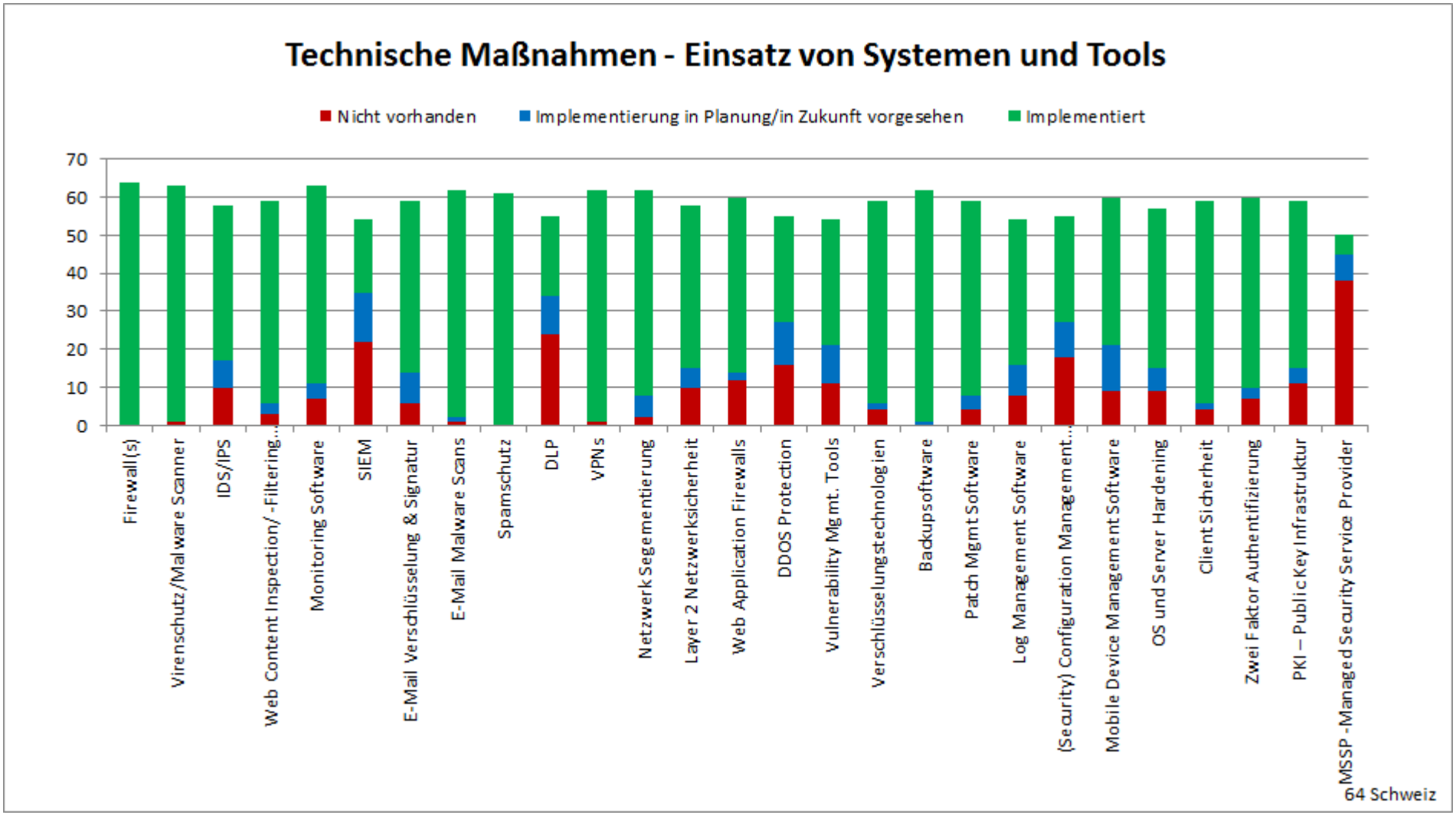
Ergebnisse Deutschland



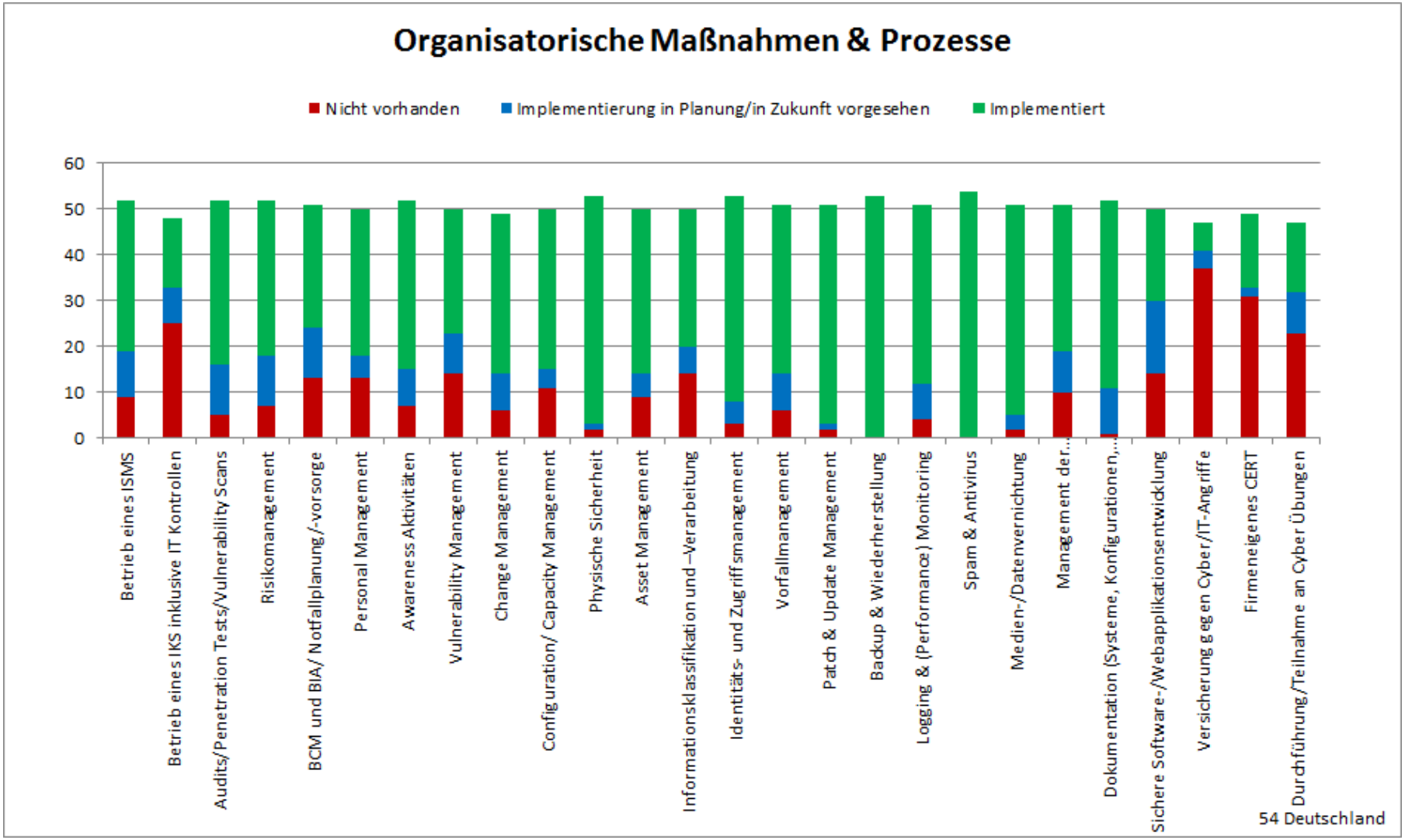
Ergebnisse Österreich



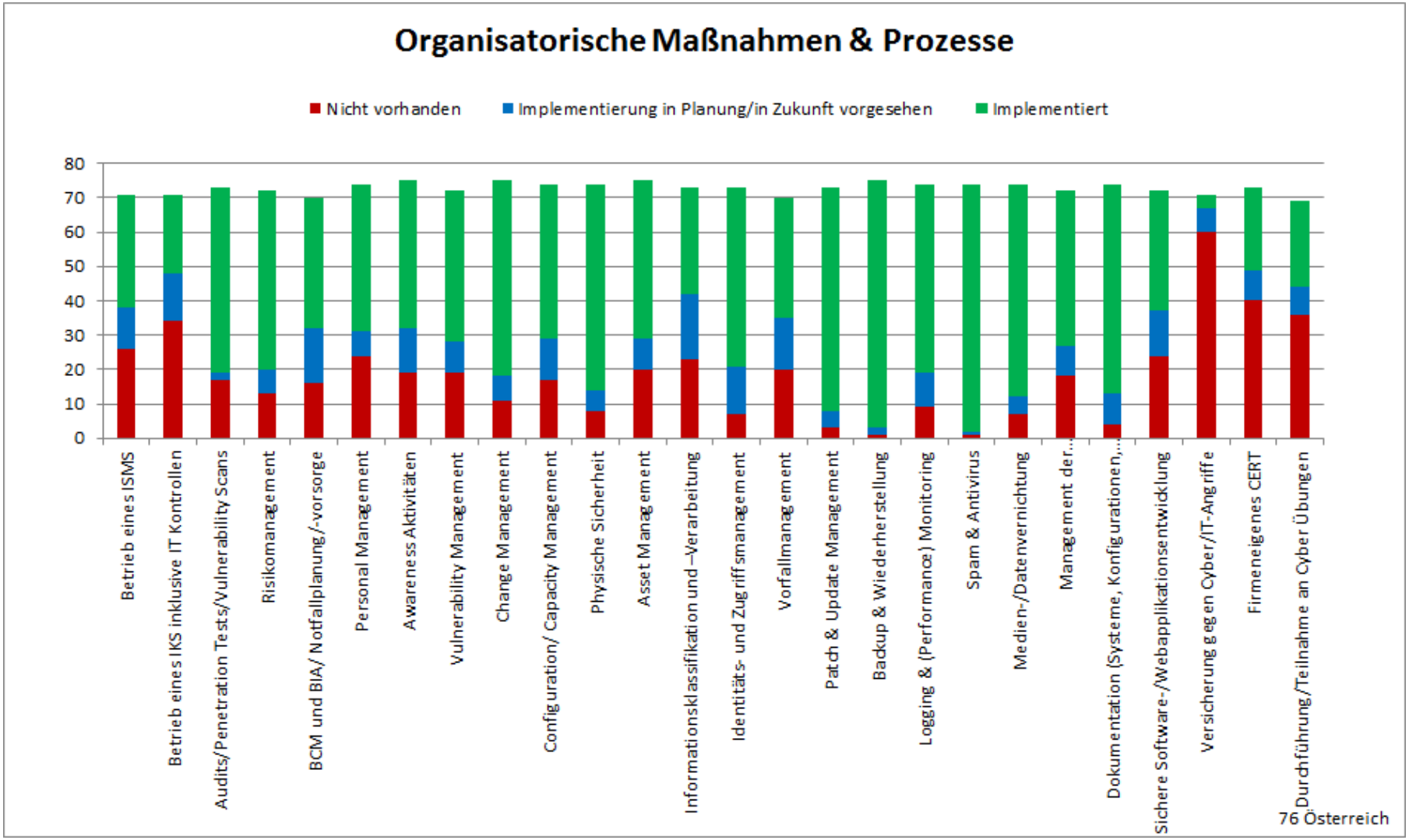
Ergebnisse Schweiz



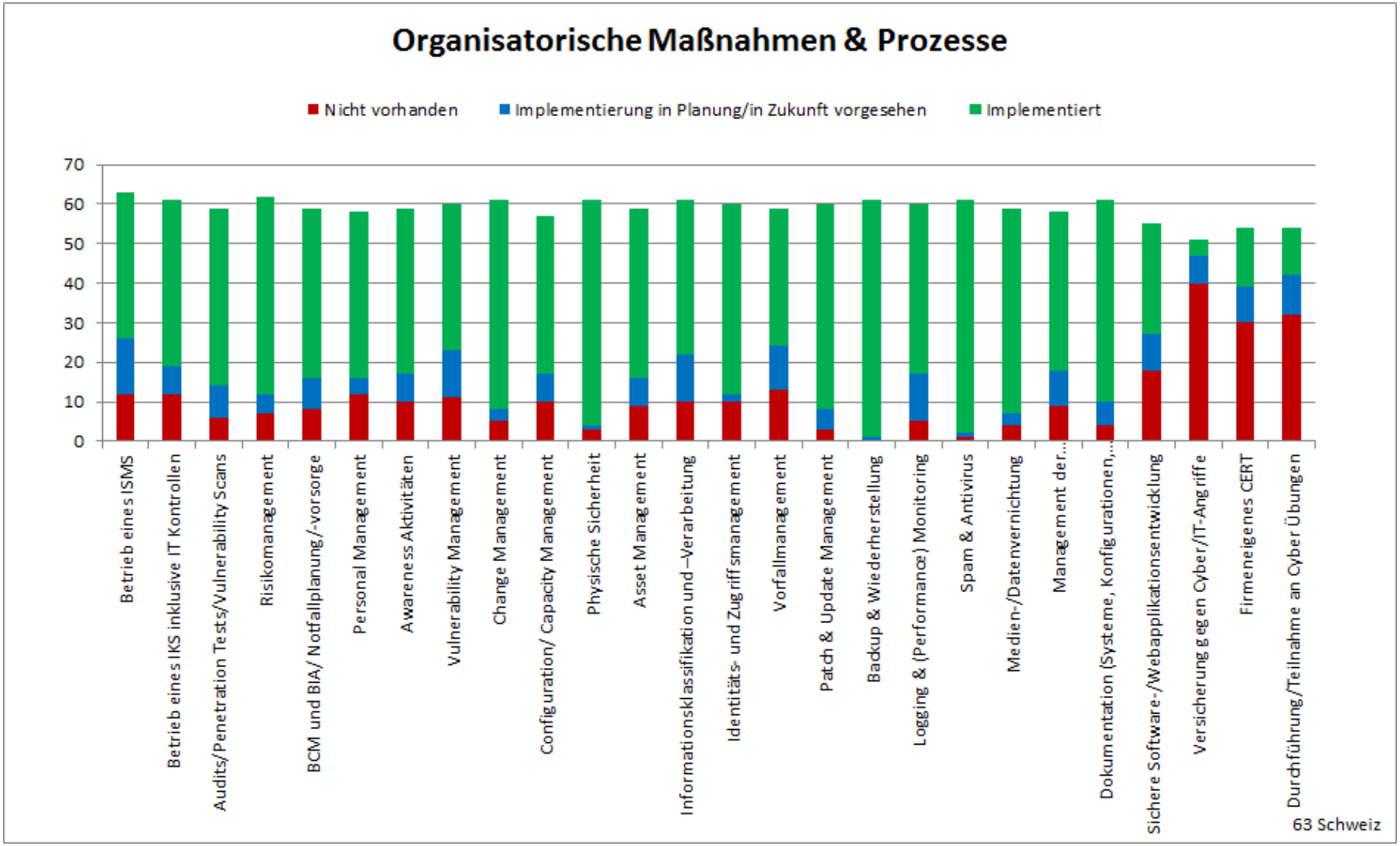
Ergebnisse Deutschland



Ergebnisse Österreich



Ergebnisse Schweiz



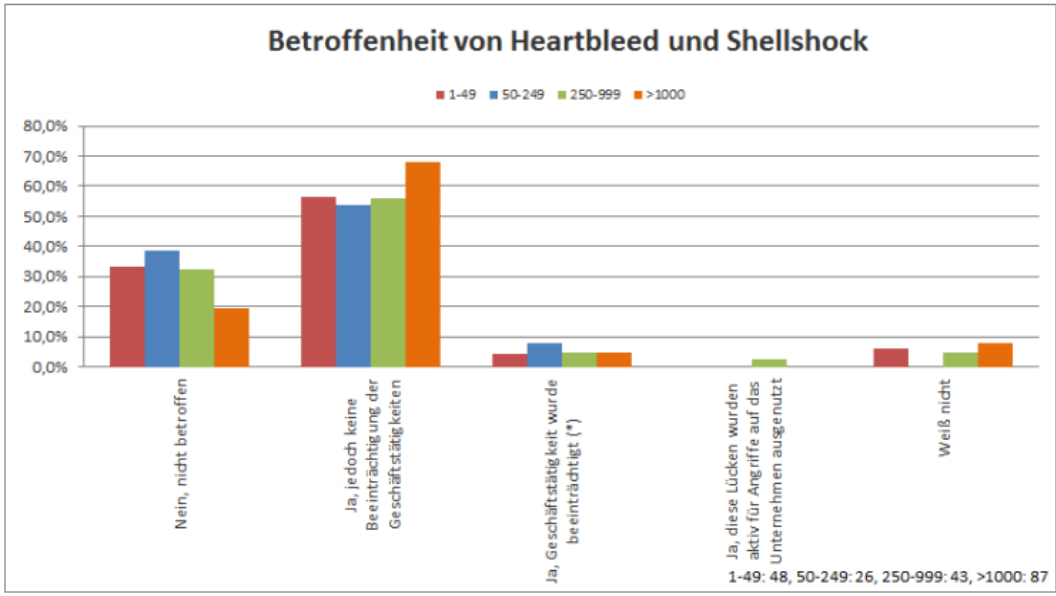
/informatik & security /fh/// st.pölten

Shellshock und **Heartbleed,** Interesse **heimische/europäische IT** nach **NSA-Enthüllungen,** Nutzung **Standards, technische** und **organisatorische Aufstellung** nach **Unternehmensgröße**

HYPOTHESEN

Hypothesen

- Hypothese V: Großteil der Unternehmen war von **Sicherheitslücken** wie **Heartbleed** oder **Shell Shock betroffen**, wobei dies jedoch große Unternehmen häufiger angeben.
  - **Beinahe zwei Drittel** der Unternehmen von diesen Lücken **betroffen**. Allerdings nur bei einer **Minderheit tatsächlichen Beeinträchtigung** der **Geschäftstätigkeiten** oder **Angriffe**
  - **Große** Unternehmen **öfter betroffen**
  - **Achtung**: tatsächliche Ausnutzung dieser Lücken (insb. Heartbleed) nur schwer bzw. kaum nachweis-bar → **ev. Angriffe nicht erkannt**?



Hypothesen

- Hypothese VIII: Nach dem NSA-Skandal gibt es größeres Interesse für heimische/europäische IT. Dies gilt insbesondere für Unternehmen aus Deutschland. Für kleine Firmen ist das Thema nicht sehr wichtig.
  - nur bedingte Aussage möglich. Grundsätzlich nur **Minderheit** von 9,3% der Unternehmen „**Planung** zur verstärkten **Beschaffung** von **IT made** in **Austria/Germany/Switzerland** bzw. **Europe**“
  - keine Vergleichsdaten (zu Jahren vor Enthüllungen)
  - Interesse an heimischer bzw. europäischer IT in Deutschland, Österreich und der Schweiz **ungefähr gleich hoch** (9,3% D, 10,1% Ö, 7,9% CH)
  - Aber: **Auch für kleine Unternehmen bedeutend** (12,2% der kleinen Unternehmen zu ebenfalls nur 9,3% bei Unternehmen >1000)
  - vertiefende Untersuchung und Marktforschung sicherlich interessant
    .

Hypothesen

- Hypothese X: Insbesondere in kleinen Unternehmen ist die Nutzung von Standards/Empfehlungen im Bereich der Informationssicherheit nicht sehr weit verbreitet.
  - Kann **bestätigt** werden. Über **28% der kleinen Unternehmen** (1-49) **keine Nutzung** Standards oder Empfehlungen
  - im Vergleich zu Unternehmen **50-249:10%**, **250-999: 7%**, **>1000 10%**
  - **Generell Nutzung** von **Standards** oder Empfehlungen jedoch **relativ weit verbreitet**. Insgesamt lediglich 12,7% keine Verwendung.
  - Höchste Verbreitung weisen **ISO 27001**, **BSI-Grundschutz** und **ITIL** auf, sowie bei großen Unternehmen (>1000) auch **COBIT**.

Hypothesen

- Hypothesen XV und XVI: Die technische Aufstellung der Unternehmen ist oft besser als die organisatorische. Viele organisatorische Maßnahmen werden erst in großen Unternehmen eingesetzt. KMU sind schlechter aufgestellt als große Unternehmen.
  - Generell **mehr technische Maßnahmen** mit **sehr hohem Umsetzungsgrad** → siehe Auswertungen zuvor
  - **Insgesamt** über alle Maßnahmen: knapp über **71% der technischen „implementiert“** im Vergleich zu **66% der organisatorischen**

Maßnahmen: Summe aller Maßnahmen, ***Imp***: Implementiert, ***Pl***: Implementierung in Planung/ in Zukunft vorgesehen, ***NA***: Nicht vorhanden

Maßnahmen	*Imp*	*Pl*	*NA*	*Summe*
Technisch	71,27%	10,59%	18,14%	
Anzahl Beantwortungen	3761	559	957	5277
Organisatorisch	66,72%	12,29%	20,98%	
Anzahl Beantwortungen	3294	607	1036	4937

Umsetzung technischer und organisatorischer Maßnahmen nach Unternehmensgröße

/informatik & security /fh/// st.pölten

Organisatorische Maßnahmen	1-49	50-249	250-999	>1000
Betrieb eines ISMS	25,58%	50,00%	56,41%	72,62%
Betrieb eines IKS inklusive IT Kontrollen	19,05%	37,50%	40,54%	64,63%
Audits/Penetration Tests/Vulnerability Scans	52,38%	65,38%	71,05%	89,29%
Risikomanagement	54,55%	69,23%	68,42%	87,06%
BCM und BIA/ Notfallplanung/-vorsorge	39,53%	73,08%	52,78%	73,17%
Personal Management	44,44%	64,00%	56,76%	80,00%
Awareness Aktivitäten	45,45%	57,69%	74,36%	76,19%
Vulnerability Management	40,91%	61,54%	62,16%	70,37%
Change Management	56,82%	73,08%	86,84%	89,29%
Configuration/ Capacity Management	51,11%	65,38%	70,27%	75,00%
Physische Sicherheit	73,33%	92,31%	89,47%	96,51%
Asset Management	45,45%	64,00%	71,05%	81,93%
Informationsklassifikation und -Verarbeitung	40,00%	38,46%	56,76%	69,88%
Identitäts- und Zugriffsmanagement	67,44%	69,23%	75,68%	88,51%
Vorfallmanagement	31,82%	50,00%	66,67%	76,54%
Patch & Update Management	85,71%	92,31%	81,58%	95,29%
Backup & Wiederherstellung	93,33%	96,15%	100,00%	98,84%
Logging & (Performance) Monitoring	66,67%	80,77%	64,86%	80,95%
Spam & Antivirus	93,33%	100,00%	97,30%	100,00%
Medien-Datenvernichtung	77,78%	91,67%	78,38%	95,24%
Management der Leistungserbringung/Verträge Externe IT Dienstleister	40,48%	65,38%	63,16%	79,27%
Dokumentation (Systeme, Konfigurationen, Organisatorische Prozesse etc.)	78,26%	76,92%	79,49%	86,75%
Sichere Software-/Webapplikationsentwicklung	45,65%	40,00%	48,65%	52,63%
Versicherung gegen Cyber/IT-Angriffe	6,82%	8,33%	2,86%	14,29%
Firmeneigenes CERT	20,93%	23,08%	22,22%	46,75%
Durchführung/Teilnahme an Cyber Übungen	21,43%	12,00%	30,56%	43,84%
*Anzahl Beantwortungen bis zu (*4.3)*	*46*	*26*	*39*	*88*

Legende: Hell-/Dunkelgrau Min/Max der Zeilen

Technische Maßnahmen	1-49	50-249	250-999	>1000
Firewall(s)	95,83%	100,00%	100,00%	100,00%
Virenschutz/Malware Scanner	93,48%	100,00%	100,00%	100,00%
IDS/IPS	48,89%	61,54%	59,46%	76,83%
Web Content Inspection/ -Filtering /Monitoring	50,00%	79,17%	89,74%	89,29%
Monitoring Software	75,56%	88,00%	80,49%	88,24%
SIEM	14,63%	30,43%	16,22%	36,11%
E-Mail Verschlüsselung & Signatur	53,33%	52,00%	45,95%	76,25%
E-Mail Malware Scans	91,49%	92,31%	97,44%	95,40%
Spamschutz	95,65%	92,31%	100,00%	100,00%
DLP	23,08%	25,00%	20,00%	44,59%
VPNs	88,64%	100,00%	95,00%	97,70%
Netzwerk Segmentierung	79,07%	88,46%	90,24%	82,35%
Layer 2 Netzwerksicherheit	42,22%	72,00%	84,62%	75,95%
Web Application Firewalls	46,67%	44,00%	71,05%	67,07%
DDOS Protection	39,13%	36,00%	48,48%	58,11%
Vulnerability Mgmt. Tools	36,36%	54,17%	40,54%	65,33%
Verschlüsselungstechnologien	78,26%	80,00%	81,08%	94,05%
Backupsoftware	93,62%	100,00%	100,00%	100,00%
Patch Mgmt Software	71,11%	80,00%	91,67%	94,05%
Log Management Software	45,45%	65,38%	51,43%	66,25%
(Security) Configuration Management Software	34,88%	33,33%	38,24%	55,84%
Mobile Device Management Software	29,55%	48,00%	65,00%	73,49%
OS und Server Hardening	65,91%	54,17%	66,67%	75,64%
Client Sicherheit	81,82%	88,00%	84,21%	91,67%
Zwei Faktor Authentifizierung	45,45%	69,23%	65,79%	81,71%
PKI-Public Key Infrastruktur	55,56%	61,54%	60,00%	78,48%
MSSP-Managed Security Service Provider	7,14%	12,00%	5,88%	21,21%
*Anzahl Beantwortungen bis zu (*4.3)*	*48*	*26*	*42*	*89*

Legende: Hell-/Dunkelgrau Min/Max der Zeilen

Hypothesen

- **Achtung**: höhere Umsetzungsraten und „**bessere“ Ergebnisse großer Unternehmen nicht** unbedingt in **direktem Zusammen-hang** (Ursache –> Wirkung) zur **Unternehmensgröße** alleine
- eher besteht eine gewisse **Korrelation:**
  - Bei Großen Nutzung von Standards (etwa ISO 27002) weiter verbreitet, welche sich ebenfalls sehr stark auf die organisatorische und technische Aufstellung der Unternehmen auswirken kann
  - Betrieb eines ISMS „nur“ in knapp einem Viertel der Kleinen, im Vergleich zu beinahe drei Viertel der Unternehmen >1000
- neben Unternehmensgröße **weitere Faktoren** wie **Bewusstsein** für Informationssicherheit, deren **Stellenwert** bzw. **Notwendigkeit** im **Unternehmenskontext**, **Nutzung** von **Standards** etc.

/informatik & security /fh/// st.pölten

Limitations of Validity, Links & Fragen, Weitere Informations-sicherheits-Studien

WEITERE INFORMATIONEN

Limitations of Validity

- diverse Faktoren und **Einschränkungen** bei Verteilung und Durchführung der Umfrage (insbesondere Selbst-Selektion, Stichprobengröße, unterschiedliche Stichprobenzusammensetzung im Ländervergleich)
- gewisse **Verzerrung der Ergebnisse** (Über-/Unterrepräsentation von Unternehmen gewisser Größe/Branche bzw. IT-Affinität & Sicherheitsbewusstsein etc.) **möglich** und **wahrscheinlich**.
- viele Teilnehmer **höheres Bewusstsein** und Interesse für das Thema der Informationssicherheit und **besser aufgestellt** als ein „**typisches durchschnittliches Unternehmen**“
- **kein Anspruch auf Repräsentativität**
- **Gesamtsituation** der Informationssicherheit in D, Ö und CH **könnte „anders“** bzw. **„schlechter**“ sein

Links & Fragen

- Studie selbst und Material:
  - download
- Berichte
  - FH
  - Computerwelt
  - IKT?

- Fragen & Vormerkung zukünftige Studie
  - bei Fragen bzw. Interesse oder Bereitschaft zur Teilnahme an zukünftiger Studie
  - gerne e-mail an Philipp Reisinger is131510@fhstp.ac.at

Weitere Informationssicherheits-Studien

- Weltweit
  - Information Week: Strategic Security Survey 2014
  - Ernst & Young: Global Information Security Survey 2014
  - Kaspersky: IT Security Risks Survey 2014
  - PWC, CIO Magazine, CSO Magazine: Global State of Information Security Survey 2015
- Studien Datenlecks und Vorfälle
  - Ponemon: Global Cost of Data Breach Study 2015
  - Verizon: Data Breach Investigation Report 2015

Weitere Informationssicherheits-Studien

- Deutschland
  - BSI: Cyber-Sicherheits-Umfrage 2014
  - Security Bilanz Deutschland 2015
  - <kes>/Microsoft-Sicherheitsstudie 2014
  - BITKOM: Digitale Wirtschaftsspionage, Sabotage und Datendiebstahl 2015
  - Corporate Trust: Studie: Industriespionage 2014
  - NIFIS: IT-Sicherheit und Datenschutz 2015

Weitere Informationssicherheits-Studien

- Österreich
  - Cyber Security Fitness Index Austria (inkl. KMU Cyber Security Monitor) 2015
  - Studie Informationssicherheit in österreichischen Unternehmen 2013
  - DAMON - Monitoring zur Datensicherheit in Österreich 2013
  - ASF: IT-Security in Österreich 2012
  - Informationssicherheit in österreichischen klein- und mittelständischen Unternehmen 2006
- Schweiz
  - Melani: Informationssicherheit in Schweizer Unternehmen 2006