Vorstellung und Diskussion der Studienergebnisse: IT-Sicherheitsstandards und IT-Compliance 2010

BSI, IT-Grundschutztag / it-sa 2010
Nürnberg, 20.10.2010

Dr. Stefan Kronschnabl, Research Director
ibi research an der Universität Regensburg GmbH

Kooperationspartner der Studie

research
an der Universität
Regensburg

Bundesamt
für Sicherheit in der
Informationstechnik

IT·Grundschutz
Informationsdienst

Agenda

1. Vorstellung der Kooperationspartner
2. Ziel, Durchführung und Aufbau der Studie
3. Teilnehmerstruktur
4. Wesentliche Ergebnisse

Agenda

1. **Vorstellung der Kooperationspartner**
2. Ziel, Durchführung und Aufbau der Studie
3. Teilnehmerstruktur
4. Wesentliche Ergebnisse

Institut für Bankinnovation (ibi research) an der Universität Regensburg GmbH

- Aktuelle Spitzenforschung gefördert durch BMBF und BMWI
- Entwicklung von Innovationen (Konzepte, Software) und Unterstützung bei der Umsetzung
- Anfertigung von Marktstudien und individuelle Beratung
- Know-How-Networking

Wie entwickeln sich die Informations- und Kommunikations-Technologien?

- Geräte und Infrastrukturen
- Softwaresysteme und Methoden

Schwerpunkte: Konvergenz, Standards, Potenziale

Wie verändert sich das Kundenverhalten?

- Privatkunden
- Geschäftskunden

Schwerpunkte: Technologienutzung und Akzeptanz, Kundenbedürfnisse

Wie verändert sich der Markt?

- Akteure und Rahmenbedingungen
- Treibende Kräfte

Schwerpunkte: Non- und Nearbanks, Fragmentierung, E-Business

Wie reagieren die Unternehmen?

- Strategie und IT-Systeme
- Organisation und Prozesse

Schwerpunkte: Vertriebsstrukturen, vernetzte Leistungserstellung, Systemarchitekturen

Partnernetzwerk

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Nationale Sicherheitsbehörde, zentraler IT-Sicherheits-dienstleister des Bundes
- **Ziel: „**Voranbringen“ der IT-Sicherheit in Deutschland
- Angebot für private und gewerbliche Nutzer und Anbieter von Informationstechnik
- **Anliegen:** enge Zusammenarbeit mit allen Akteuren der IT- und Internetbranche auf dem Gebiet der IT-Sicherheit

Bundesamt
für Sicherheit in der
Informationstechnik

IT-Grundschutz / SecuMedia Verlag

- Der **SecuMedia Verlag** liefert seit 30 Jahren verlässliche Informationen zum Thema Sicherheit
- Selbstverständnis:
  - Plattform für den Austausch von Informationen
  - Veröffentlichungen mit hohem Praxisbezug
- **Informationsdienst IT-Grundschutz:**
  - monatlich erscheinende, 16-seitige Fachblatt für CIOs, IT-Manager und Verantwortliche für Informationssicherheit
  - **Ziel:** Unterstützung bei der täglichen Arbeit und fundierte Berichterstattung über aktuelle Trends im Bereich IT-Sicherheit sowie Neues in Rechtsprechung, Technik und Anwendungen

IT·Grundschutz
Informationsdienst

Agenda

1. Vorstellung der Kooperationspartner
2. **Ziel, Durchführung und Aufbau der Studie**
3. Teilnehmerstruktur
4. Wesentliche Ergebnisse

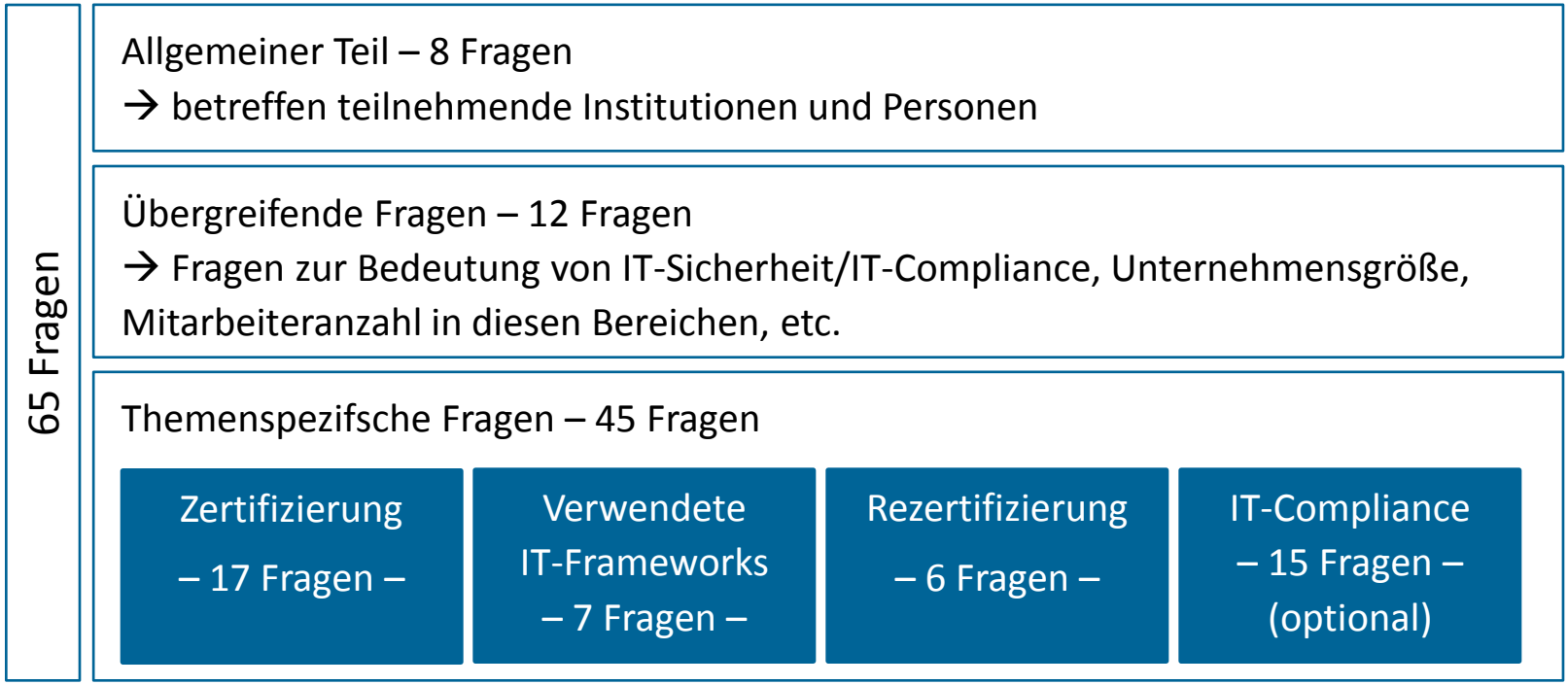
Ziele der Studie

- Aufzeigen des Status Quo und Entwicklungstendenzen hinsichtlich IT-Sicherheitsstandards und IT-Compliance:
  - Verwendung und Verbreitung von Standards bzw. IT-Frameworks
  - Umsetzung relevanter IT-Compliance Anforderungen
- Aufdeckung von Verbesserungspotentialen und Wünschen durch Anwender
- Darstellung von Schwächen vorhandener Softwarelösungen

Durchführung der Studie

- Offene Umfrage über Onlinebefragungstool sowie in gedruckter Form
- Aufforderung zur Teilnahme über
  - die Fachzeitschrift Banking and Information Technology (BIT),
  - den Informationsdienst IT-Grundschutz,
  - den Newsletter von ibi research,
  - den SecuMedia Verlag
  - sowie die Homepage des BSI.
- Zeitraum der Befragung: 04.05.2010 – 05.08.2010

Fragebogenstruktur



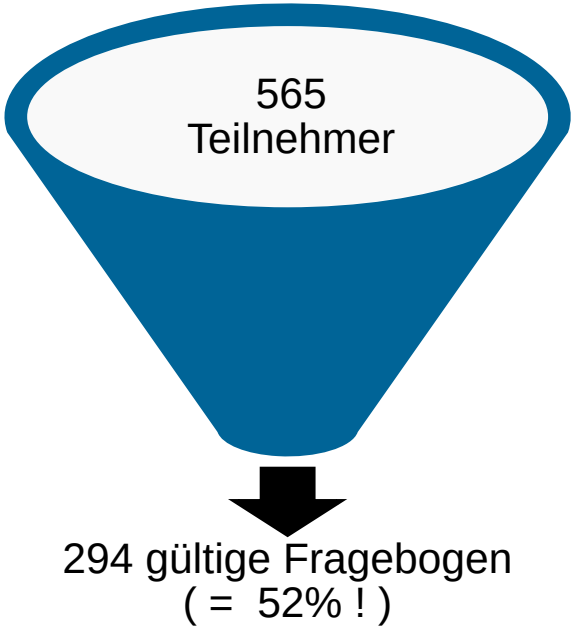
Durch optionale bzw. irrelevante Fragen variierte die Zahl der beantworteten Fragen je nach Teilnehmer zwischen 26 und 65.

Agenda

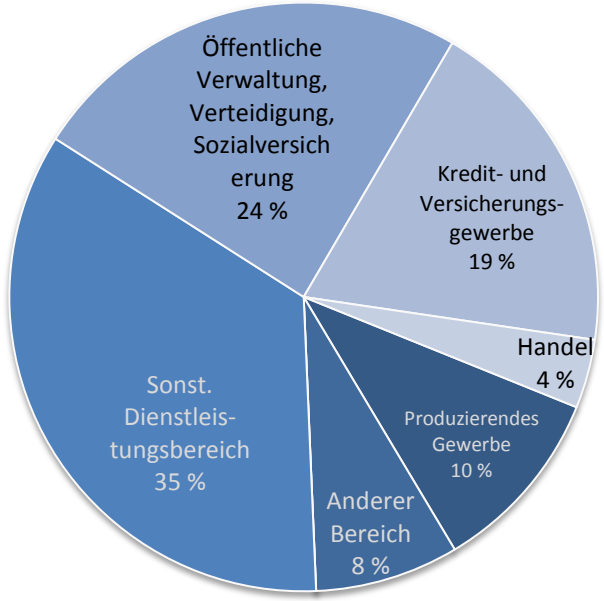
1. Vorstellung der Kooperationspartner
2. Ziel, Durchführung und Aufbau der Studie
3. **Teilnehmerstruktur**
4. Wesentliche Ergebnisse

Teilnehmeranzahl und -struktur

- Hohe Akzeptanz der Studie

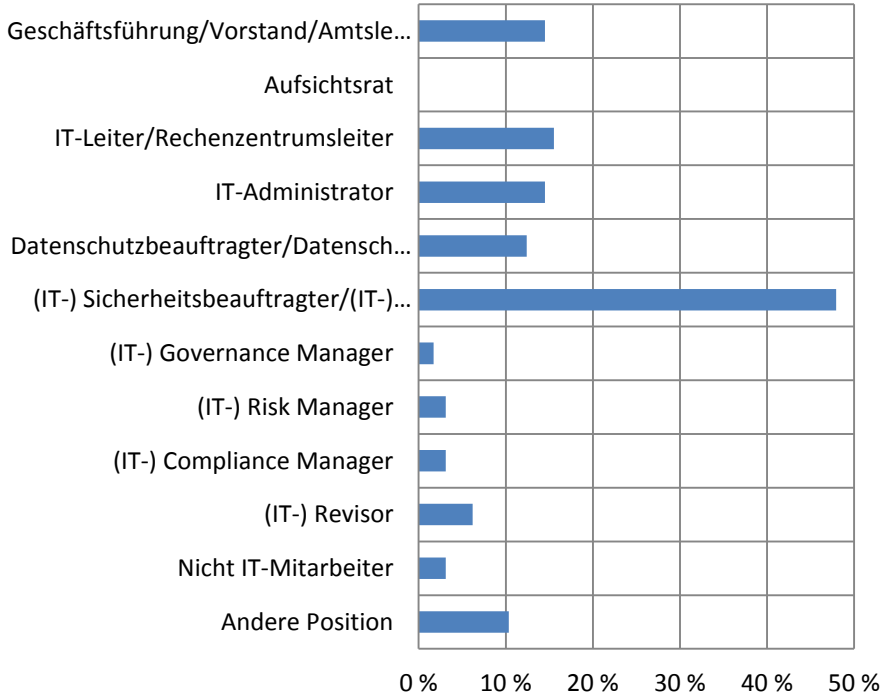


- Teilnehmer aus nahezu allen Branchen
- Aber: 82 % aus der Dienstleistungs-branche; Verteilung:

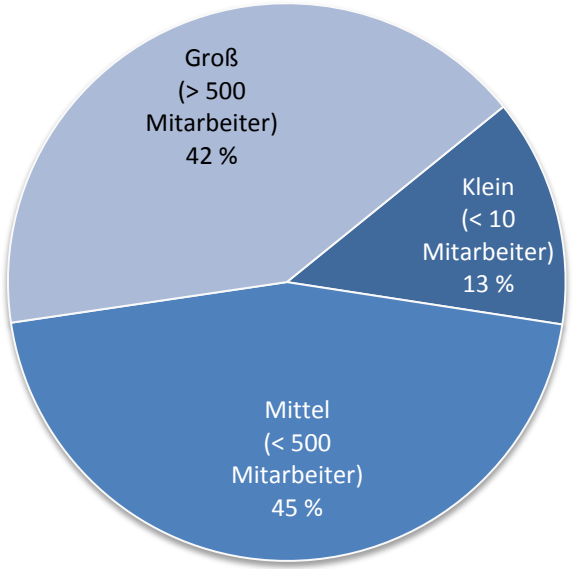


Teilnehmerstruktur

- Überwiegend wurde der Fragebogen durch (IT-) Sicherheitsbeauftragte ausgefüllt



- Die Beteiligung kleiner Unternehmen war sehr gering.
- IT-Sicherheitsbeauftragte nur bei 15 % in kleinen Unternehmen



Agenda

1. Vorstellung der Kooperationspartner

2. Ziel, Durchführung und Aufbau der Studie

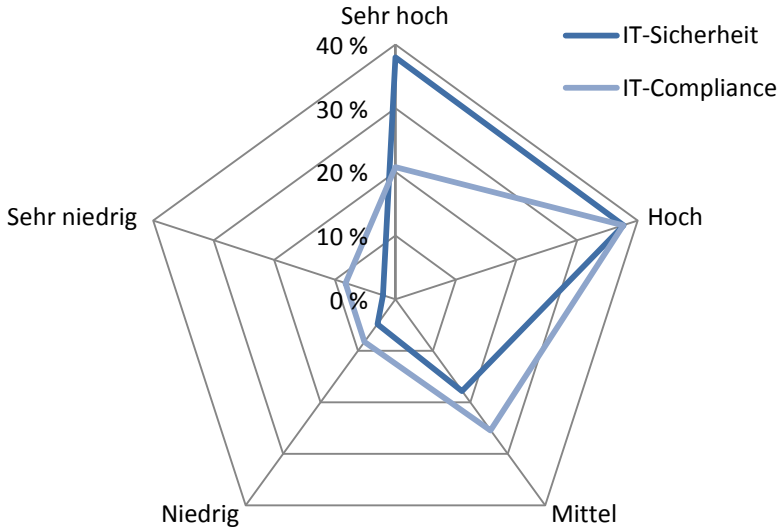
3. Teilnehmerstruktur

4. **Wesentliche Ergebnisse**

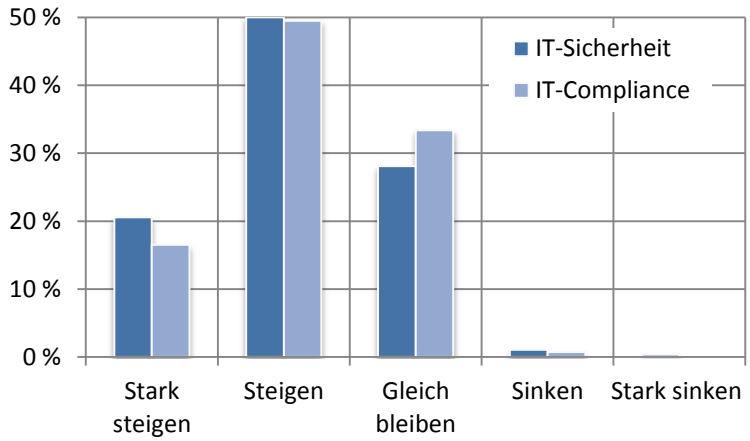
Themenblock 1: Bedeutung und Relevanz

Hohe Bedeutung der Thematik **unterstreicht die Relevanz der Studie**

- Hoher bis sehr hoher Stellenwert von IT-Sicherheit



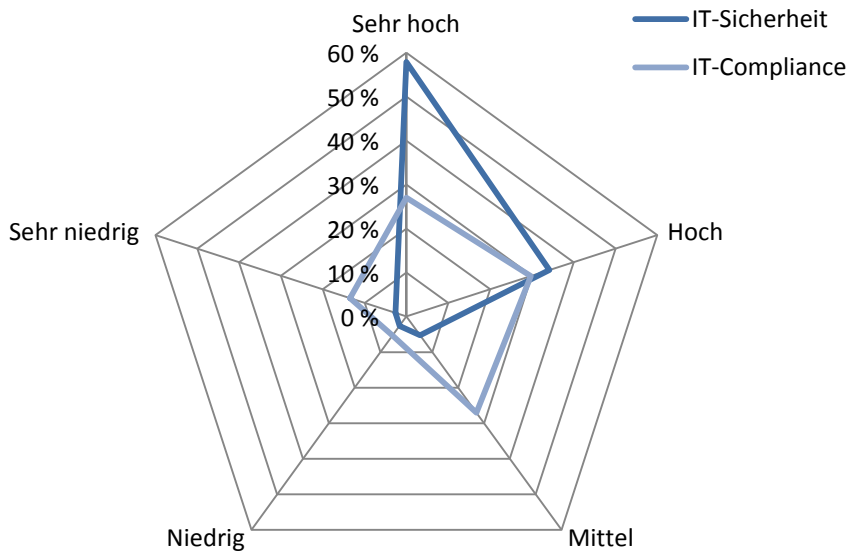
- Mehrheit geht von weiter steigender Bedeutung von IT-Sicherheit und IT-Compliance aus



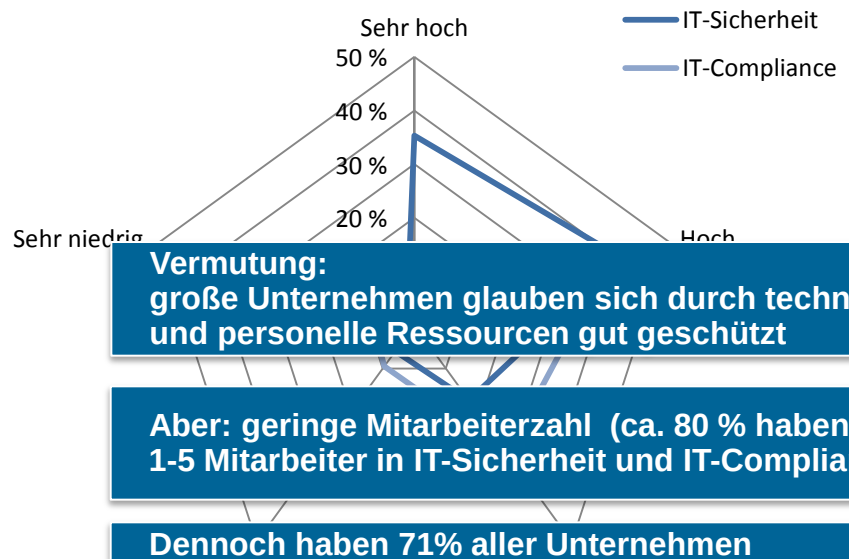
Bedeutung von IT-Sicherheit/IT-Compliance

- Allgemein: Bedeutung von IT-Sicherheit höher als von IT-Compliance
- Bedeutung von IT-Sicherheit bei kleinen Institutionen am größten

kleinen Institutionen



großen Institutionen



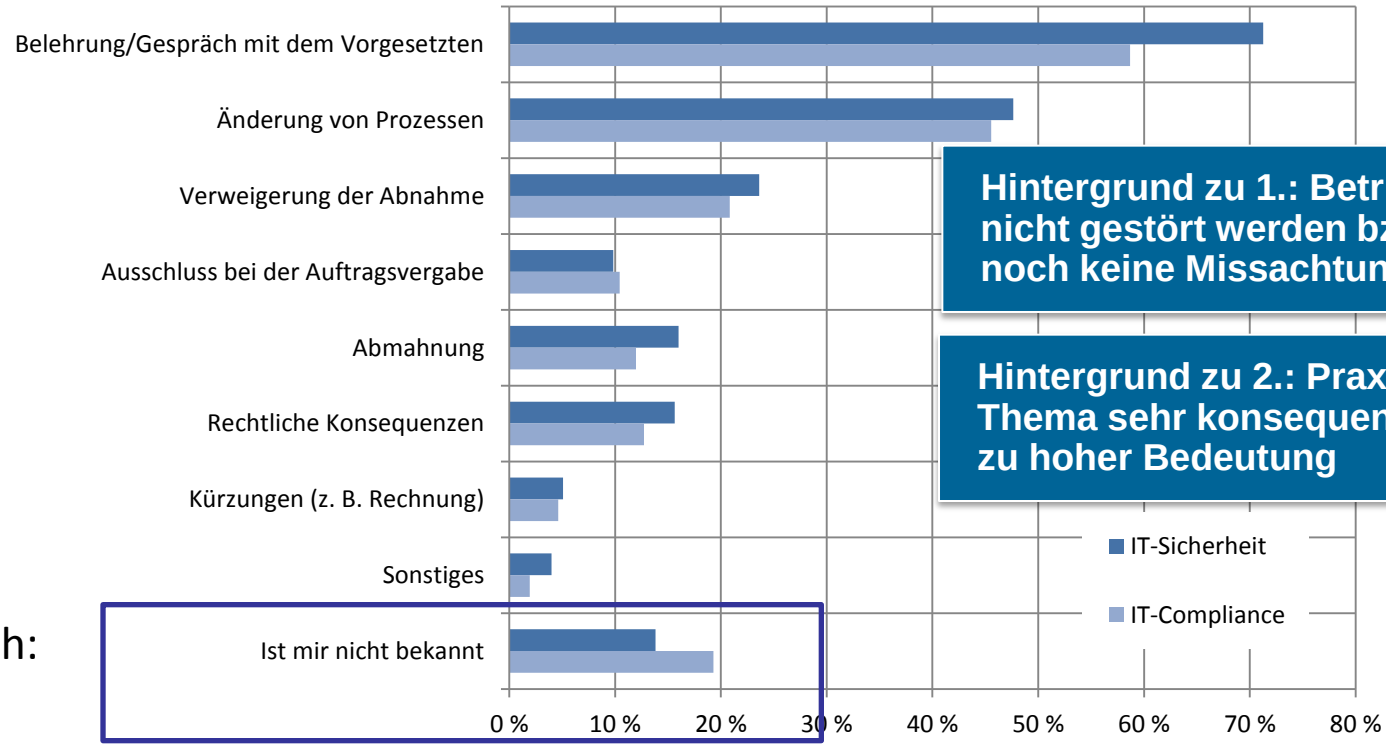
Vermutung:
große Unternehmen glauben sich durch technische und personelle Ressourcen gut geschützt

Aber: geringe Mitarbeiterzahl (ca. 80 % haben nur 1-5 Mitarbeiter in IT-Sicherheit und IT-Compliance)

Dennoch haben 71% aller Unternehmen Sicherheitsziele definiert; nur 8% wollen keine Sicherheitsziele definieren.

Hat hohe Bedeutung Auswirkungen auf die Vorgehensweise bei Missachtung von Vorgaben?

1. Belehrung/Gespräch mit dem Vorgesetzten meist der erste Schritt
2. Anpassung von Prozessen direkt als zweite Konsequenz



Hintergrund zu 1.: Betriebsfrieden soll nicht gestört werden bzw. es wurde noch keine Missachtung bekannt

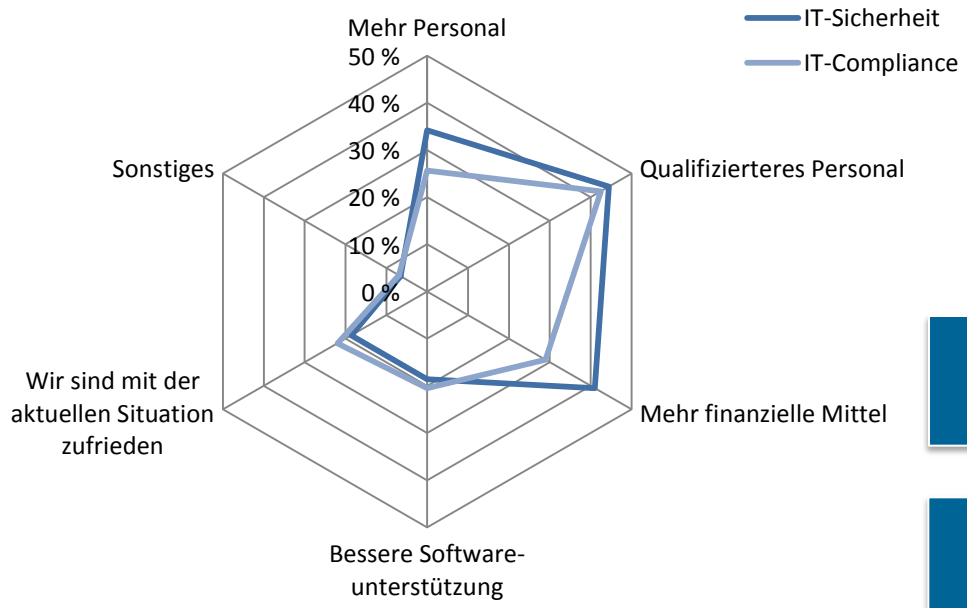
Hintergrund zu 2.: Praxis geht mit dem Thema sehr konsequent um, in Einklang zu hoher Bedeutung

Aber auch:

Themenblock 2: Optimierungshemmnisse

Hindernisse bei der Optimierung

- Steigende Anforderungen erfordern mehr finanziellen Mitteln und mehr qualifiziertes Personal
- 45 % der Befragten klagen über Mangel an Mitarbeiter in der IT-Sicherheit

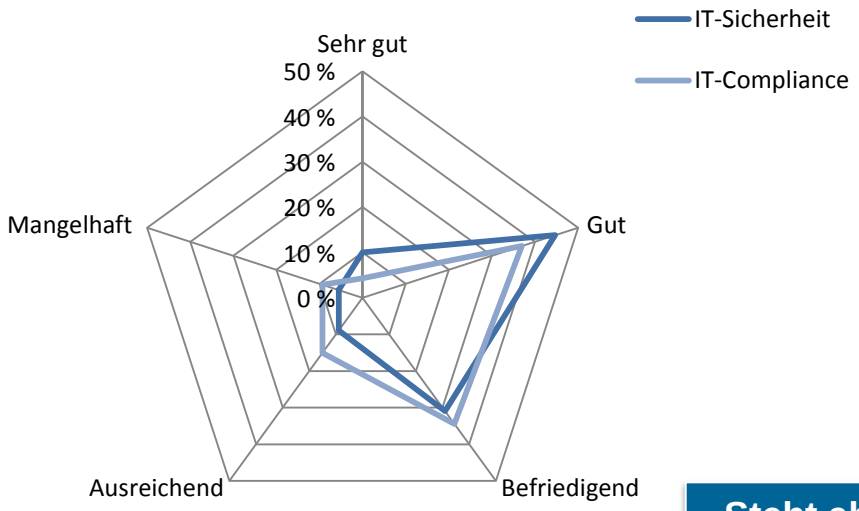


Personaldecke von oft nur 5 Mitarbeitern!

Steht in Diskrepanz zur hohen Bedeutung, die insb. der IT-Sicherheit zugestanden wird

Qualitätsbewertung der Umsetzung

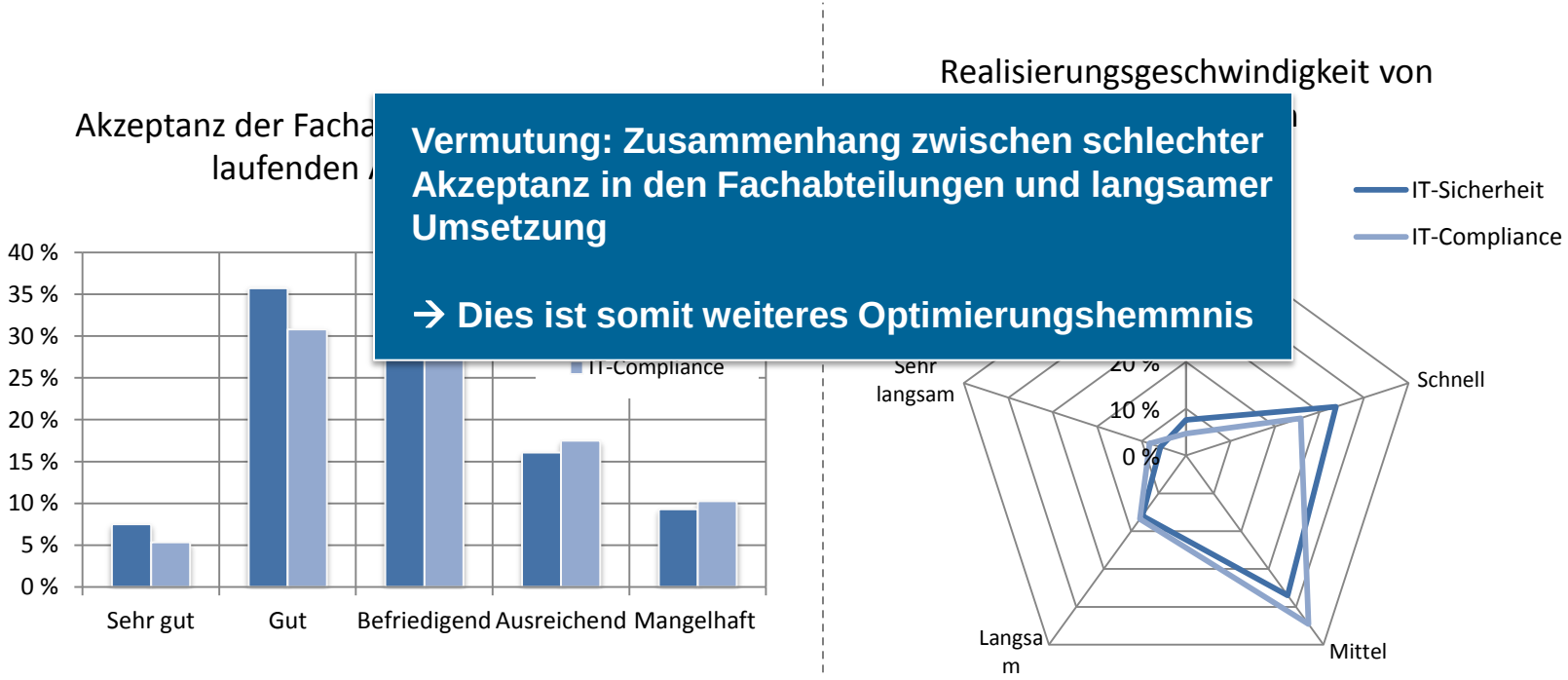
- Die meisten Teilnehmer bewerten ihre Umsetzung zu IT-Sicherheit und IT-Compliance als befriedigend bis gut



Steht ebenso in Diskrepanz zur hohen Bedeutung, die der IT-Sicherheit und IT-Compliance zugestanden wird

Bewertung der Umsetzung von Anforderungen

- Mangelnde Akzeptanz der Fachabteilungen durch (vermutlich) unzureichende Einbindung der Mitarbeiter
- Umsetzungsgeschwindigkeit meist nur mittelmäßig

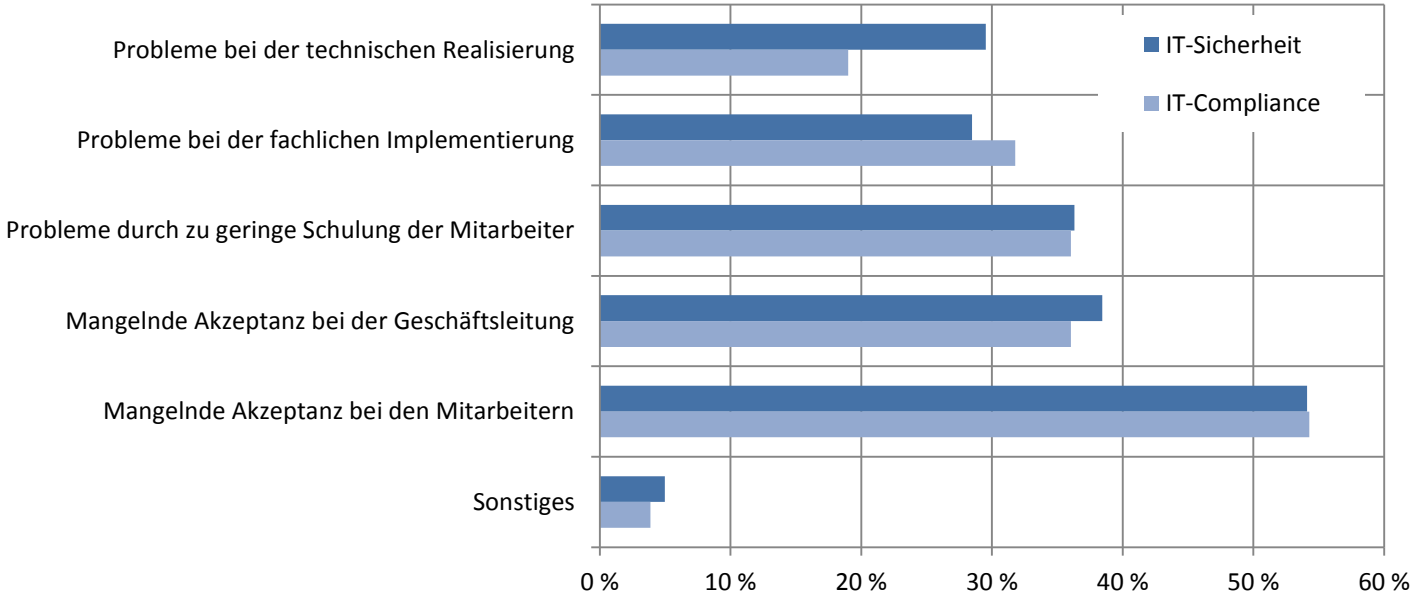


Vermutung: Zusammenhang zwischen schlechter Akzeptanz in den Fachabteilungen und langsamer Umsetzung

→ Dies ist somit weiteres Optimierungshemmnis

Hintergrund: Hauptprobleme des IT-Sicherheit und IT Compliance Managements

- Mangelnde Akzeptanz bei Mitarbeitern und Geschäftsleitung
- Ebenso Unterstützung durch die Geschäftsführung, Vorstand oftmals zu gering

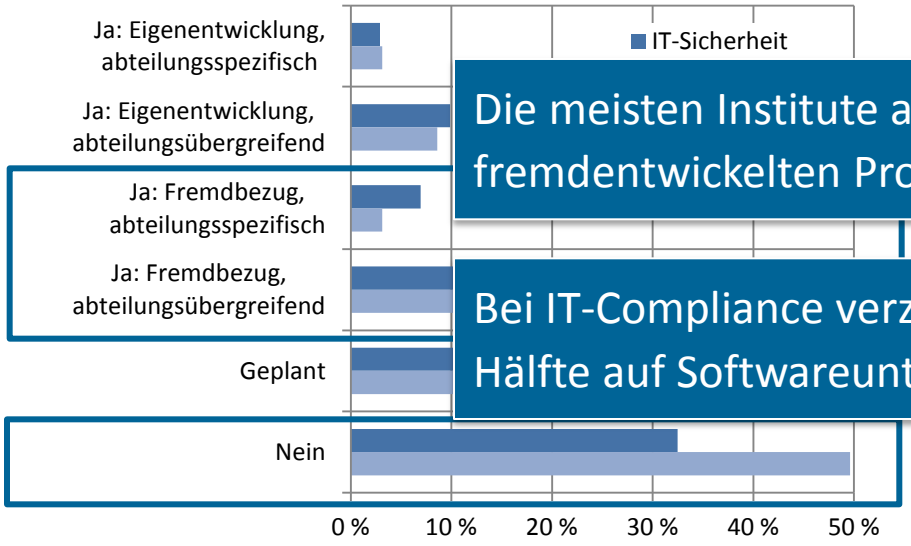


Themenblock 3: Softwareunterstützung und Zertifizierung

Software und deren Mängel

- Softwareunterstützung im Bereich IT-Sicherheit ausgeprägter als im Bereich IT-Compliance
- Dilemma der Hersteller: Mehr Funktionsumfang zu niedrigerem Preis gefordert

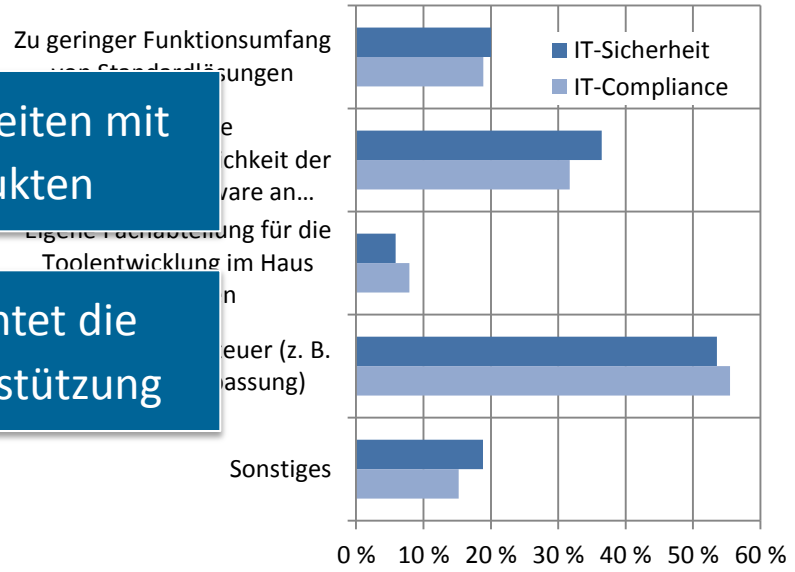
Wird durch Software unterstützt?



Die meisten Institute arbeiten mit fremdentwickelten Produkten

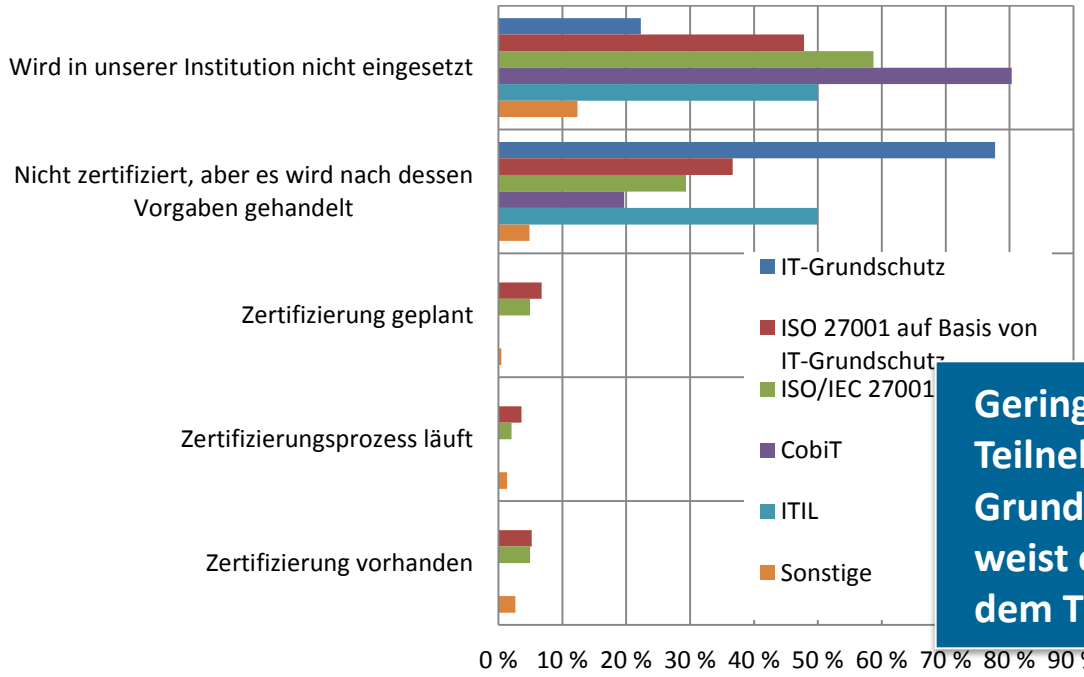
Bei IT-Compliance verzichtet die Hälfte auf Softwareunterstützung

Mängel von Standardsoftware



Zertifizierung und Anwendung von Standards

- Nur wenige Institutionen sind nach ISO 27001 auf Basis von IT-Grundschutz und ISO/IEC 27001 zertifiziert.
- Dennoch handelt ein Großteil nach den Vorgaben dieser Standards.

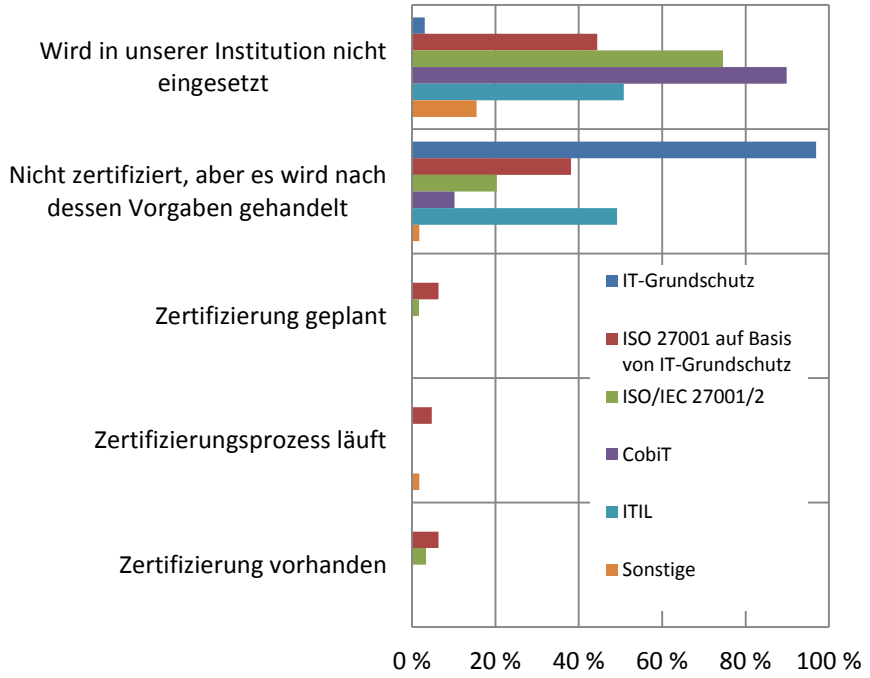


Geringe Zertifizierung verwunderlich: Teilnehmer vielfach Leser des Infodienst IT-Grundschutz bzw. des BSI Newsletters → weist eigentlich auf aktive Beschäftigung mit dem Thema hin!

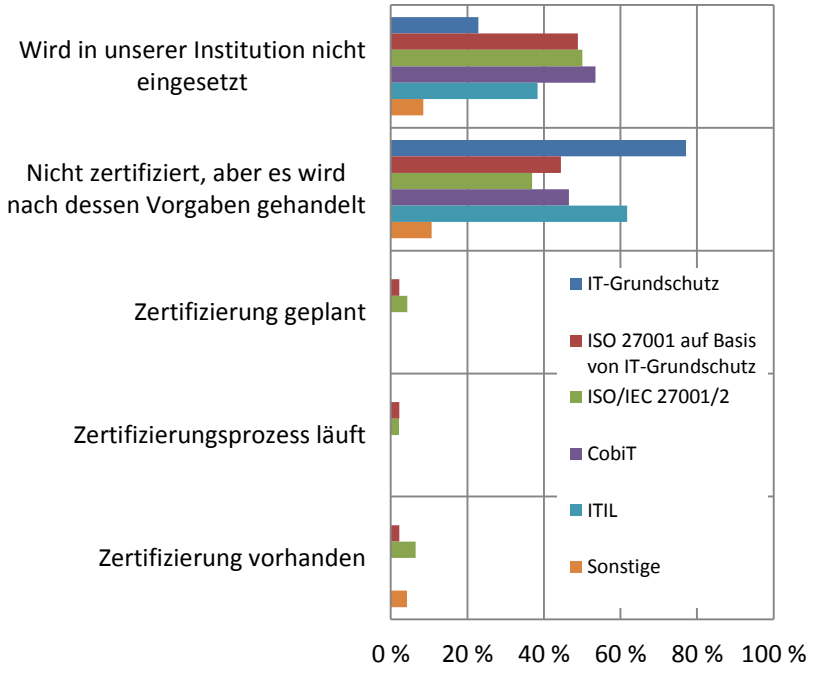
Zertifizierung und Anwendung von Standards

- Der IT-Grundschutz ist in der öffentlichen Verwaltung weit verbreitet

Öffentliche Verwaltung, Verteidigung und Sozialversicherung

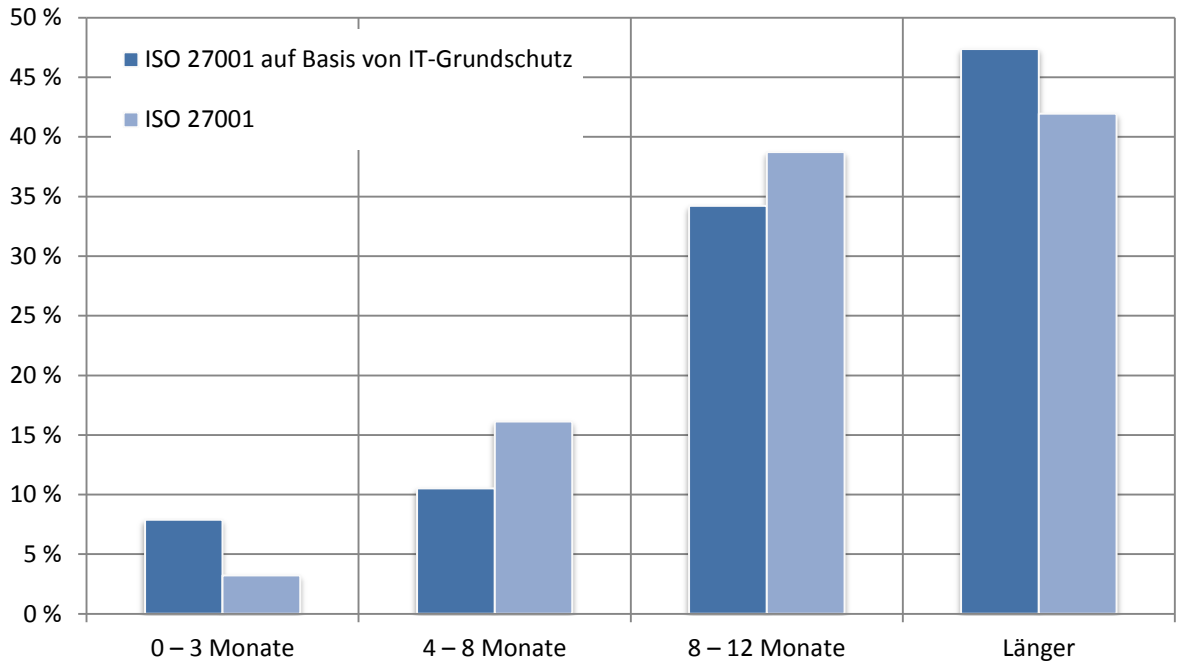


Kredit- und Versicherungsgewerbe



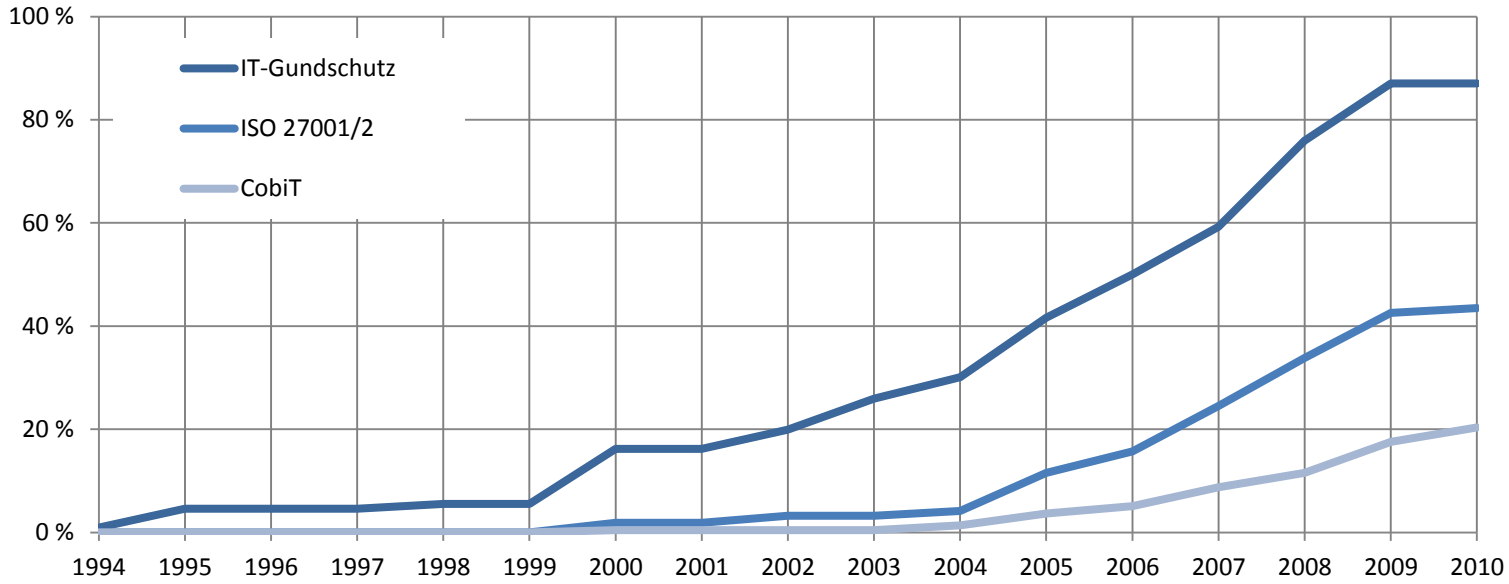
Vorbereitungszeit für die Zertifizierung

- Vorbereitungszeit für Zertifizierung meist länger als 8 Monate



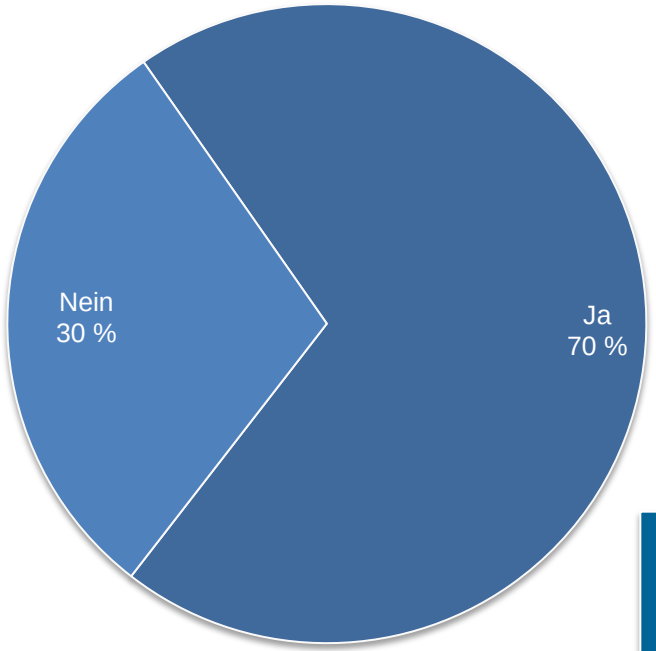
Nutzungsdauer von Standards / IT-Frameworks

- IT-Grundschutz seit 16 Jahren ein Erfolgsmodell
- Signifikante Anstiege zwischen 2004 und 2009



Relevanz „Qualified IT-Grundschutz Expert”

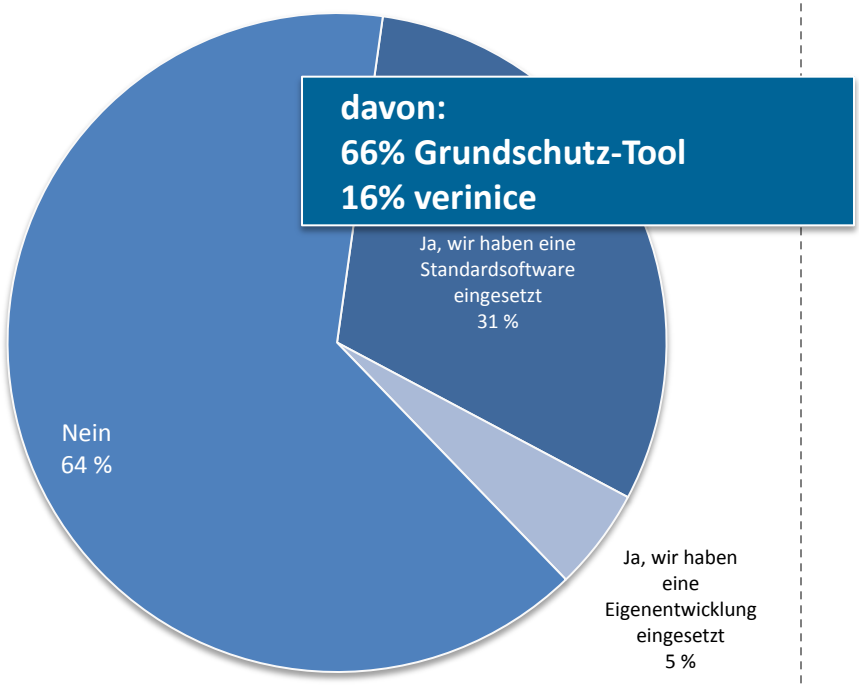
- Experte für den IT-Grundschutz wird von den meisten Teilnehmern gewünscht



Zeigt, dass Fachkompetenz oftmals fehlt und Unterstützung erwünscht wird.

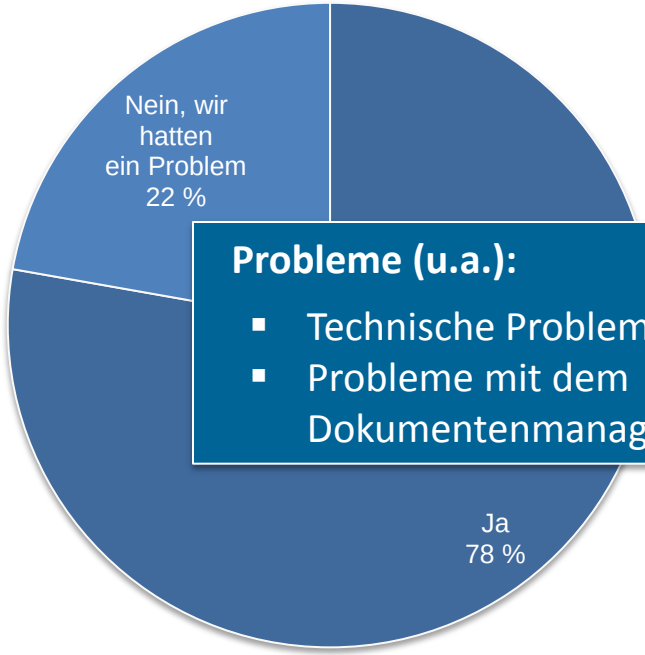
Softwareunterstützung

Softwareunterstützung zur Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz



davon:
66% Grundschutz-Tool
16% verinice

Aufgabenbewältigung durch das GSTool bei ISO 27001 auf Basis von IT-Grundschutz

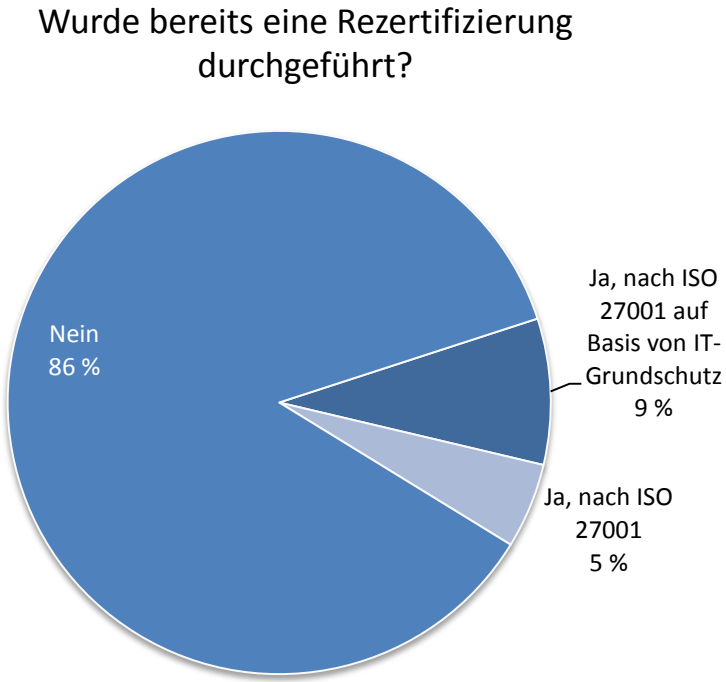


Probleme (u.a.):

- Technische Probleme bzgl. Zugriff
- Probleme mit dem Dokumentenmanagement

Re-Zertifizierung

- Die meisten Institutionen ließen sich bisher nicht rezertifizieren
- Mehr als die Hälfte plant künftig keine Rezertifizierung

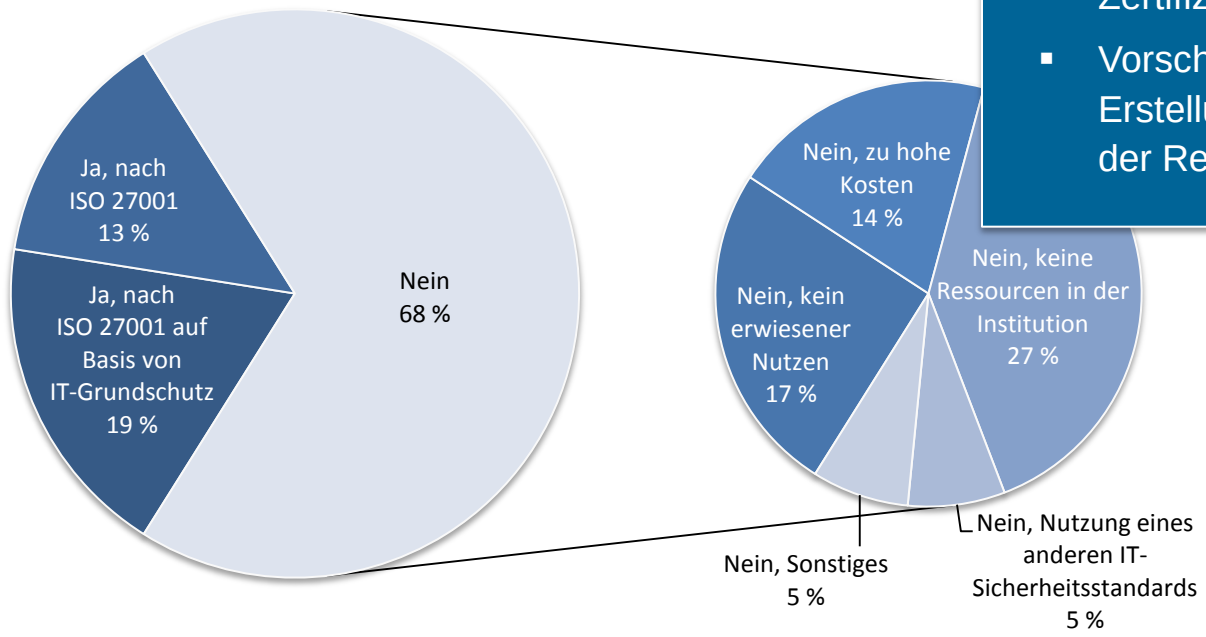


- Schaffung von Anreizen notwendig, um Zertifizierungen voran zu treiben
- Vorschlag:
  Erstellung von Regularien zur Reduzierung der Rezertifizierungsaufwände

Re-Zertifizierung

- Die meisten Institutionen ließen sich bisher nicht rezertifizieren
- Mehr als die Hälfte plant künftig keine Rezertifizierung

Ist eine Refinanzierung in Planung?

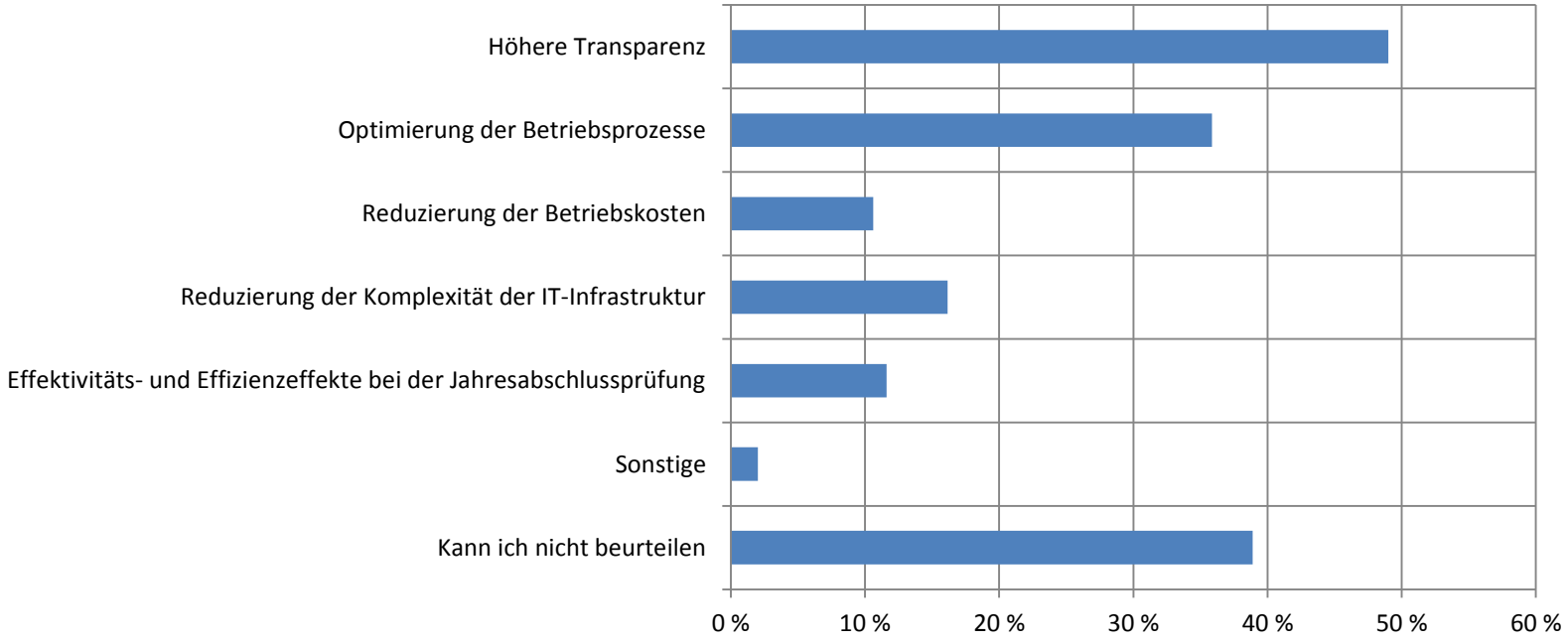


- Schaffung von Anreizen notwendig, um Zertifizierungen voran zu treiben
- Vorschlag:
  Erstellung von Regularien zur Reduzierung der Rezertifizierungsaufwände

Themenblock 4: IT-Compliance special

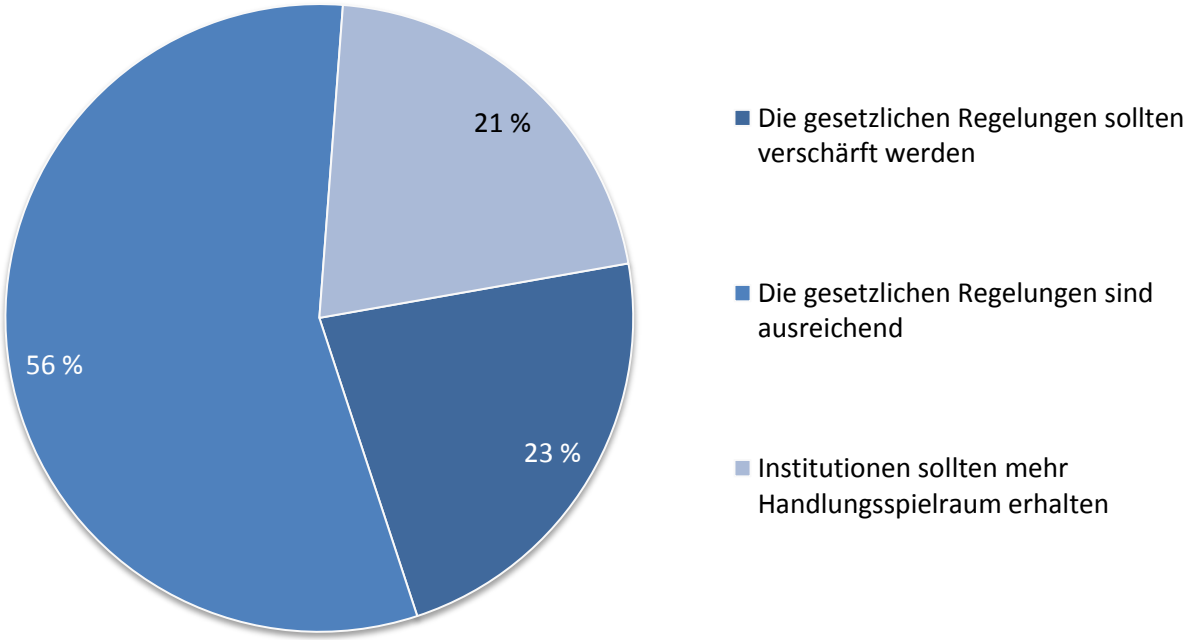
Positive Effekte durch IT-Compliance Management

- Institutionen versprechen sich vom IT-Compliance Management einen höhere Transparenz



Gesetzlicher Handlungsbedarf zum Datenschutz

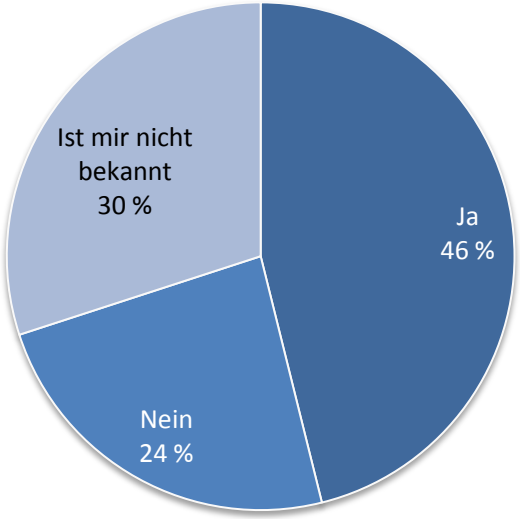
- Datenschutzgesetze wird insgesamt als ausreichend angesehen



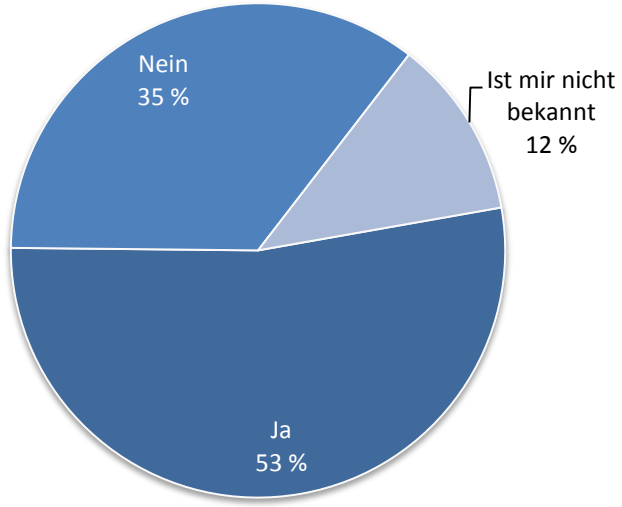
Umgang mit Gesetzen und Reglungen

- Das Wissen um Gesetze und Regelungen ist nicht ausreichend
- Bei über einem Drittel der Institutionen fehlt ein Verantwortlicher für die Bekanntmachung von Gesetzen und Regelungen

Sind die zuständigen Mitarbeiter mit den maßgeblichen Gesetzen und Reglungen vertraut?

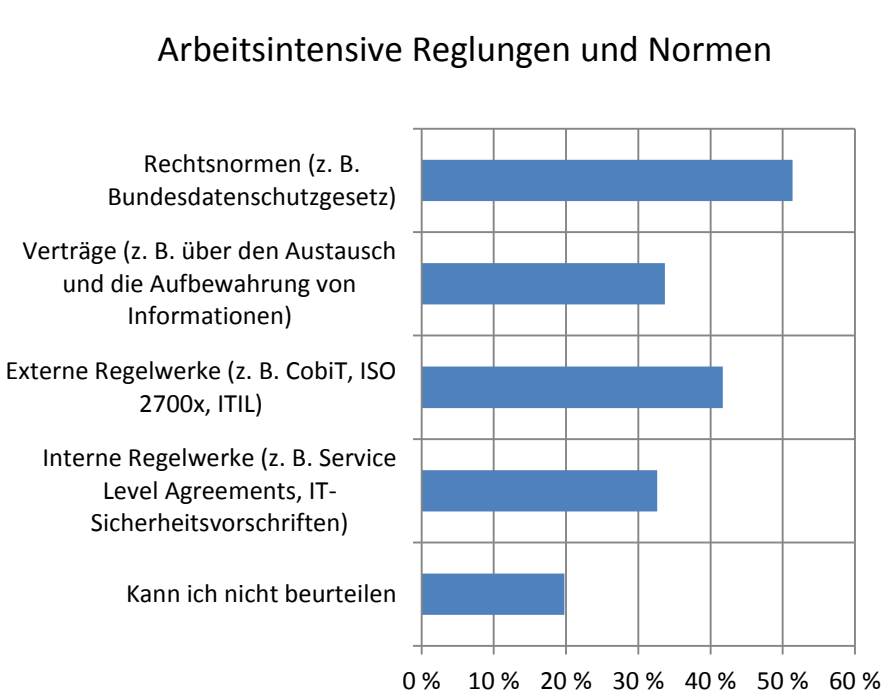


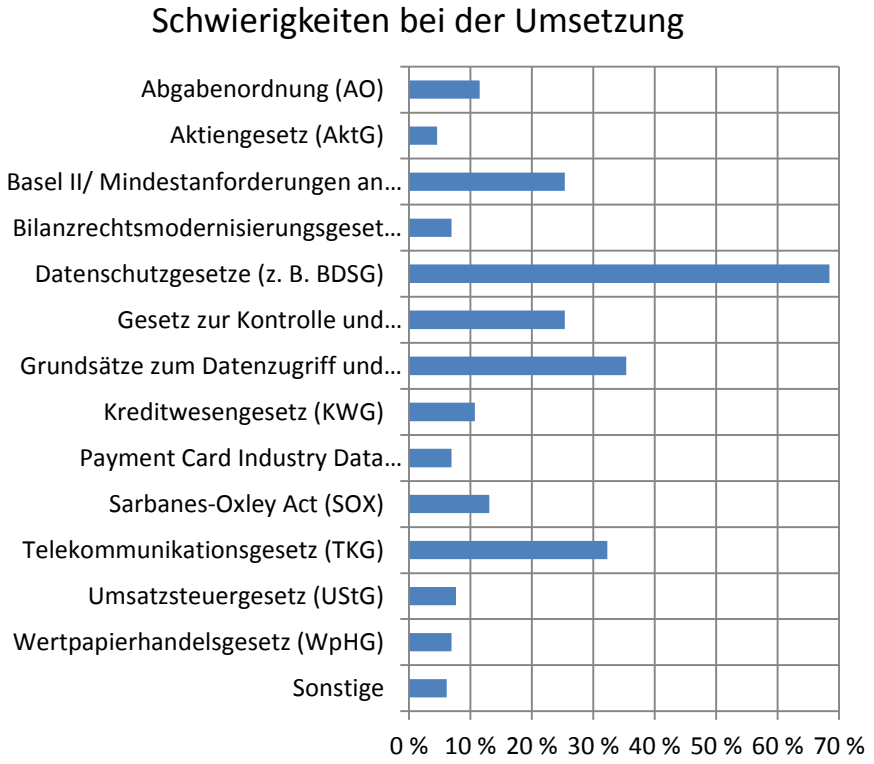
Gibt es einen Verantwortlichen für die Bekanntmachung neuer Gesetze und Reglungen?



Implementierung von Normen und Gesetzen

- Rechtsnormen benötigen die meiste Zeit zur Implementierung
- Am häufigsten gibt es Umsetzungsschwierigkeiten bei Datenschutzgesetzen





Key-Findings

- Bedeutung der Thematik sehr hoch und weiterhin zunehmend
- Qualität der IT-Sicherheit und IT-Compliance noch nicht ausreichend
- Optimierungshemmnisse: Fehlende finanzielle Mittel und fehlendes qualifiziertes Personal
- Mangelnde Akzeptanz seitens der Mitarbeiter stellt größtes Problem dar und verzögert die Umsetzung
- Institutionen lassen sich kaum (re-)zertifizieren, aber handeln oftmals nach den Standards
- Kaum Einsatz von Software zur Unterstützung

Was folgt daraus?

- Dringender Handlungsbedarf bei Unternehmen im Bezug auf Personal und Budget
  → Erster möglicher Schritt: Kompetenz aufbauen durch einen „Qualified IT-Grundschutz Expert“
- Akzeptanz der Mitarbeiter muss verbessert werden
  → Verbesserung der Business-IT-Alignment notwendig
  → eine kontinuierliche Einbindung der Mitarbeiter in Anpassungsprozesse erhöht die Akzeptanz
- Anreize zur Rezertifizierung müssen geschaffen werden:
  → Regularien könnten sinnvolle Hilfe darstellen
- Handlungsbedarf bei Softwareherstellern
  → Software muss besser auf die Bedürfnisse der Institutionen zugeschnitten werden

Sponsoren der Studie

secunet

apeec applied security

DB3

DFN CERT

FINANCE SECURITY

infodas
Cologne IT Solutions & Services

intersoft consulting services

ITSECURITY
Bavarian IT Security & Safety Cluster

JAKOBSOFTWARE

Microsoft

seed forensics

SONICWALL

Tele-Consulting
security | networking | training gmbh

TRIGONUM consulting

UIMC
Dr. Vossbein GmbH & Co KG
Unternehmens- und Informations- Management Consultants

UIMCert GmbH
Unternehmens- und Informations- Management Certification

VALIDD
DIGITAL FORENSICS

Die Autoren

Dr. Stefan Kronschnabl
Research Director
Ibi research GmbH

Elmar Török
Chefredakteur Infodienst IT-Grundschutz
Fachredaktion BSI Grundschutzkataloge
SecuMedia Verlag

Stephan Weber
Business Consulant
Ibi research GmbH

Isabel Münch
Referatsleiterin IT-Sicherheitsmanagement und IT-Grundschutz
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Christian Dirnberger
Universität Regensburg

Vielen Dank für Ihre Aufmerksamkeit

- Vollständige Studie erhältlich unter:
  - http://www.ibi.de
  - http://buchshop.secumedia.de

- Ansichtsexemplare und weitere Informationen am **Stand 318 bei „GRC-Suite iRIS“** neben „Psylock“