DEUTSCHER LANDKREISTAG

Wie sag ich´s meinem Chef?

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

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

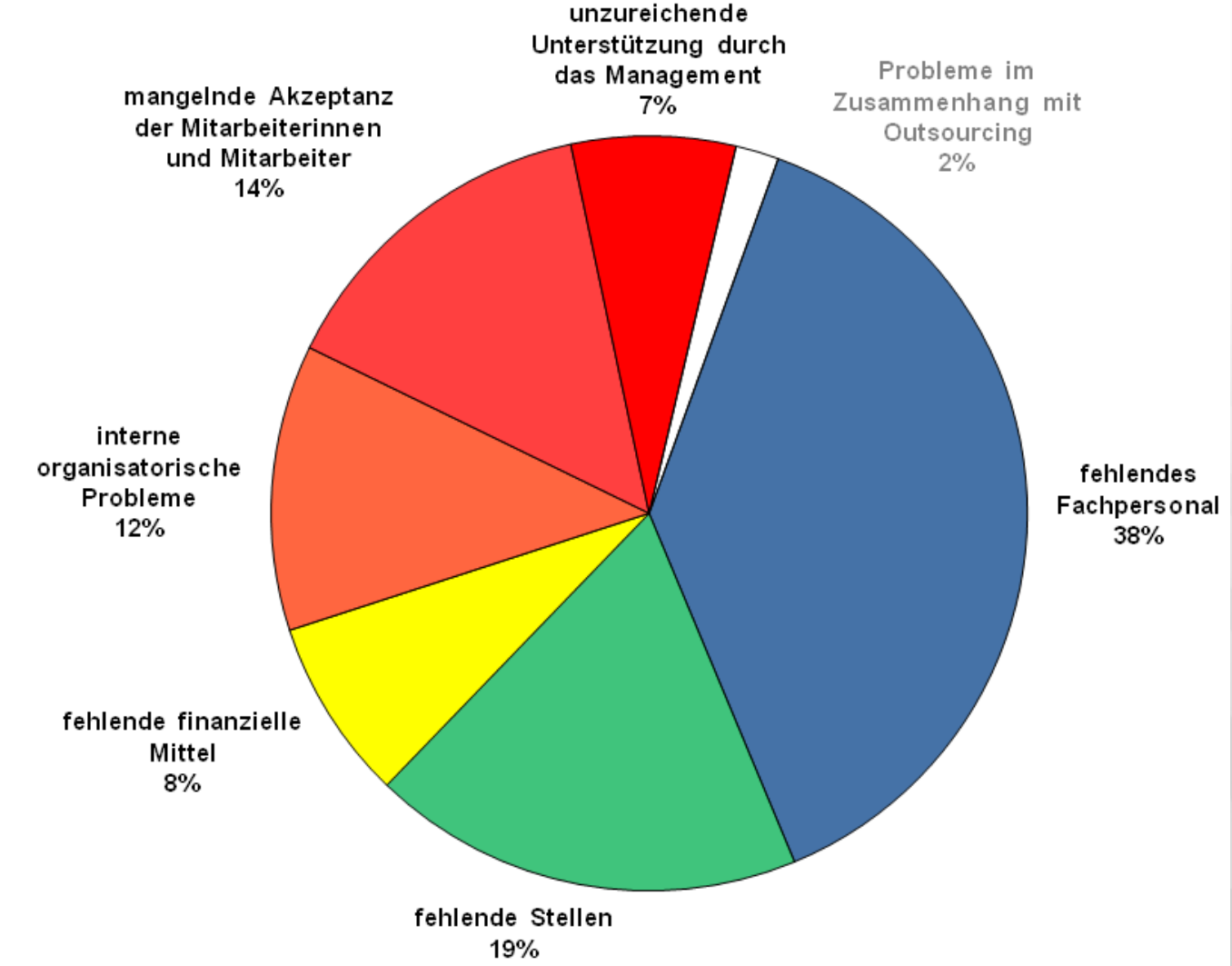
„Die folgenden Überlegungen verdeutlichen […] die **Bedeutung der Leitungsebene im Sicherheitsprozess**:

- 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

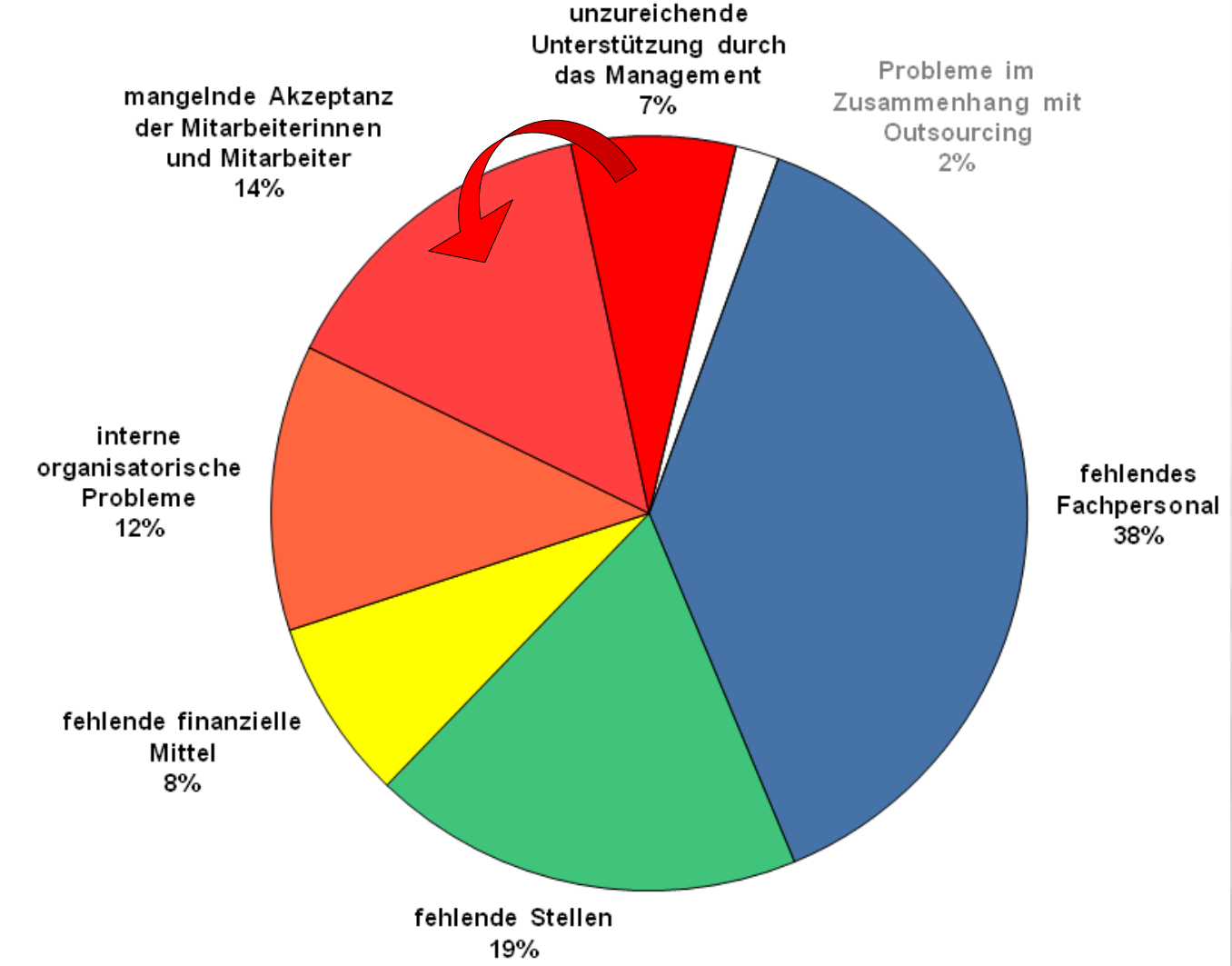
In einer Umfrage des DLT vom Sommer 2018, an der sich über 60% aller 294 Landkreise beteiligten, wurde die Multiple-Choice-Frage nach den **Haupthemmnissen für die Informations-sicherheit** mit folgender Häufigkeit beantwortet:



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

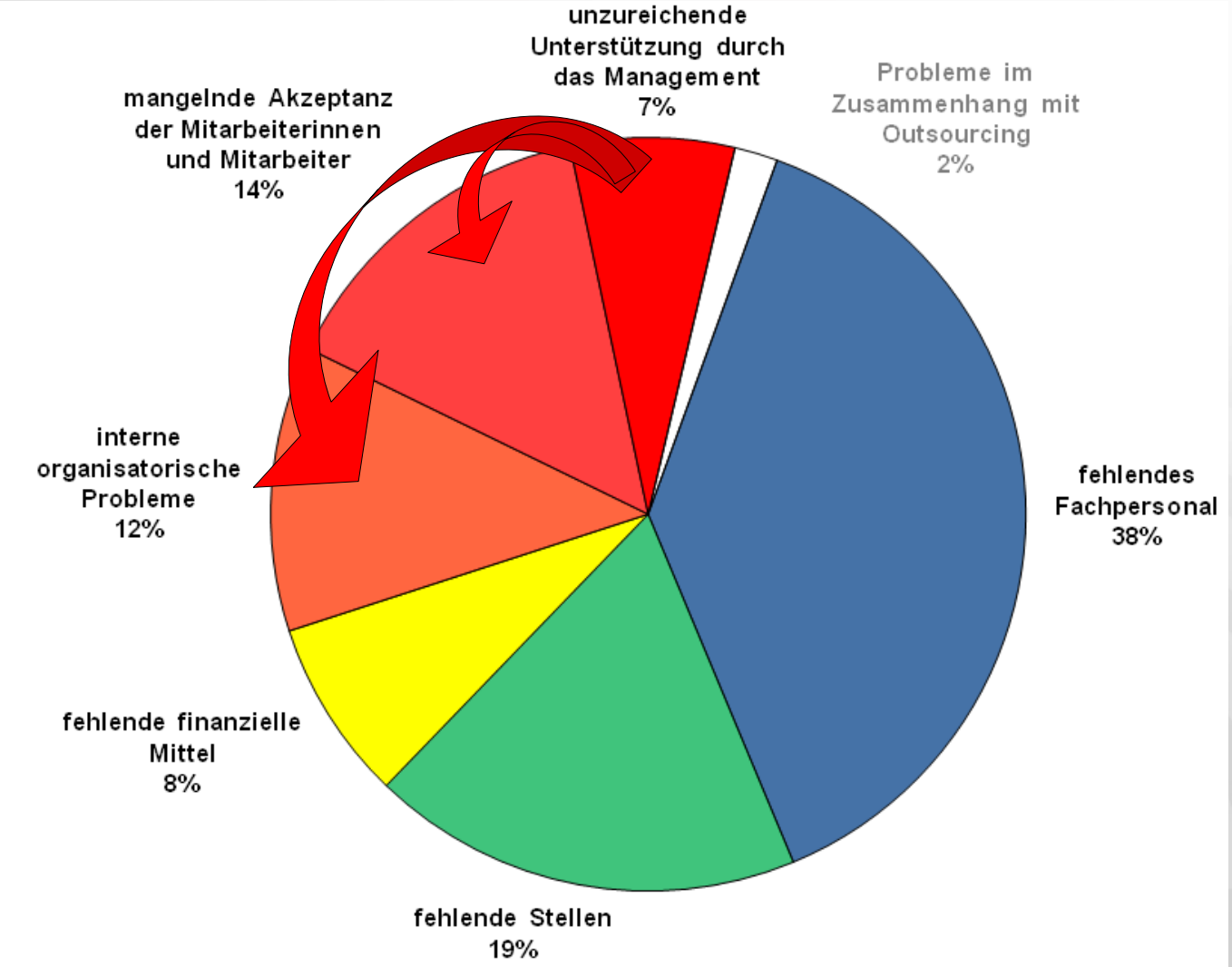


Haupthemmnisse für die Informationssicherheit

„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

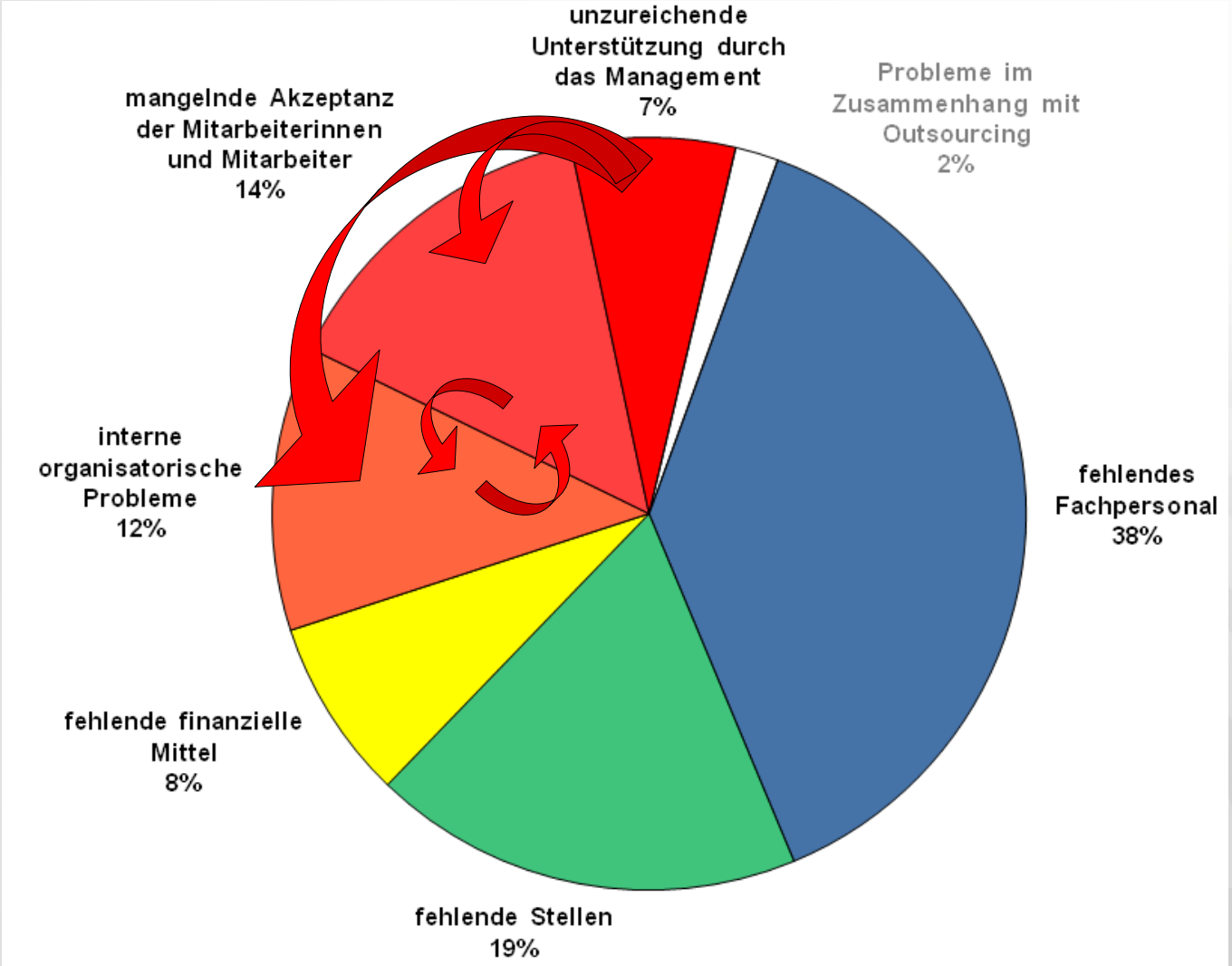


Haupthemmnisse für die Informationssicherheit

„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

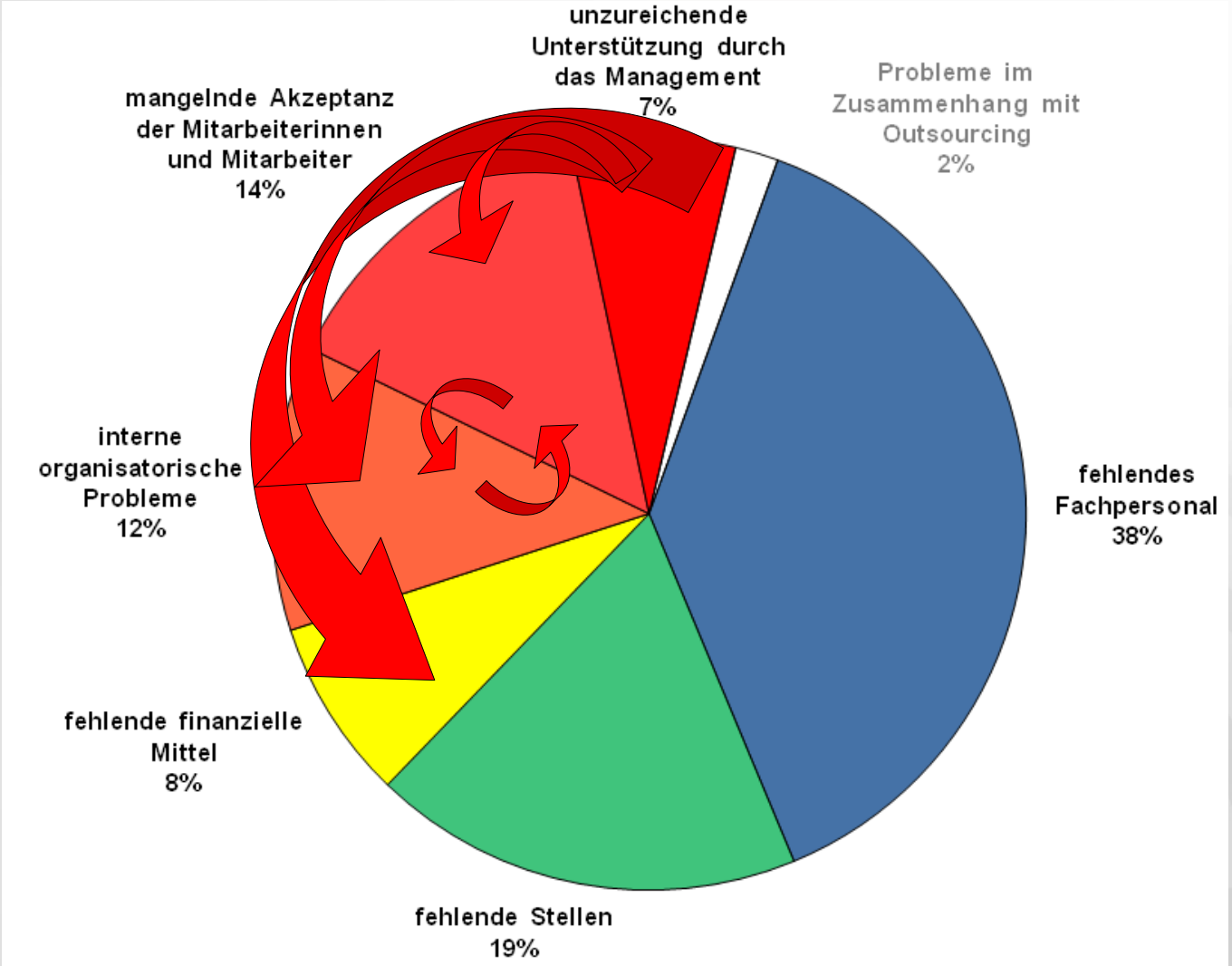


Haupthemmnisse für die Informationssicherheit

„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

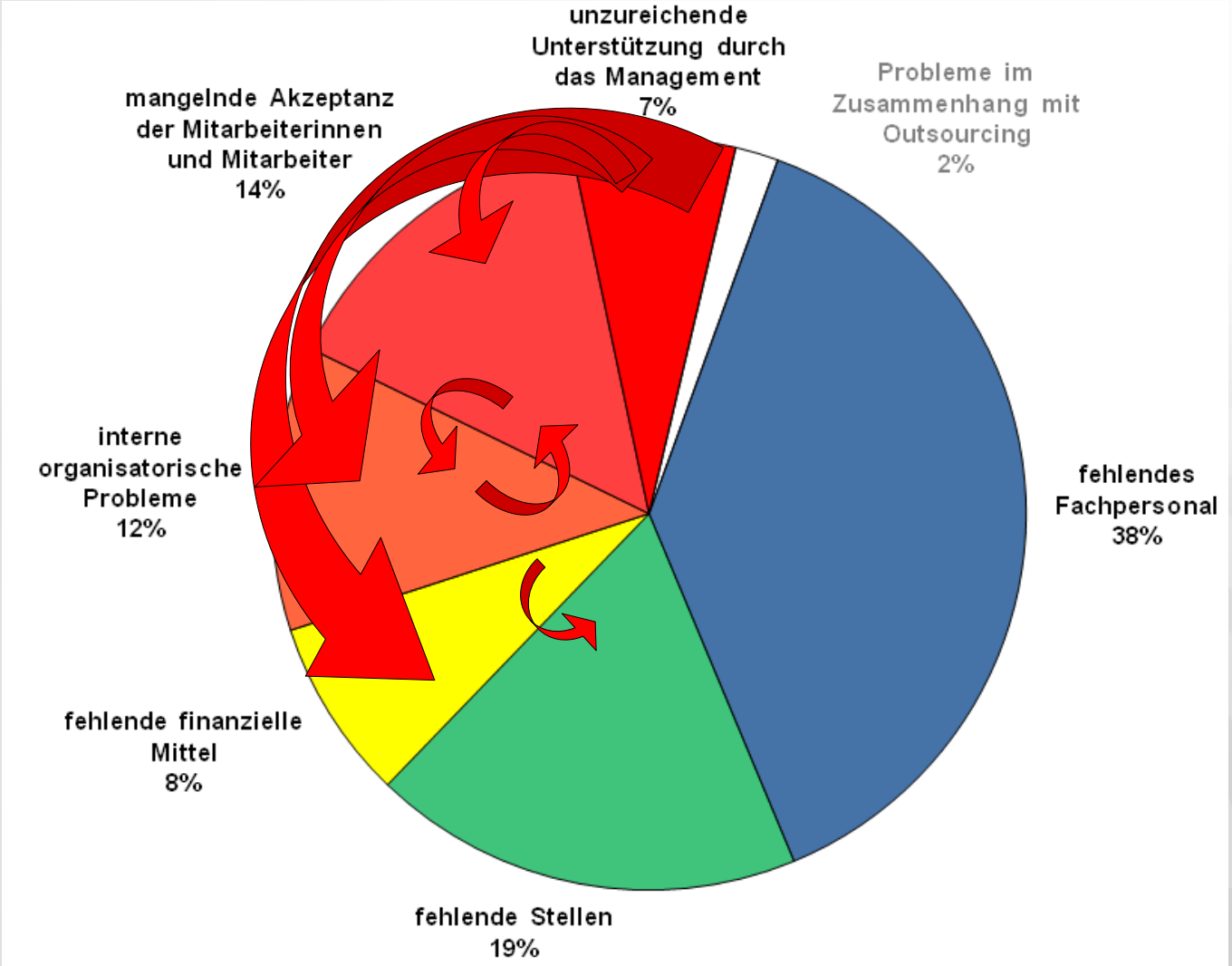


Haupthemmnisse für die Informationssicherheit

„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 […]“

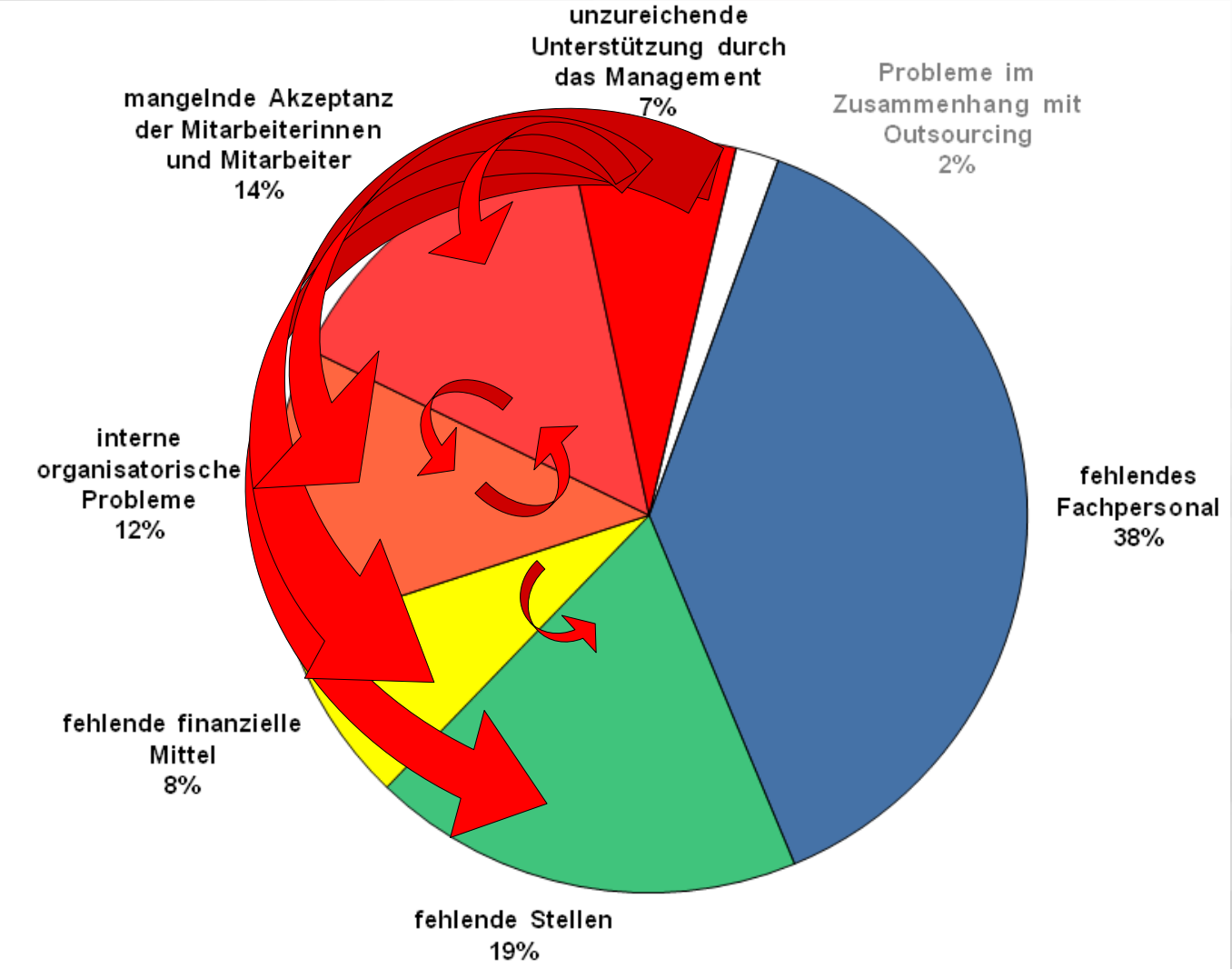
Quelle: BSI-Standard 200-1



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 „Informations-sicherheit“ wird allerdings typischerweise an einen Informations-sicherheitsbeauftragten (ISB) delegiert.“

Quelle: BSI-Standard 200-2

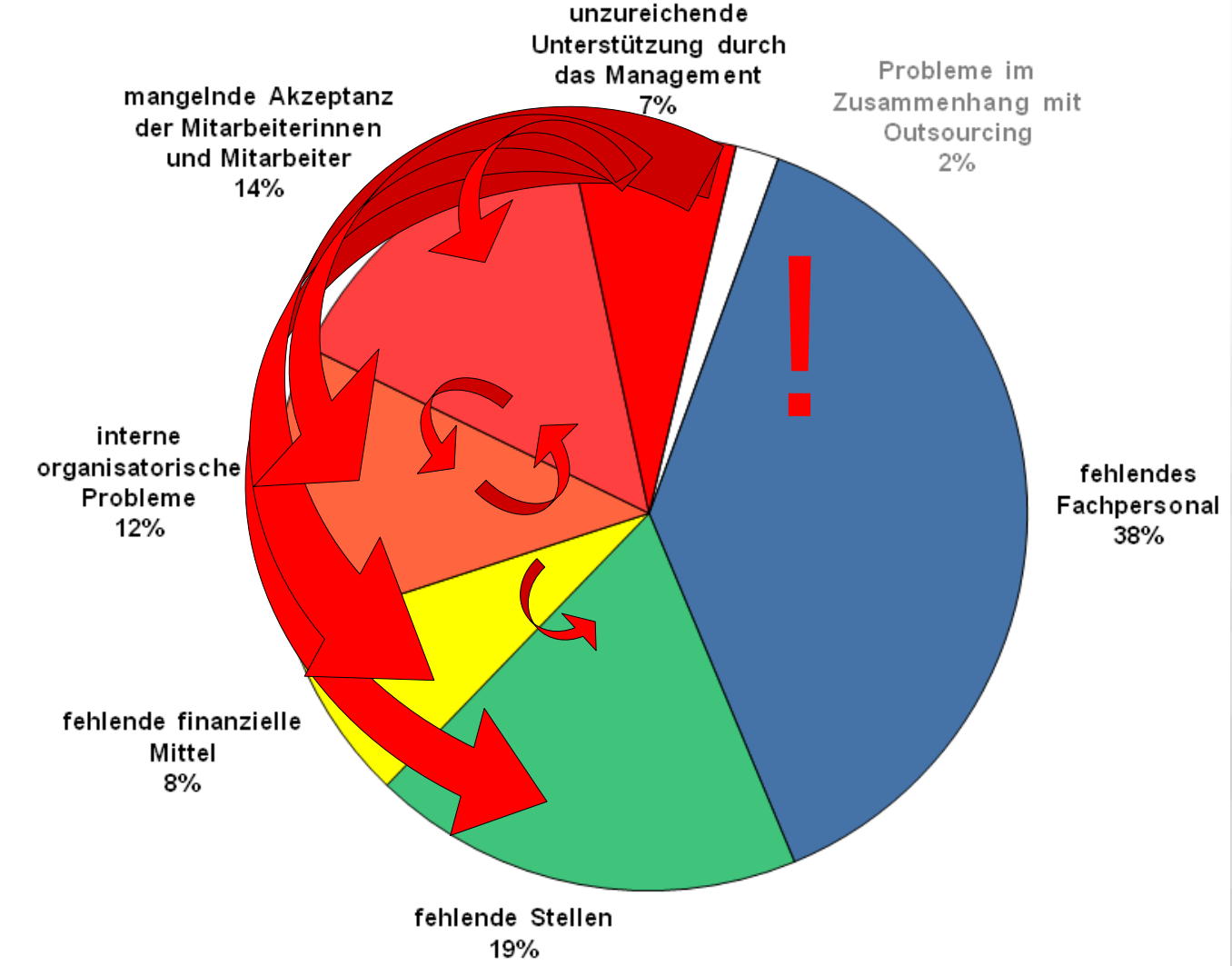


Haupthemmnisse für die Informationssicherheit

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.

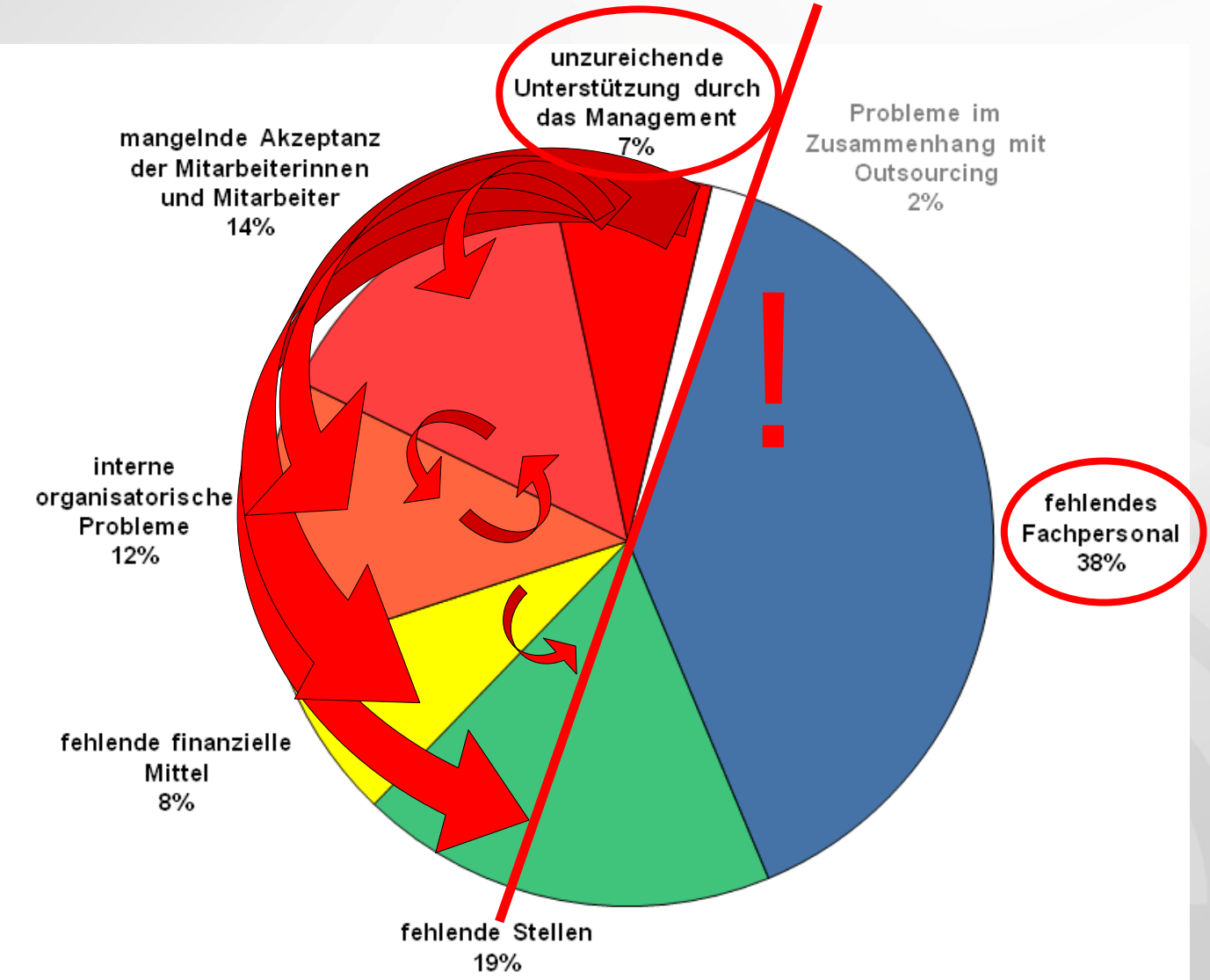


Haupthemmnisse für die Informationssicherheit

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 „Fachkräfte-mangel“ 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.



Thesen zur Awareness-Diskussion

Für die Etablierung von Informationssicherheit in öffentlichen Verwaltungen ist die Behördenspitze von entscheidender Bedeutung. Die Praxis zeigt, dass diese Zielgruppe häufig versucht, sich diesem Thema (z.B. Awareness-Veranstaltungen) zu entziehen und es als eines von vielen (wichtigen) Themen einzuordnen.

- **Mit welchen Differenzierungen können verschiedene Zielgruppen entsprechend ihren Besonderheiten wirksam angesprochen werden?**

- **Wie kann erreicht werden, dass die Behördenspitze Verständnis für Informationssicherheit entwickelt und das Thema angemessen berücksichtigt?**

Besondere Eigenschaften der Behördenspitze:

- Selbstbewusstsein / Durchsetzungsvermögen
- Konsequente Prioritätensetzung
- Erfahrung im Umgang mit Risiken
- Starke Orientierung an politischen Zielstellungen
- Sehr häufig juristische Ausbildung
- Standardreaktionen:
  - „Ich bin für vieles verantwortlich, kann aber nicht alles gleichermaßen berücksichtigen“.
  - „Wo steht, dass ich Informationssicherheit etablieren muss?“
  - „Wer kontrolliert, ob ich Informationssicherheit etabliert habe?“
  - „Was passiert, wenn ich erwischt werde?“

Thesen zur Awareness-Diskussion

Für die Etablierung von Informationssicherheit in öffentlichen Verwaltungen ist die Behördenspitze von entscheidender Bedeutung. Die Praxis zeigt, dass diese Zielgruppe häufig versucht, sich diesem Thema (z.B. Awareness-Veranstaltungen) zu entziehen und es als eines von vielen (wichtigen) Themen einzuordnen.

- **Mit welchen Differenzierungen können verschiedene Zielgruppen entsprechend ihren Besonderheiten wirksam angesprochen werden?**

- **Wie kann erreicht werden, dass die Behördenspitze Verständnis für Informationssicherheit entwickelt und das Thema angemessen berücksichtigt?**

Verhalten und Ansprechbarkeit der Nutzer ist abhängig von:

- Risiko-Typ
- Rolle / Funktion
- Wissen (über Risiken und Konsequenzen)
- Rahmenbedingungen (Vorhandensein von und Umgang mit Regelungen, Risikokultur, Gruppenzwänge)
- Alter und Erfahrungen (Zu hohe Erwartungen an „digital Natives“?)
- Geschlecht(?)

- **Mit welchen Differenzierungen können verschiedene Zielgruppen entsprechend ihren Besonderheiten wirksam angesprochen werden?**
- **Wie kann erreicht werden, dass die Behördenspitze Verständnis für Informations-sicherheit entwickelt und das Thema angemessen berücksichtigt?**

Thesen zur Awareness-Diskussion

Verhalten und Ansprechbarkeit der Nutzer ist abhängig von:

- Risiko-Typ
- Rolle / Funktion
- Wissen (über Risiken und Konsequenzen)
- Rahmenbedingungen (Vorhandensein von und Umgang mit Regelungen, Risikokultur, Gruppenzwänge)
- Alter und Erfahrungen (Zu hohe Erwartungen an „digital Natives“?)
- Geschlecht?

Besondere Eigenschaften der Behördenspitze:

- Selbstbewusstsein und Durchsetzungsvermögen
- Konsequente Prioritätensetzung
- Erfahrung im Umgang mit Risiken
- Starke Orientierung an politischen Zielstellungen
- Sehr häufig juristische Ausbildung
- Typische Standard-Abwehrreaktionen:
  - „Ich bin für vieles verantwortlich, kann aber nicht alles gleichermaßen berücksichtigen“.
  - „Wo steht, dass ich Informationssicherheit etablieren muss?“
  - „Wer kontrolliert, ob ich Informationssicherheit etabliert habe?“
  - „Was passiert, wenn ich erwischt werde?“

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

IT-SiBe-Forum