



DEUTSCHER
LANDKREISTAG

Rolle und Verantwortung der Behördenleitungen beim systematischen Aufbau der IT-Sicherheit in Kommunalverwaltungen

Heino Sauerbrey
Deutscher Landkreistag
Ulrich-von-Hassell-Haus
Lennéstraße 11
10785 Berlin
www.Landkreistag.de
www.Kreisnavigator.de



Rolle und Verantwortung der Behördenleitungen beim systematischen Aufbau der IT-Sicherheit in Kommunalverwaltungen

Agenda:

- **Begriffe: Informationssicherheit, IT-Sicherheit, Datenschutz und Datensicherheit**
- **Die kommunalen Spitzenverbände und die Informationssicherheit in Kommunalverwaltungen**
- **Die Verantwortung der obersten Managementebene für die Informationssicherheit ihrer Behörde**
- **Umfrage des DLT zur Informationssicherheit in Kreisverwaltungen (2018)**
 - **Wichtigste Hemmnisse für die Informationssicherheit**
 - **Wirkzusammenhänge zwischen den genannten Hemmnissen**
- **Fazit**



Begriffe

IT-Sicherheitsbeauftragte, Informationssicherheitsbeauftragte, ...?

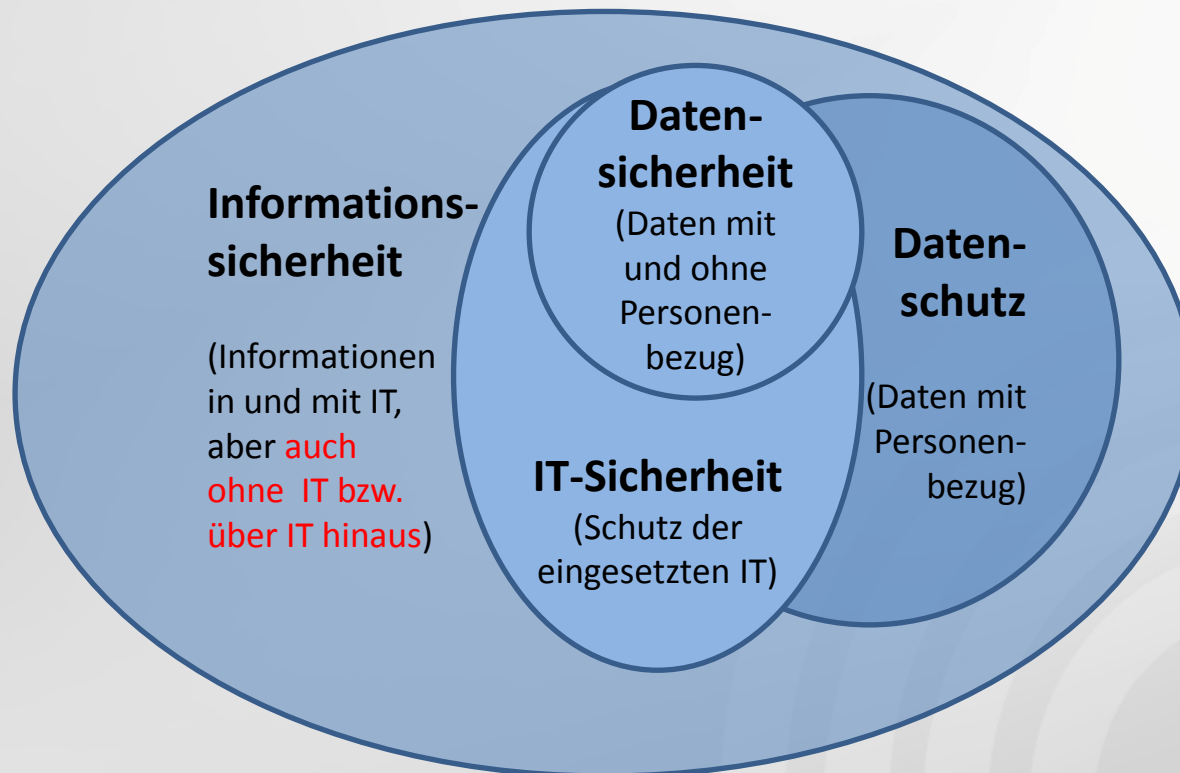
„In den IT-Grundschatz-Dokumenten wurde bisher die Bezeichnung **IT-Sicherheitsbeauftragter** verwendet, da dieser Begriff in Unternehmen und Behörden lange Zeit der am weitesten verbreitete war. Die Bezeichnung **Informationssicherheitsbeauftragter oder kurz IS-Beauftragter (ISB)** ist allerdings treffender und **ersetzt daher im IT-Grundschatz die alte Bezeichnung.**“

„So macht der Titel des Informationssicherheitsbeauftragten statt des IT-Sicherheitsbeauftragten deutlich, dass diese Person sich um die **Absicherung aller Arten von Informationen** kümmert und nicht nur um IT-bezogene Aspekte. [...] Aus diesem Grund ersetzt die Bezeichnung „Informationssicherheitsbeauftragter“ (ISB) im IT-Grundschatz in diesem Zusammenhang die Bezeichnung „IT-Sicherheitsbeauftragter“ (IT-SiBe)“

Quelle: BSI-Standard 200-2

Begriffe

- **Das Zusammenwirken von Informationssicherheit, IT-Sicherheit, Datenschutz und Datensicherheit**



Grafik: Heino Sauerbrey unter Bezug auf BSI-Standard 200-2



Kommunale Spitzenverbände

Spezifische Rahmenbedingungen in Kommunen

- länderspezifische rechtliche und organisatorische Gegebenheiten
- Föderalismus, Kommunale Selbstverwaltung, Organisationshoheit der Kommunen (Art. 28 GG)
- Verteilung in der Fläche
- heterogene (gewachsene) Strukturen
- Anbindung an unterschiedliche ebenenübergreifende Verfahren
- große Aufgabenvielfalt
- hohe Fallzahlen mit vielen direkten Bürgerkontakten
- Defizite der IT-SiBe bei Information, Erfahrung, Vernetzung, ...
- begrenzte finanzielle und personelle Ressourcen
- ad-hoc-Maßnahmen statt systematischer Entwicklung der IT-Sicherheit

Die kommunalen Spitzenverbände

Die meisten Gesetze des Bundes werden durch die Kommunalverwaltungen vollzogen. Die Kommunalen Spitzenverbände werden daher an **Gesetzesvorhaben**, die kommunale Anliegen berühren, vom Deutschen Bundestag und von den Bundesministerien beteiligt.

Zudem wirken sie in einer Vielzahl von **Gremien und Einrichtungen des Bundes und der Länder** beschließend oder beratend mit (z.B. IT-Planungsrat).

Die gemeinsame Interessenvertretung erfolgt über die **Bundesvereinigung der kommunalen Spitzenverbände (BV)**.

Bundesvereinigung der kommunalen Spitzenverbände





Die kommunalen Spitzenverbände

„Die kommunalen Spitzenverbände **vertreten die Interessen der Landkreise, Städte und Gemeinden** gegenüber anderen politischen Akteuren und üben auf Landesregierungen und Bundesregierung einen maßgeblichen Einfluss aus. Die Verbände auf Bundesebene sind

- der **Deutsche Städtetag (DST)**, der **mehr als 5.700 Kommunen** vertritt,
- der **Deutsche Städte- und Gemeindebund (DStGB)**, durch den [...] **ca. 13.000 kleine und mittlere Kommunen** vertreten werden, und
- der **Deutsche Landkreistag (DLT)**, der mit **294 Landkreisen** in 13 Landesverbänden rund **74 % der Aufgabenträger*** sowie **ca. 68 % der Bevölkerung** und **96 % der Fläche** der Bundesrepublik Deutschland repräsentiert.“

Quelle: Wikipedia (https://de.wikipedia.org/wiki/Kommunaler_Spitzenverband)

* Hierbei handelt es sich um Institutionen, denen durch Gesetz oder Satzung öffentliche Aufgaben zugewiesen wurden.

Kommunale Spitzenverbände

Was tut der DLT für Informationssicherheit in Kommunalverwaltungen?

Der Deutsche Landkreistag ...

- ist von Anfang an im **IT-Planungsrat** und in dessen **AG Informationssicherheit (AG InfoSic)** aktiv.
- vertritt die Bundesvereinigung der kommunalen Spitzenverbände im **Nationalen Cyber-Sicherheitsrat**.
- stellt den **gemeinsamen Ansprechpartner** der Bundesvereinigung der kommunalen Spitzenverbände für das BSI.
- hat mit Unterstützung von IT-PLR und AG InfoSic **5 Kommunale IT-Sicherheitskongresse** durchgeführt. Der 6. KITS am **06./07.05.2019** ist in Vorbereitung.
- hat Handreichungen, Leitlinien und weitere **Dokumenten zur IT-Sicherheit** initiiert und an der Erarbeitung mitgewirkt.
- hat sich für die Mitwirkung der Kommunen bei der Modernisierung des IT-Grundschutzes eingesetzt und die **ebenenübergreifende Koordinierung bei der Erarbeitung des „Kommunalen Grundschutzprofils“** übernommen.
- betreibt gemeinsam mit dem IT-SiBe der Stadt Kassel ein **Internetforum für IT-Sicherheitsbeauftragte von Kommunen und Ländern (IT-SiBe-Forum)**.



Verantwortung für Informationssicherheit

Wer ist für Informationssicherheit verantwortlich?

„Die **oberste Managementebene** jeder Behörde und jedes Unternehmens ist für **das zielgerichtete und ordnungsgemäße Funktionieren** der Institution verantwortlich und damit auch für die **Gewährleistung der Informationssicherheit** nach innen und außen.“

„**Der Leitungsebene kommt daher eine hohe Verantwortung für die Informationssicherheit zu.** Fehlende Steuerung, eine ungeeignete Sicherheitsstrategie oder falsche Entscheidungen können sowohl durch Sicherheitsvorfälle als auch durch verpasste Chancen und Fehlinvestitionen weitreichende negative Auswirkungen haben. Eine intensive Beteiligung der Führungsebene ist somit unerlässlich:

Informationssicherheit ist Chefsache!^{“1)}

„**Die Leitungsebene informiert sich über mögliche Risiken und Konsequenzen aufgrund fehlender Informationssicherheit.**“²⁾

- 1) *Quelle: BSI-Standard 200-1*
- 2) *BSI-Standard 200-2*

Verantwortung für Informationssicherheit

Voraussetzungen zur Verbesserung der Informationssicherheit

- Die Beteiligten aller Ebenen müssen ihre **Verantwortung kennen und wahrnehmen**.
- **Informationssicherheit ist kein Projekt**, sondern eine dauerhafte Aufgabe.
- Informationssicherheit ist **nur systematisch erreichbar**.
- Informationssicherheit ist zwar auch eine technische, primär aber eine **Management- und Organisationsaufgabe**
- Bei Digitalisierungsaufgaben und Prozessen sind Sicherheitsaspekte von Anfang an zu berücksichtigen (**Security by Design**)*.
- Informationssicherheit ist **kein Selbstläufer**. Sie erfordert **strategische Vorbereitungen und dauerhaft konsequente Maßnahmen** auf allen Ebenen.

* vgl. **DIN SPEC 90158** „Handlungsleitfaden für ein strategisches und operatives Prozessmanagement in der öffentlichen Verwaltung“



Verantwortung für Informationssicherheit

Informationssicherheit erfordert systematisches Vorgehen

„Für die Gestaltung des Sicherheitsprozesses ist ein **systematisches Vorgehen** erforderlich, damit ein **angemessenes Sicherheitsniveau** erreicht werden kann.

Im Rahmen des IT-Grundschutzes besteht der Sicherheitsprozess aus den folgenden Phasen:

- **Initiierung des Sicherheitsprozesses**
- **Übernahme der Verantwortung durch die Leitungsebene**
- Konzeption und Planung des Sicherheitsprozesses
- **Bereitstellung von finanziellen, personellen und zeitlichen Ressourcen**
- [...]“

Quelle: BSI-Standard 200-1



Verantwortung für Informationssicherheit

Die Rolle der Leitungsebene für die Gestaltung des Informationssicherheitsprozesses

„Die folgenden Überlegungen verdeutlichen [...] die **Bedeutung der Leitungsebene im Sicherheitsprozess**:

- Die Leitungsebene trägt die Verantwortung dafür, dass gesetzliche Regelungen und Verträge mit Dritten eingehalten werden und dass wichtige Geschäftsprozesse störungsfrei ablaufen.
- **Die Leitungsebene ist diejenige Instanz, die über den Umgang mit Risiken entscheidet.**
- Informationssicherheit hat Schnittstellen zu vielen Bereichen einer Institution und **betrifft wesentliche Geschäftsprozesse und Aufgaben**. Nur die Leitungsebene kann daher für eine reibungslose Integration des Informationssicherheitsmanagements in bestehende Organisationsstrukturen und Prozesse sorgen.
- **Die Leitungsebene ist zudem für den wirtschaftlichen Einsatz von Ressourcen verantwortlich.**

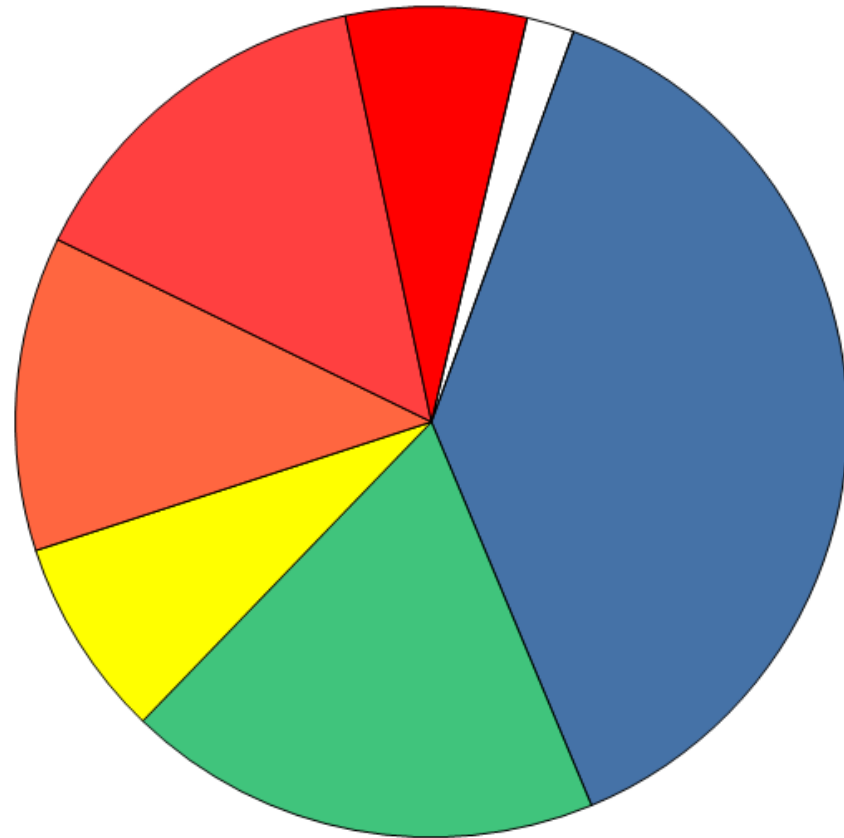
Quelle: BSI-Standard 200-1



Haupthemmnisse für die Informationssicherheit

In einer Umfrage des DLT vom Sommer 2018, an der sich über 60% aller 294 Landkreise beteiligten, wurde die Multiple-Choice-Frage nach den **Haupthemmnissen für die Informationssicherheit** mit folgender Häufigkeit beantwortet:

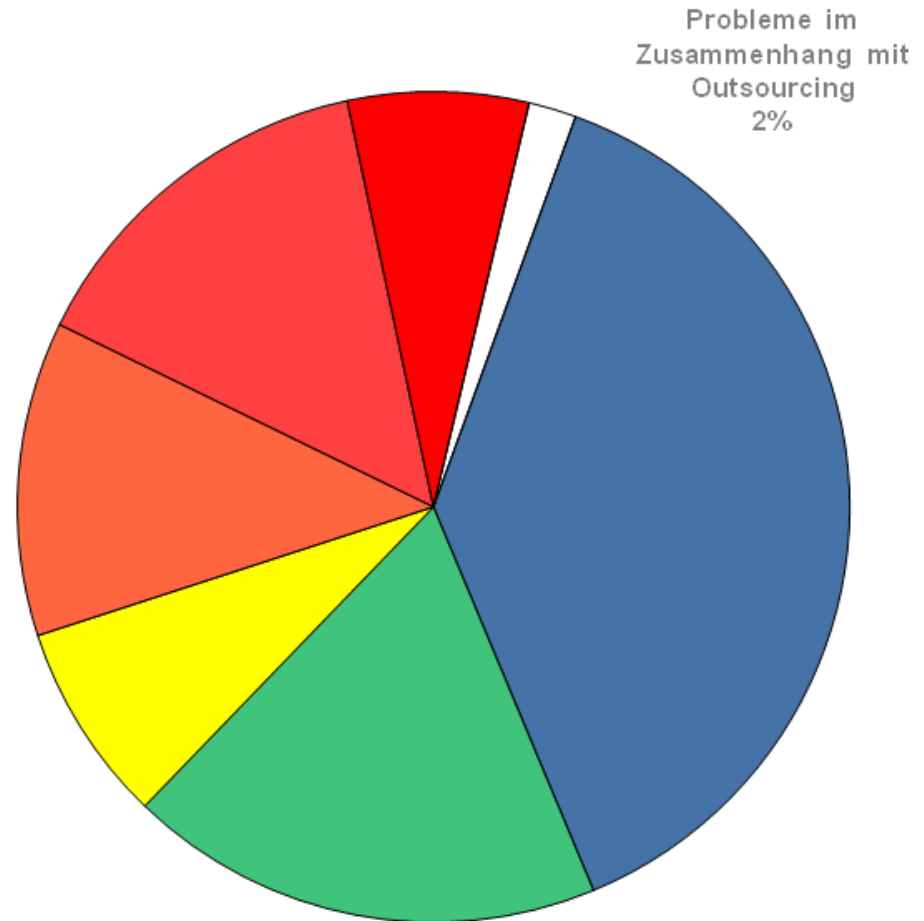
Umfrage des DLT zur Informationssicherheit in Kreisverwaltungen





Haupthemmnisse für die Informationssicherheit

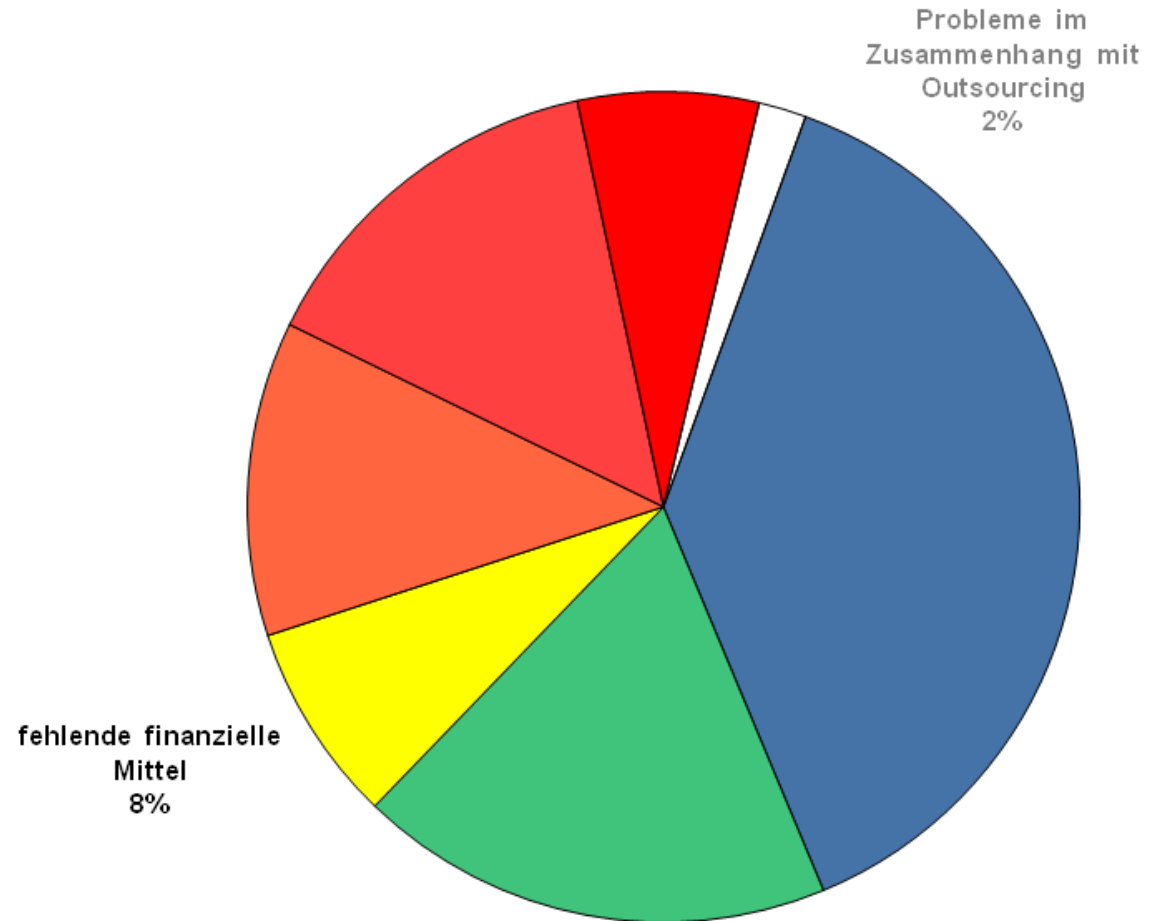
In einer Umfrage des DLT vom Sommer 2018, an der sich über 60% aller 294 Landkreise beteiligten, wurde die Multiple-Choice-Frage nach den **Haupthemmnissen für die Informationssicherheit** mit folgender Häufigkeit beantwortet:





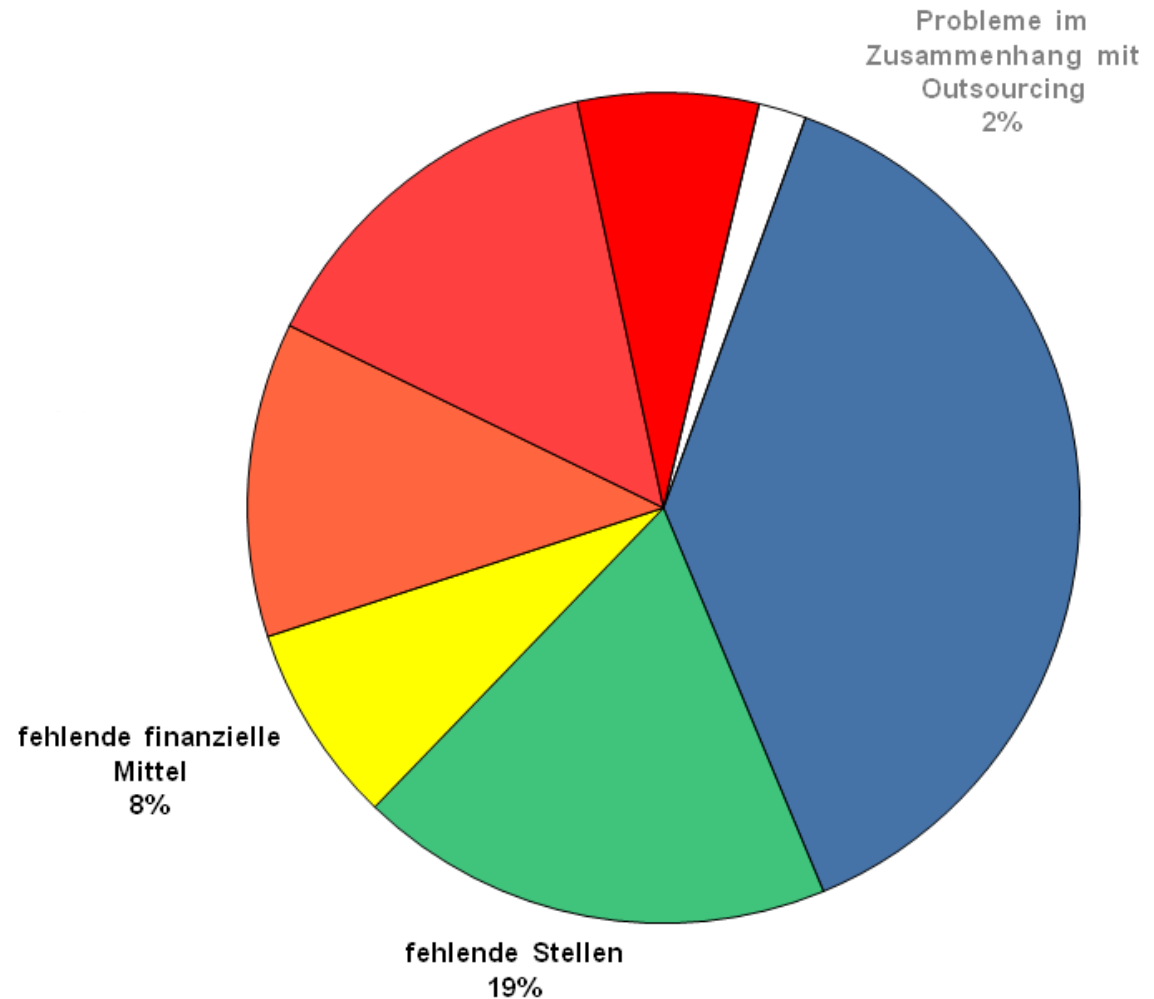
Haupthemmnisse für die Informationssicherheit

In einer Umfrage des DLT vom Sommer 2018, an der sich über 60% aller 294 Landkreise beteiligten, wurde die Multiple-Choice-Frage nach den **Haupthemmnissen für die Informationssicherheit** mit folgender Häufigkeit beantwortet:



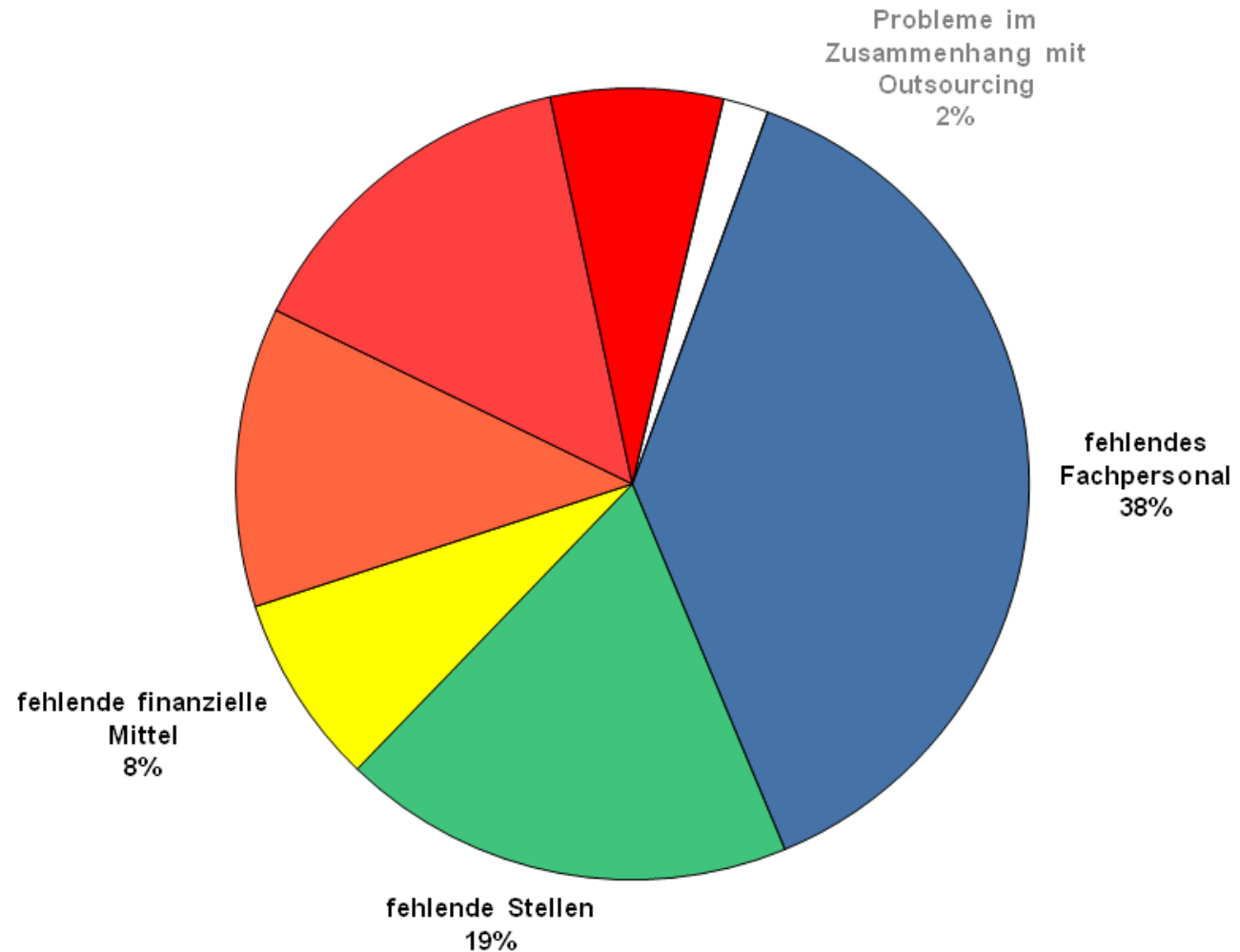
Haupthemmnisse für die Informationssicherheit

In einer Umfrage des DLT vom Sommer 2018, an der sich über 60% aller 294 Landkreise beteiligten, wurde die Multiple-Choice-Frage nach den **Haupthemmnissen für die Informationssicherheit** mit folgender Häufigkeit beantwortet:



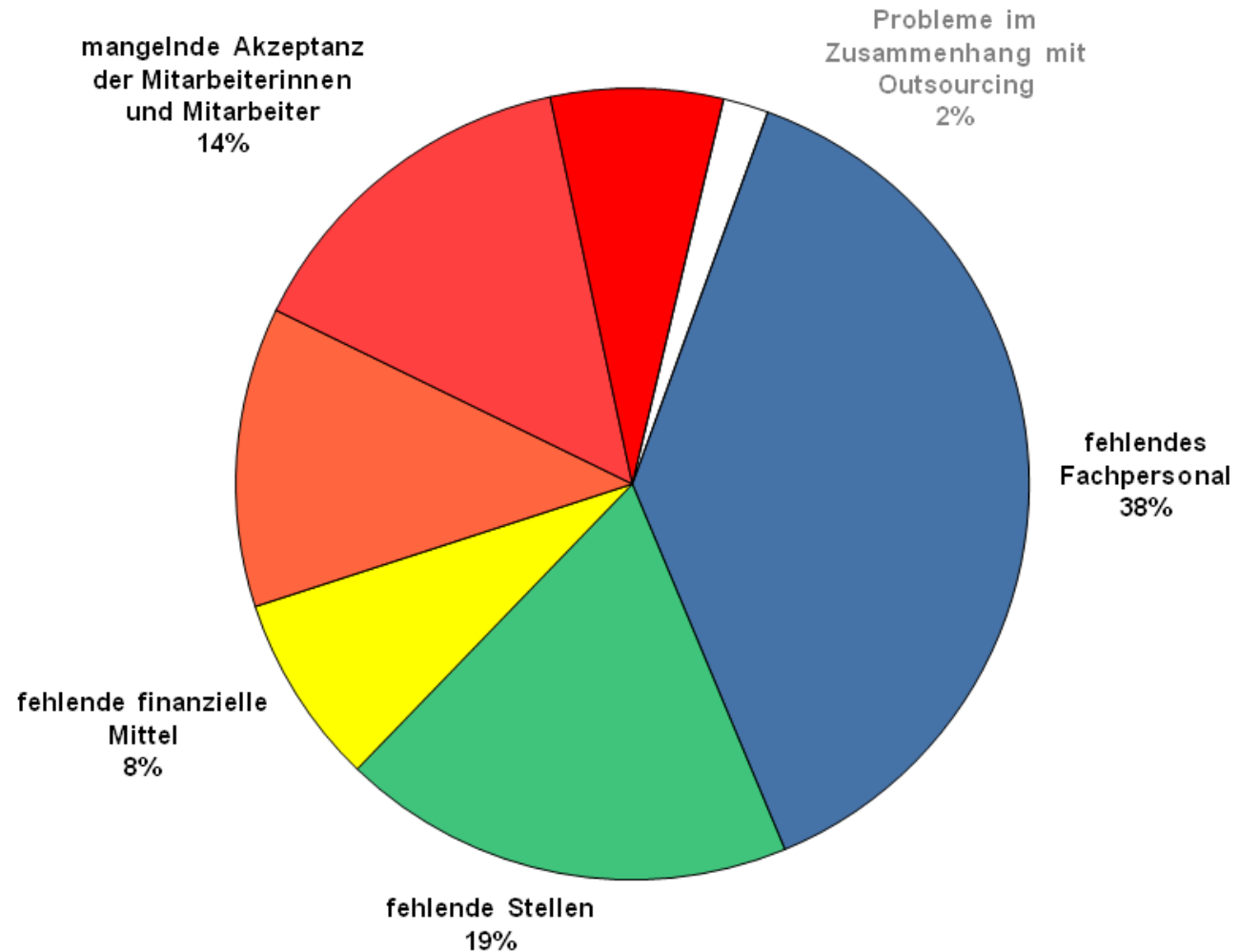
Haupthemmnisse für die Informationssicherheit

In einer Umfrage des DLT vom Sommer 2018, an der sich über 60% aller 294 Landkreise beteiligten, wurde die Multiple-Choice-Frage nach den **Haupthemmnissen für die Informationssicherheit** mit folgender Häufigkeit beantwortet:



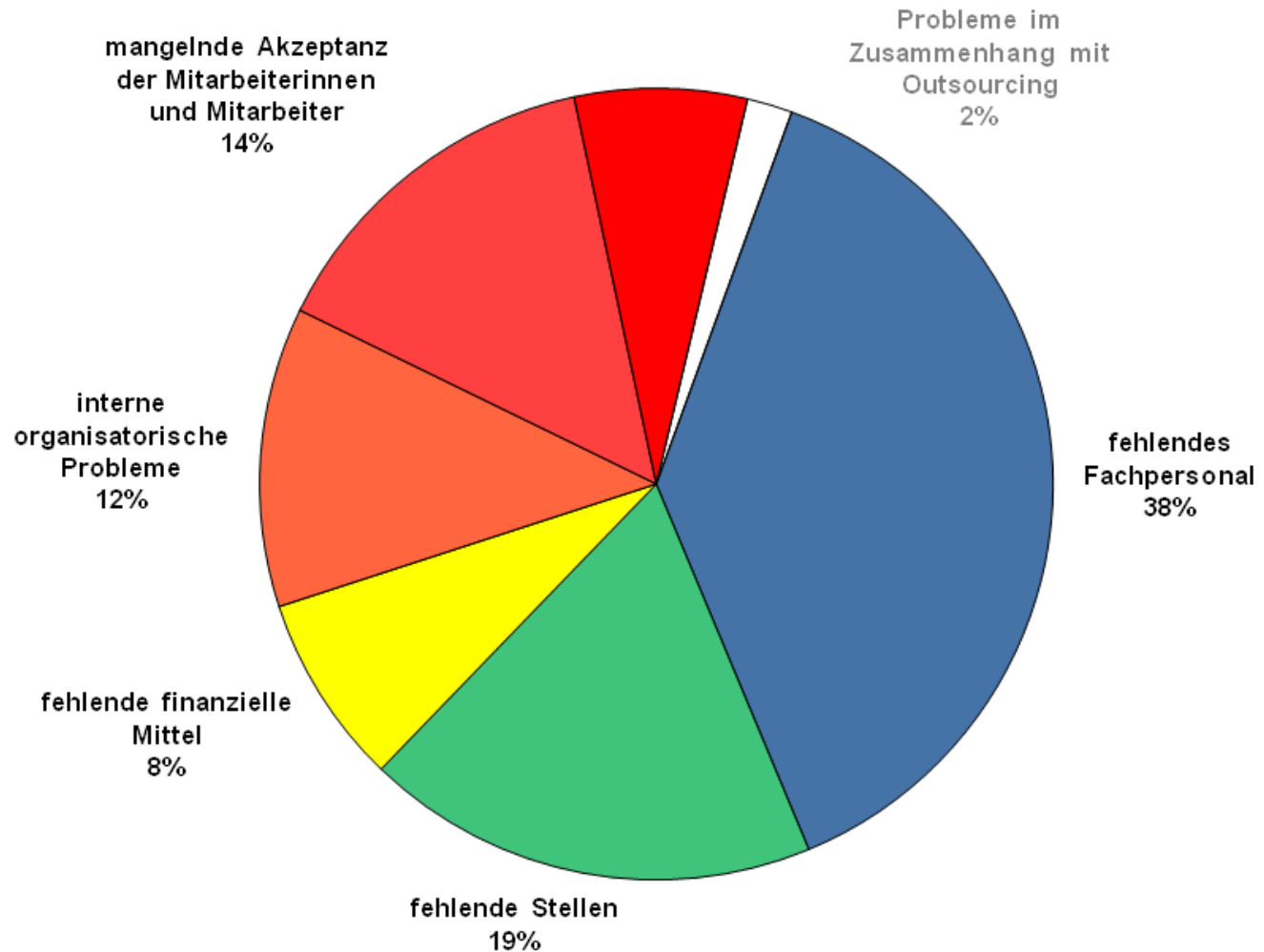
Haupthemmnisse für die Informationssicherheit

In einer Umfrage des DLT vom Sommer 2018, an der sich über 60% aller 294 Landkreise beteiligten, wurde die Multiple-Choice-Frage nach den **Haupthemmnissen für die Informationssicherheit** mit folgender Häufigkeit beantwortet:



Haupthemmnisse für die Informationssicherheit

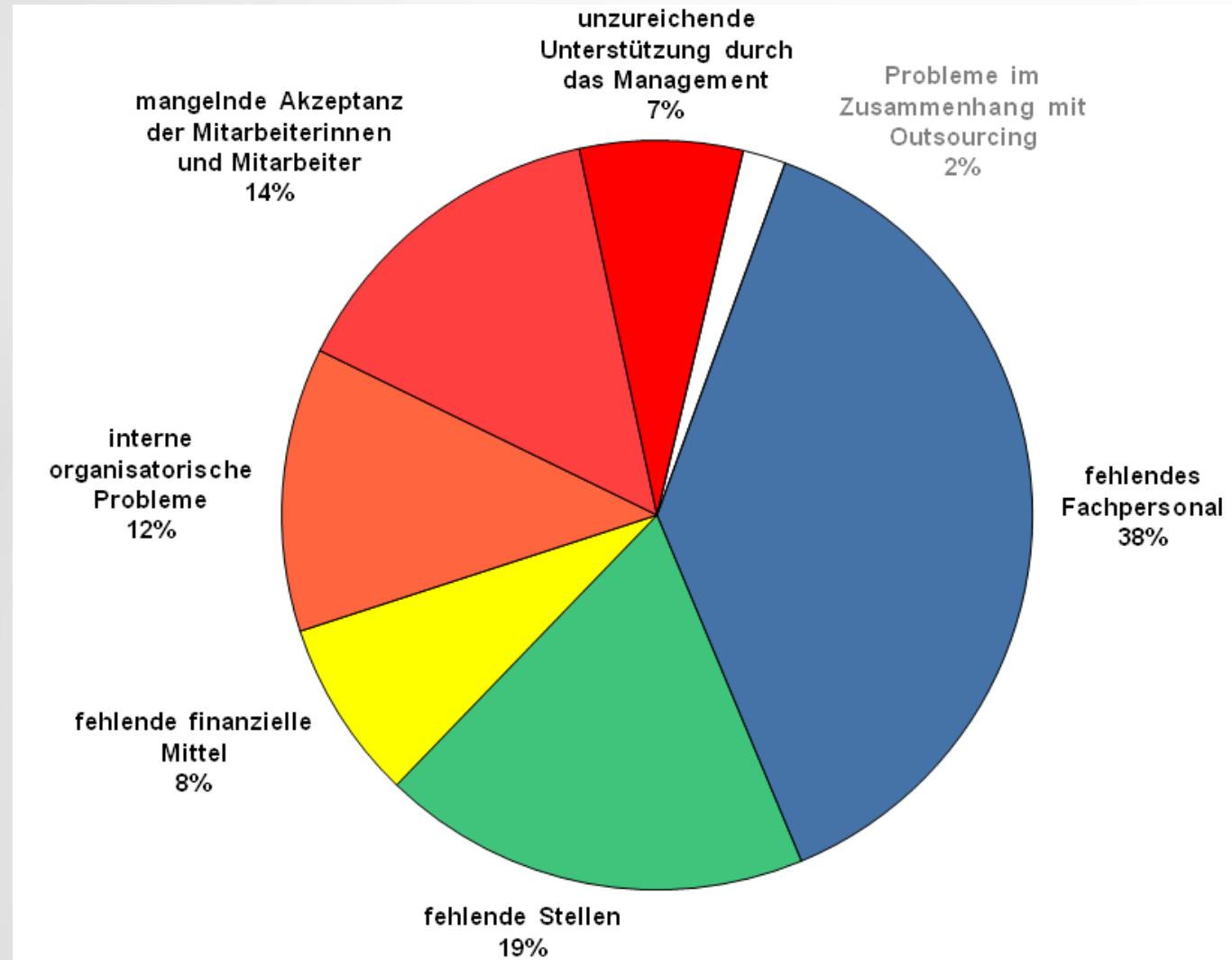
In einer Umfrage des DLT vom Sommer 2018, an der sich über 60% aller 294 Landkreise beteiligten, wurde die Multiple-Choice-Frage nach den **Haupthemmnissen für die Informationssicherheit** mit folgender Häufigkeit beantwortet:





Haupthemmnisse für die Informationssicherheit

In einer Umfrage des DLT vom Sommer 2018, an der sich über 60% aller 294 Landkreise beteiligten, wurde die Multiple-Choice-Frage nach den **Haupthemmnissen für die Informationssicherheit** mit folgender Häufigkeit beantwortet:

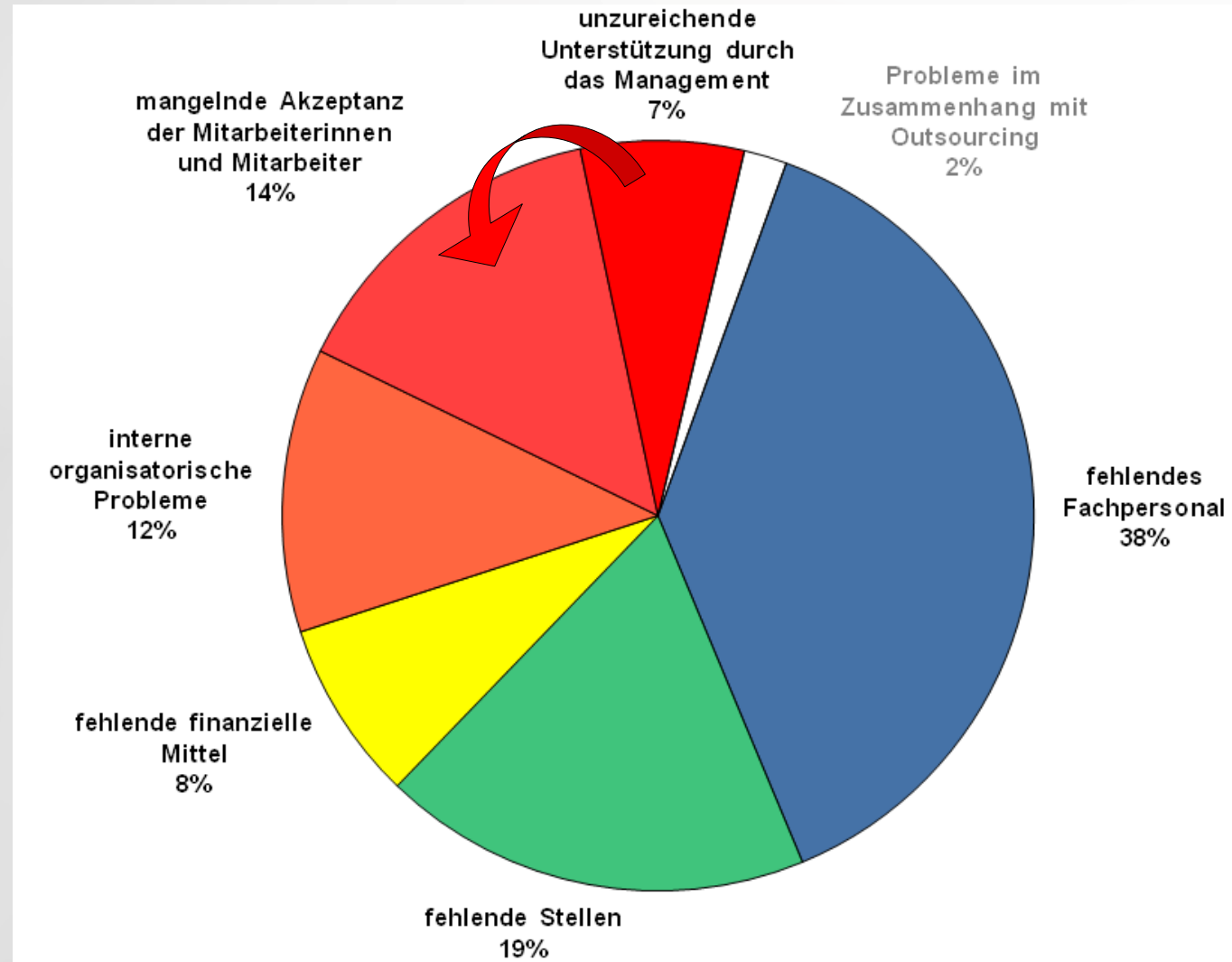




Haupthemmnisse für die Informationssicherheit

„Die oberste Managementebene jeder Behörde und jedes Unternehmens ist für das **zielgerichtete und ordnungsgemäße Funktionieren der Institution** verantwortlich und damit auch für die **Gewährleistung der Informationssicherheit nach innen und außen.**“

Quelle: BSI-Standard 200-1



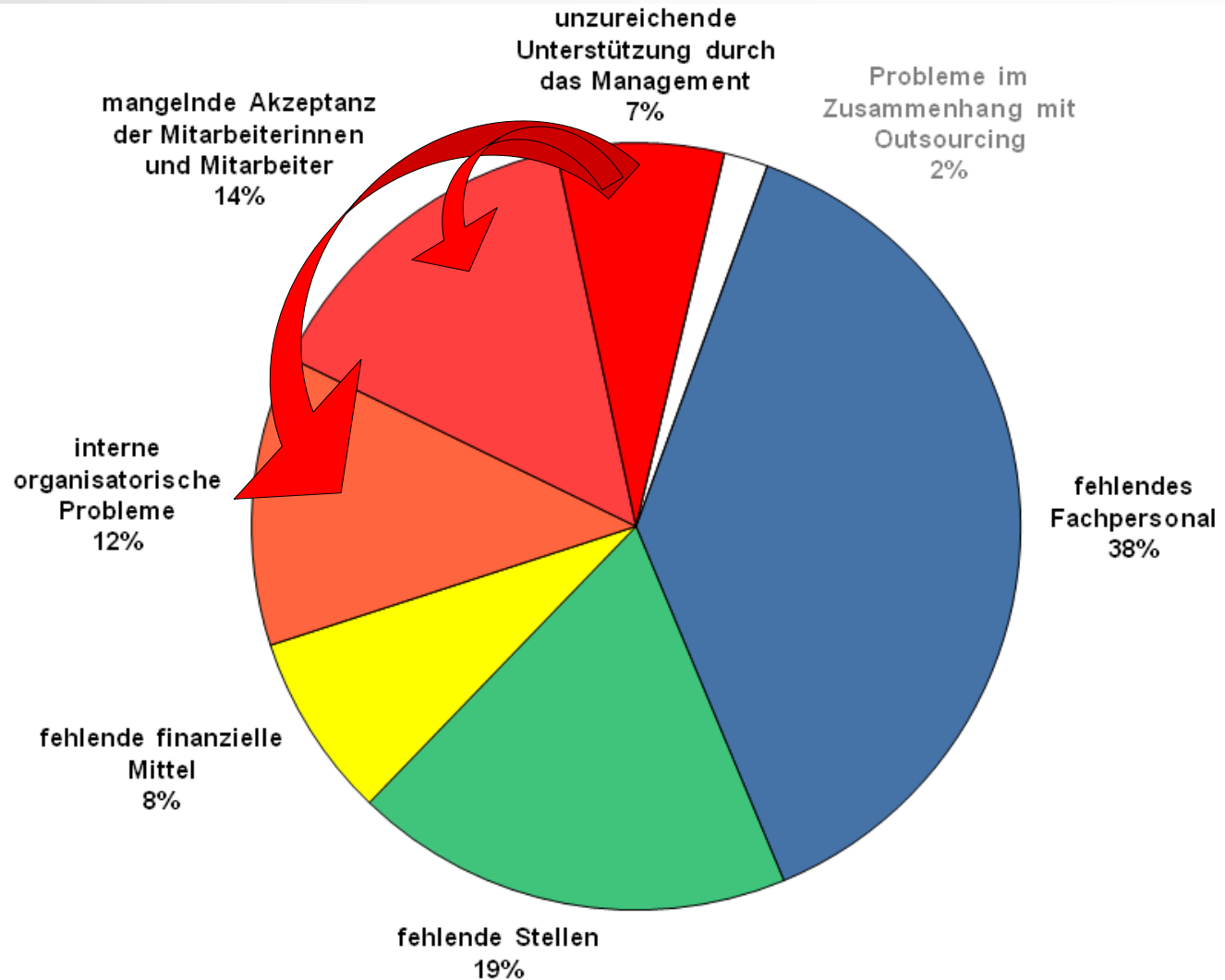


Haupthemmnisse für die Informationssicherheit

„Der Leitungsebene kommt daher eine hohe Verantwortung für die Informationssicherheit zu. Fehlende **Steuerung**, eine ungeeignete Sicherheitsstrategie oder falsche Entscheidungen können sowohl durch Sicherheitsvorfälle als auch durch verpasste Chancen und Fehlinvestitionen weitreichende negative Auswirkungen haben.

Eine intensive Beteiligung der Führungsebene ist somit unerlässlich:
Informationssicherheit ist Chefsache!“

Quelle: BSI-Standard 200-1

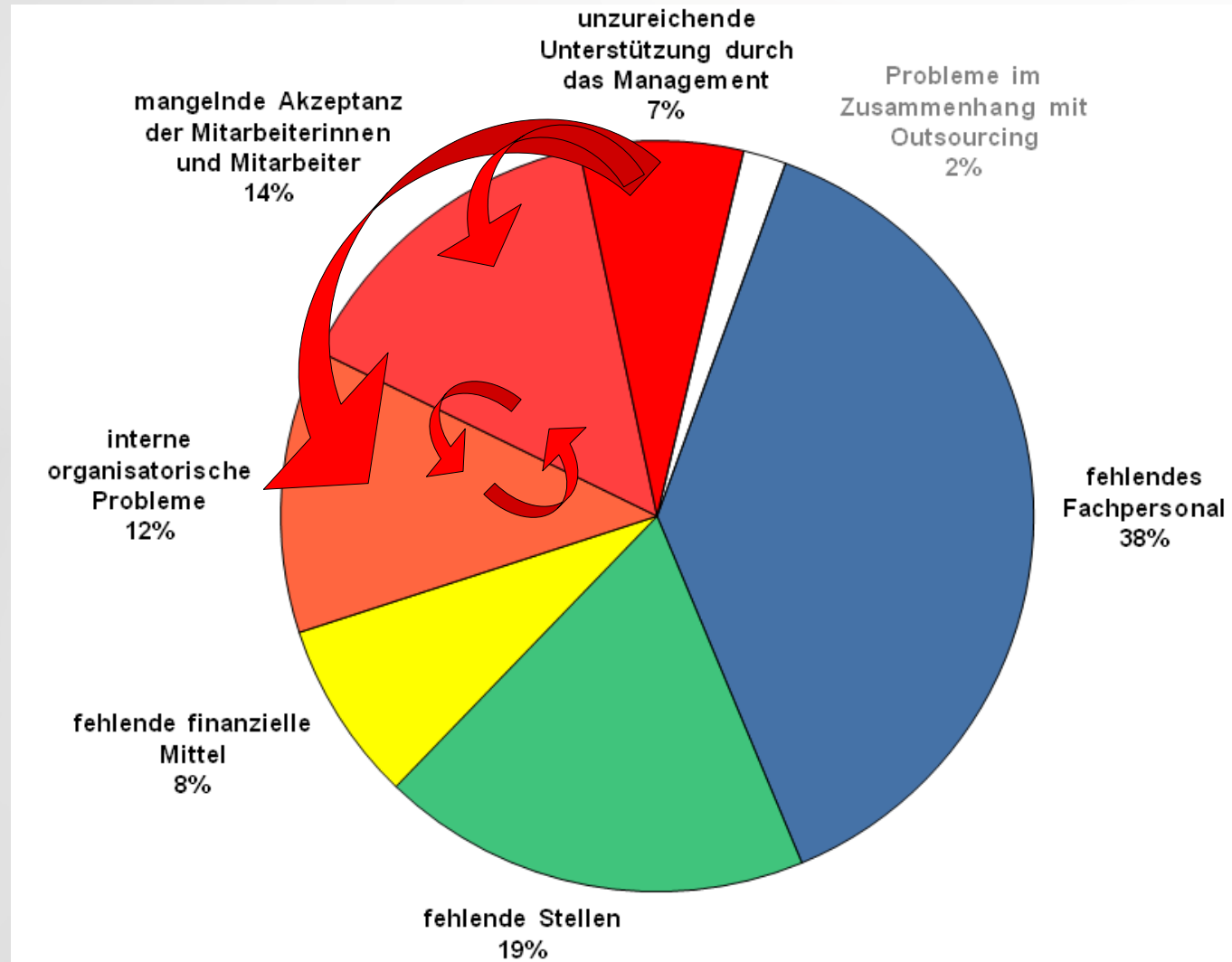


Haupthemmnisse für die Informationssicherheit

„Der Leitungsebene kommt daher eine hohe Verantwortung für die Informationssicherheit zu. Fehlende **Steuerung**, eine ungeeignete Sicherheitsstrategie oder falsche Entscheidungen können sowohl durch Sicherheitsvorfälle als auch durch verpasste Chancen und Fehlinvestitionen weitreichende negative Auswirkungen haben.

Eine intensive Beteiligung der Führungsebene ist somit unerlässlich:
Informationssicherheit ist Chefsache!“

Quelle: BSI-Standard 200-1



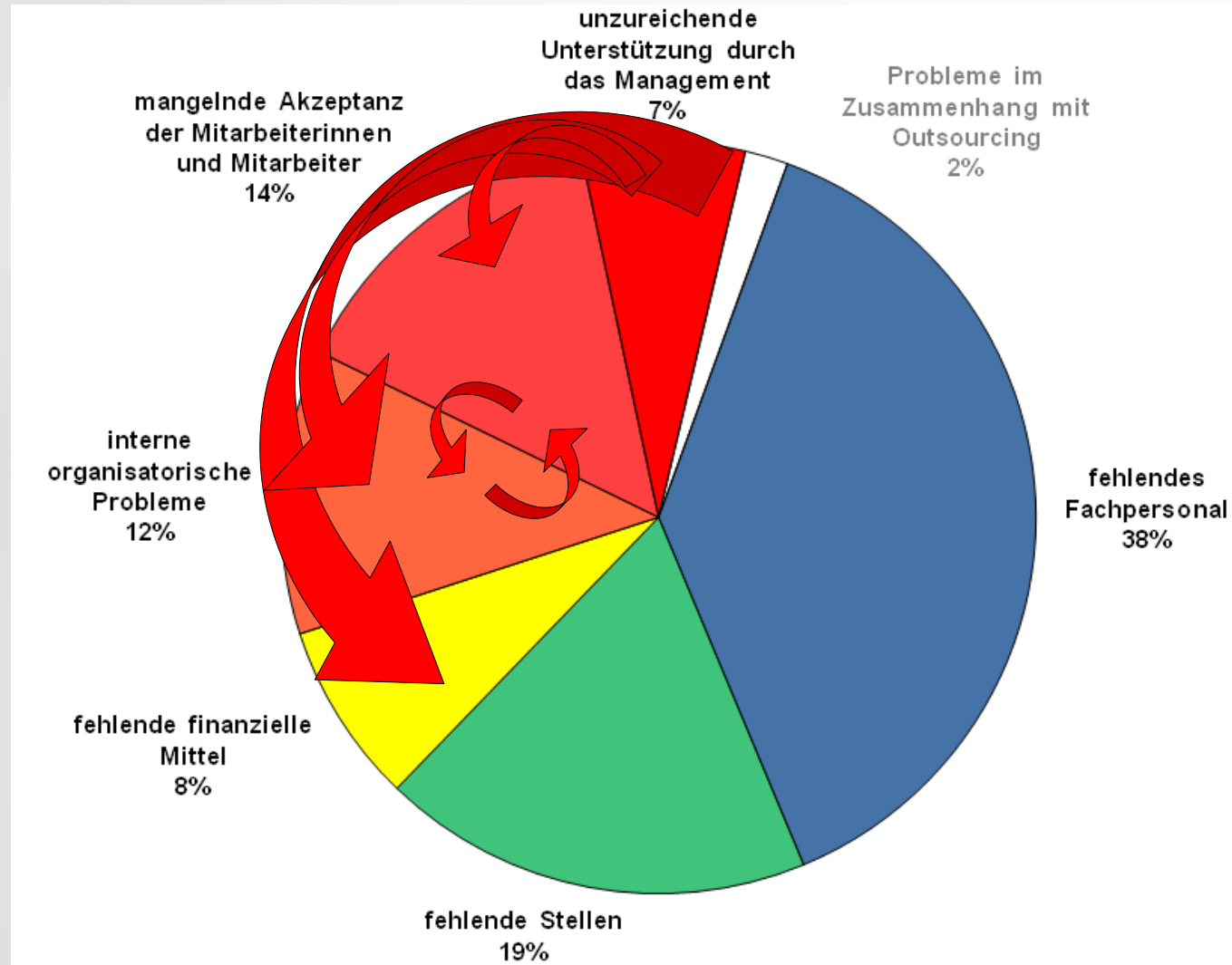


Haupthemmnisse für die Informationssicherheit

„Für die Gestaltung des Sicherheitsprozesses ist ein **systematisches Vorgehen** erforderlich, damit ein angemessenes Sicherheitsniveau erreicht werden kann.

Im Rahmen des IT-Grundschutzes besteht der Sicherheitsprozess aus den folgenden Phasen:

- Initiierung des Sicherheitsprozesses
- **Übernahme der Verantwortung durch die Leitungsebene**
- Konzeption und Planung des Sicherheitsprozesses
- **Bereitstellung von finanziellen, personellen und zeitlichen Ressourcen** [...]“



Quelle: BSI-Standard 200-1

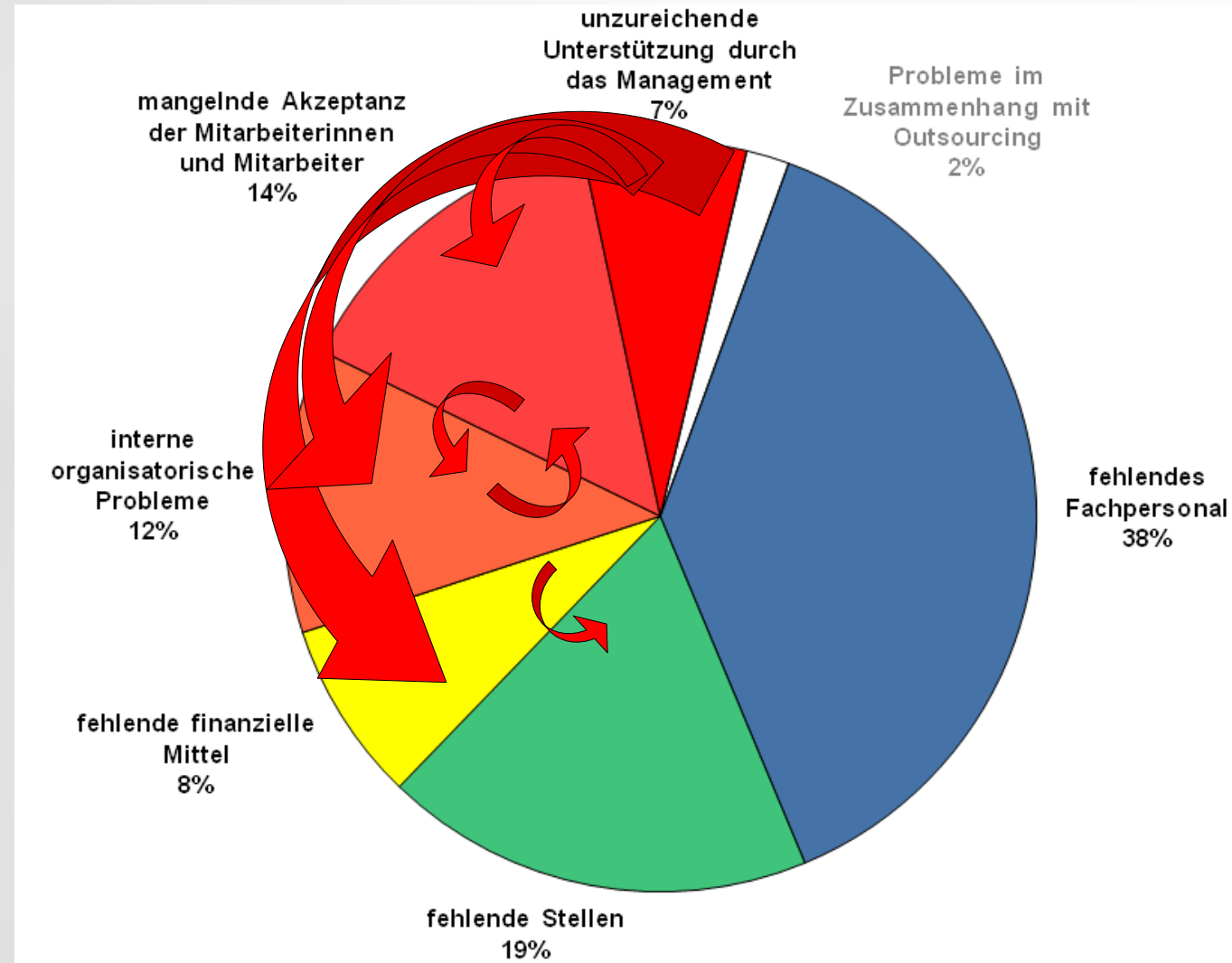


Haupthemmnisse für die Informationssicherheit

„Für die Gestaltung des Sicherheitsprozesses ist ein **systematisches Vorgehen** erforderlich, damit ein angemessenes Sicherheitsniveau erreicht werden kann.

Im Rahmen des IT-Grundschutzes besteht der Sicherheitsprozess aus den folgenden Phasen:

- Initiierung des Sicherheitsprozesses
- **Übernahme der Verantwortung durch die Leitungsebene**
- Konzeption und Planung des Sicherheitsprozesses
- **Bereitstellung von finanziellen, personellen und zeitlichen Ressourcen** [...]“



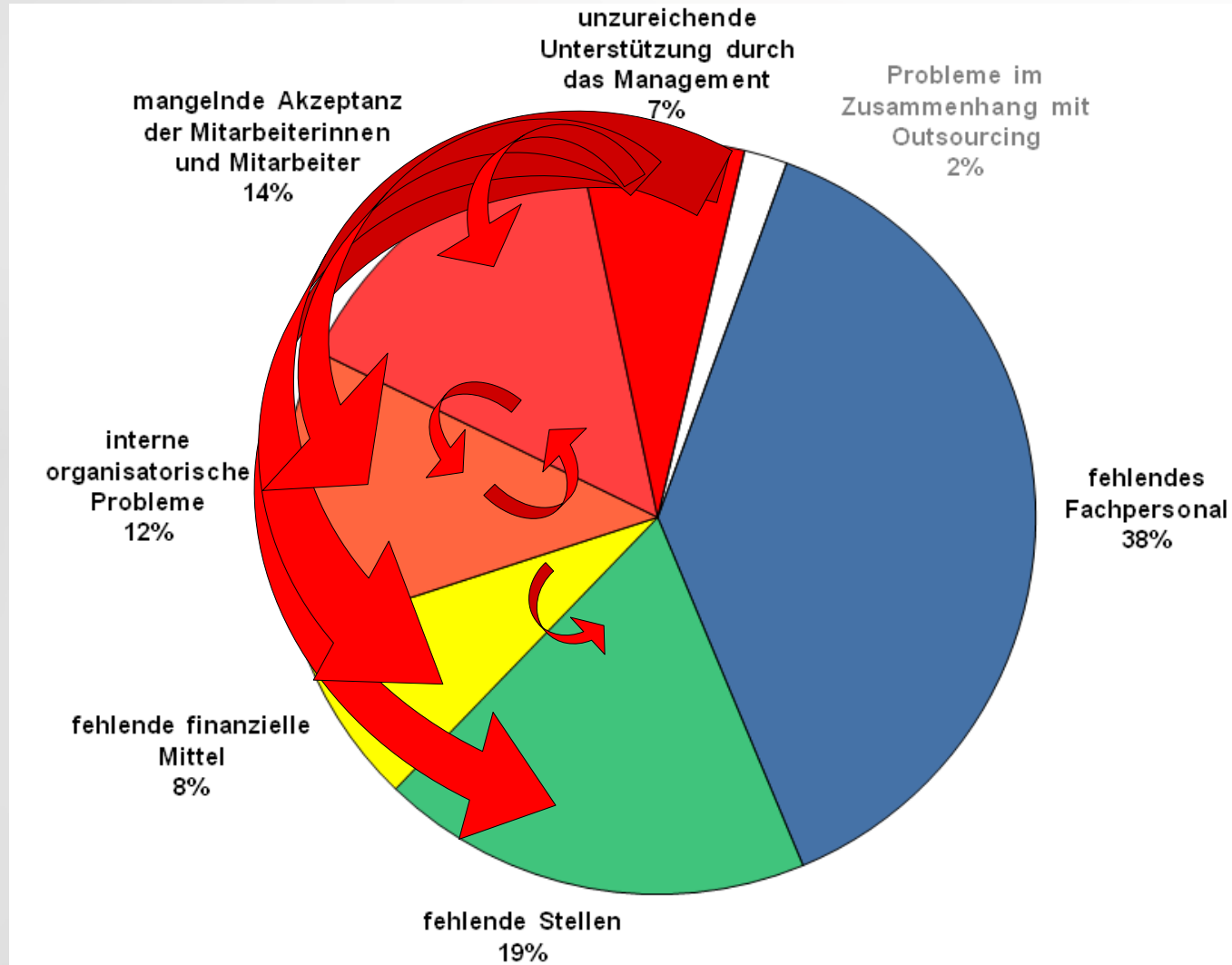
Quelle: BSI-Standard 200-1



Haupthemmnisse für die Informationssicherheit

„Die oberste Leitungsebene muss den **Sicherheitsprozess initiieren, steuern und kontrollieren.**

Die Leitungsebene ist diejenige Instanz, die die **Entscheidung über den Umgang mit Risiken** treffen und die entsprechenden Ressourcen zur Verfügung stellen muss. Die Verantwortung für Informationssicherheit verbleibt dort. Die operative Aufgabe „Informationssicherheit“ wird allerdings typischerweise an einen **Informationssicherheitsbeauftragten (ISB)** delegiert.“



Quelle: BSI-Standard 200-2

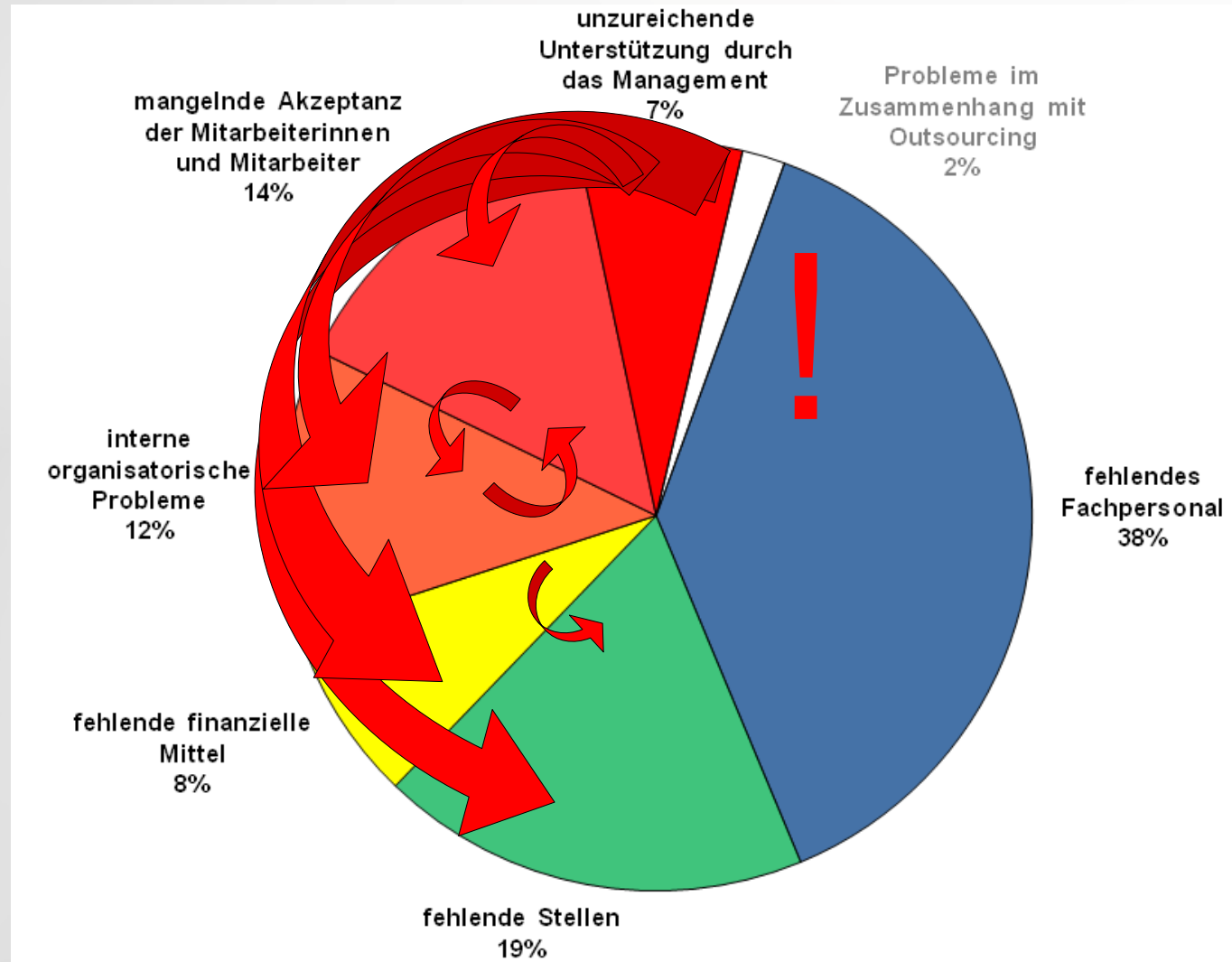


Hauptthemennisse für die Informationssicherheit

Durch die Schaffung von Stellen und den zunehmenden Einsatz von Fachkräften wird der Fachkräftemangel weiter verstärkt.

Kommunalverwaltungen können das Problem nicht lösen, aber im Rahmen ihrer Möglichkeiten Maßnahmen zur **Entwicklung, Gewinnung und Bindung der Fachkräfte** treffen.

Ausschließlich auf externe Dienstleister zu setzen, kann sich auf Dauer sowohl hinsichtlich der Kosten als auch unter dem Gesichtspunkt der Loyalität als problematisch erweisen.



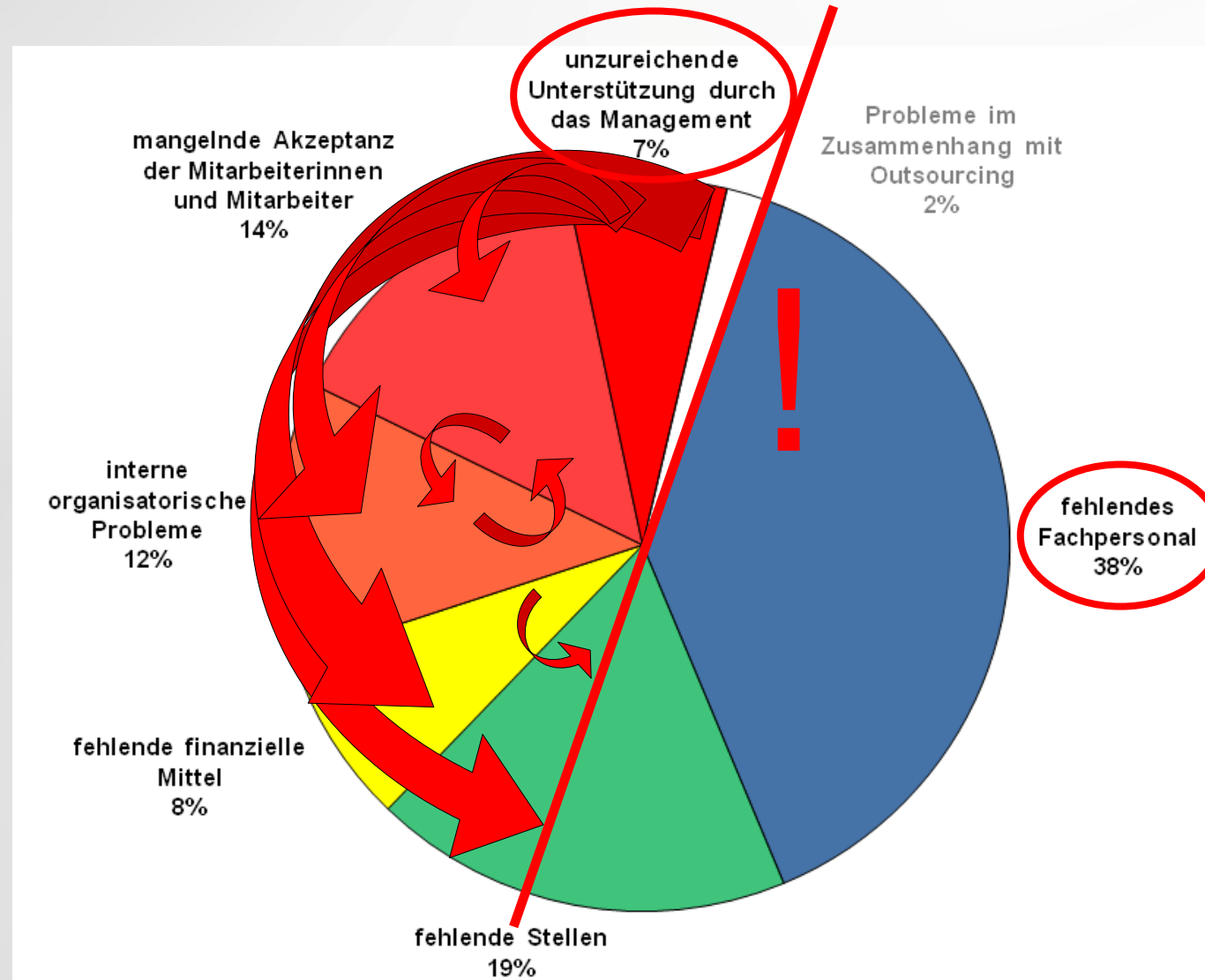


Haupthemmnisse für die Informationssicherheit

Fazit:

Etwa die Hälfte der genannten Hemmnisse scheint durch die **wirksame Wahrnehmung der Verantwortung der obersten Managementebene** der Kommunalverwaltungen lösbar.

Das am häufigsten genannte Hemmnis „**Fachkräftemangel**“ wird **weiter verstärkt** und erfordert - neben Maßnahmen auf Bundes- und Länderebene - im Rahmen der Möglichkeiten der Kommunalverwaltungen die Schaffung **attraktiver Rahmenbedingungen** sowie **nachhaltige Schritte der Personalentwicklung und -bindung**.





Info.IT-SiBe-Forum.de

Internetforum für IT-Sicherheitsbeauftragte von Kommunen und Ländern

Heino Sauerbrey

IT-Sicherheit,
Informationsmanagement,
Webmaster

Tel.: (030) 59 00 97 - 355

Fax.: (030) 59 00 97 - 400

E-Mail:

Heino.Sauerbrey@Landkreistag.de



Deutscher Landkreistag

Ulrich-von-Hassell-Haus

Lennéstraße 11

10785 Berlin

www.Landkreistag.de

www.Kreisnavigator.de

