DEUTSCHER LANDKREISTAG

Informationssicherheit in Kommunalverwaltungen

- **Was wurde bisher erreicht?**
- **Was sind die wichtigsten Hemmnisse?**
- **10 Tipps gegen lästige Informationssicherheitsbeauftragte**
- **Nachlese: Verantwortung für Informationssicherheit**

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

Informationssicherheit in Kommunen

Was wurde erreicht?

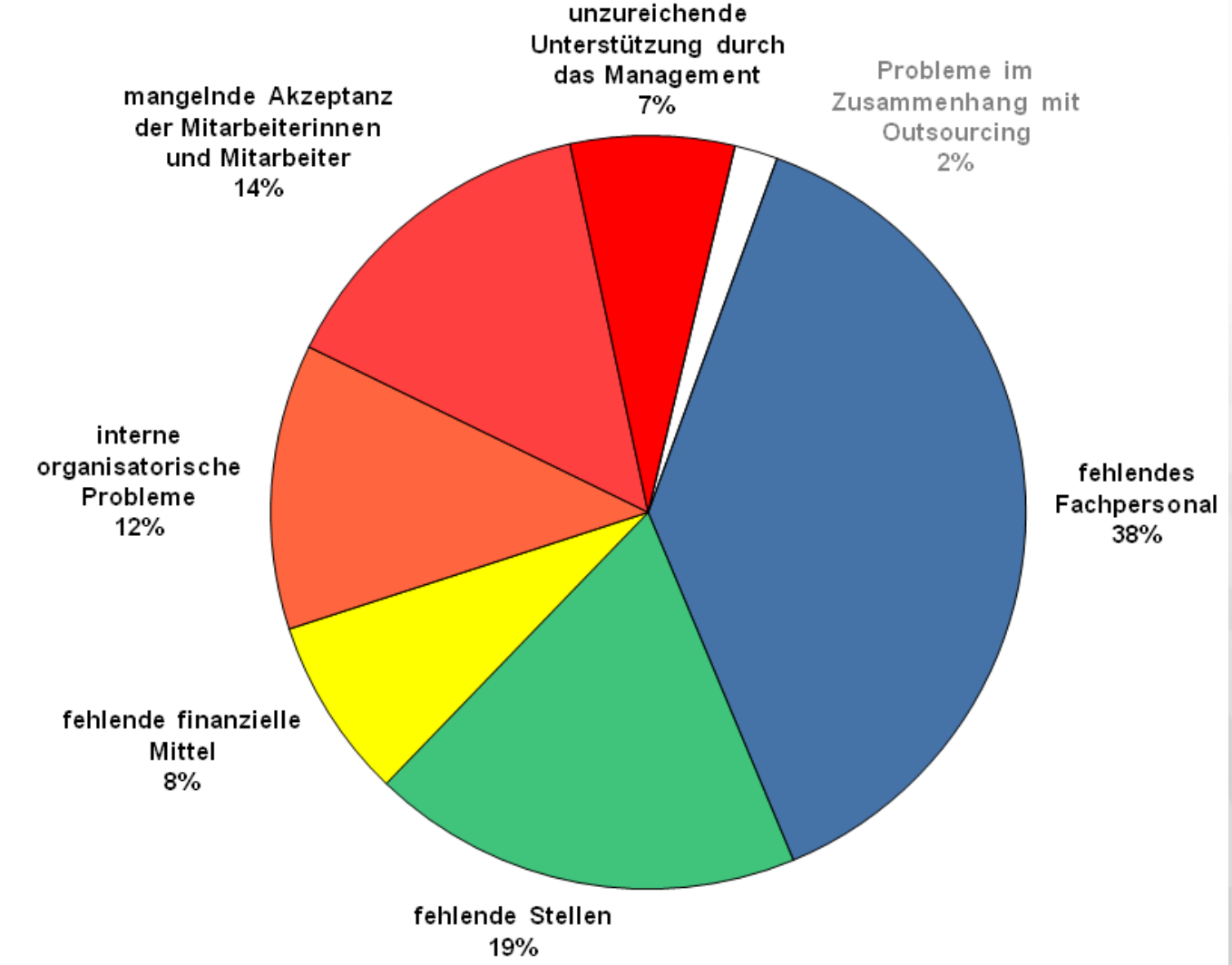
Ausgewählte Beispiele:

- Informationsaustausch von derzeit ca. 700 ISB von Kommunen und Ländern über das IT-SiBe-Forum (http://info.it-sibe-forum.de/) (seit 2013)
- Erarbeitung der „Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie des IT-Planungsrates in Kommunalverwaltungen“.
- Erarbeitung der „Leitlinie zum ersetzenden Scannen in Kommunen nach TR RESISCAN“ einschl. Schutzbedarfsanalyse und Musterverfahrensbeschreibung.
- Erarbeitung des IT-Grundschutzprofils „Basis-Absicherung Kommunalverwaltung“ (sog. „Kommunalprofil“) als erstes Branchenprofil des modernisierten IT Grundschutzes.
- Bisher 6 Kommunale IT-Sicherheitskongresse
- Hospitationen des BSI in Kommunalverwaltungen
- Geplante Erarbeitung eines IT-Grundschutzprofils „Schule“
- …

Informationssicherheit in Kommunen

Was sind die wichtigsten Hemmnisse?

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:

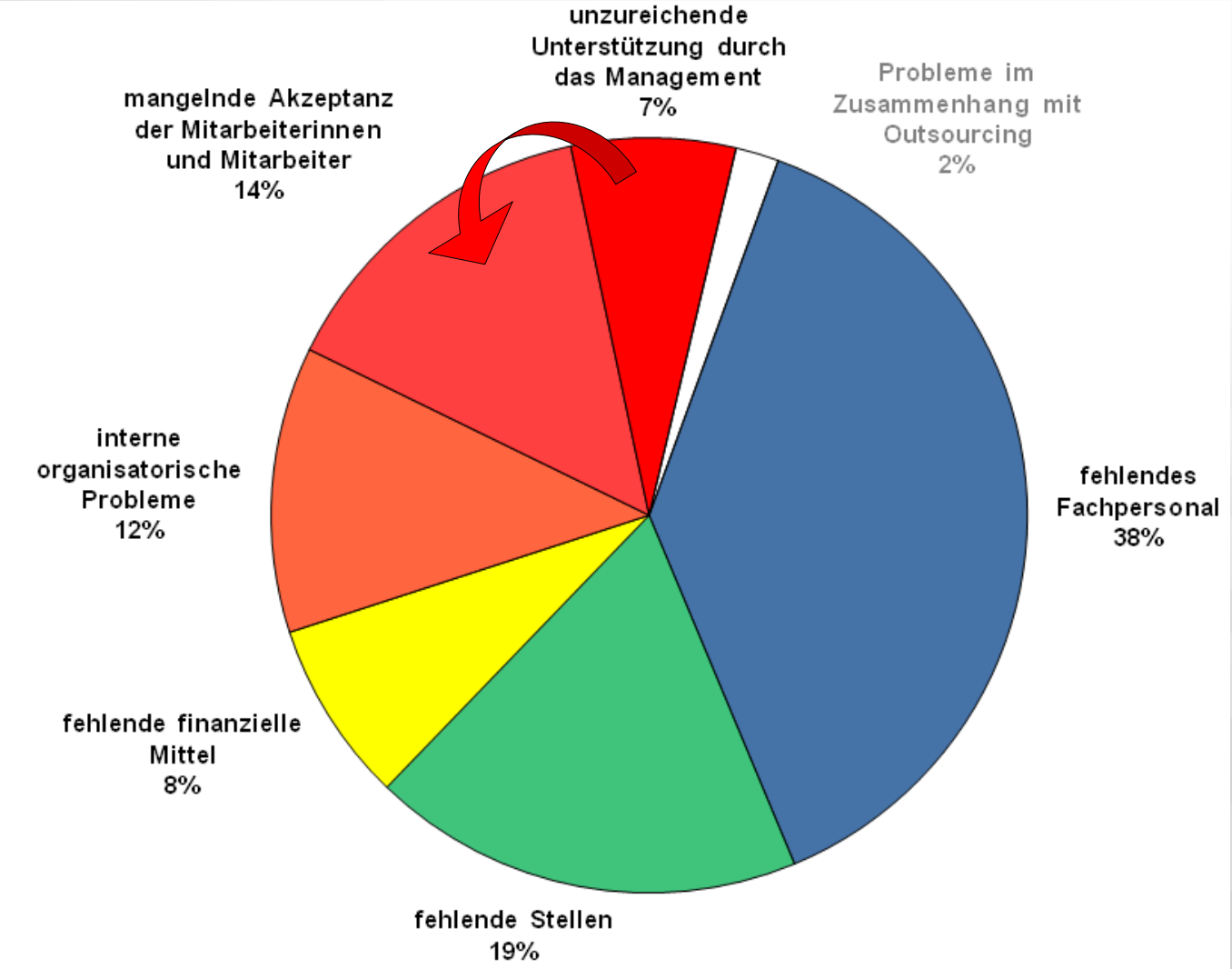


Informationssicherheit in Kommunen

Was sind die wichtigsten Hemmnisse?

„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



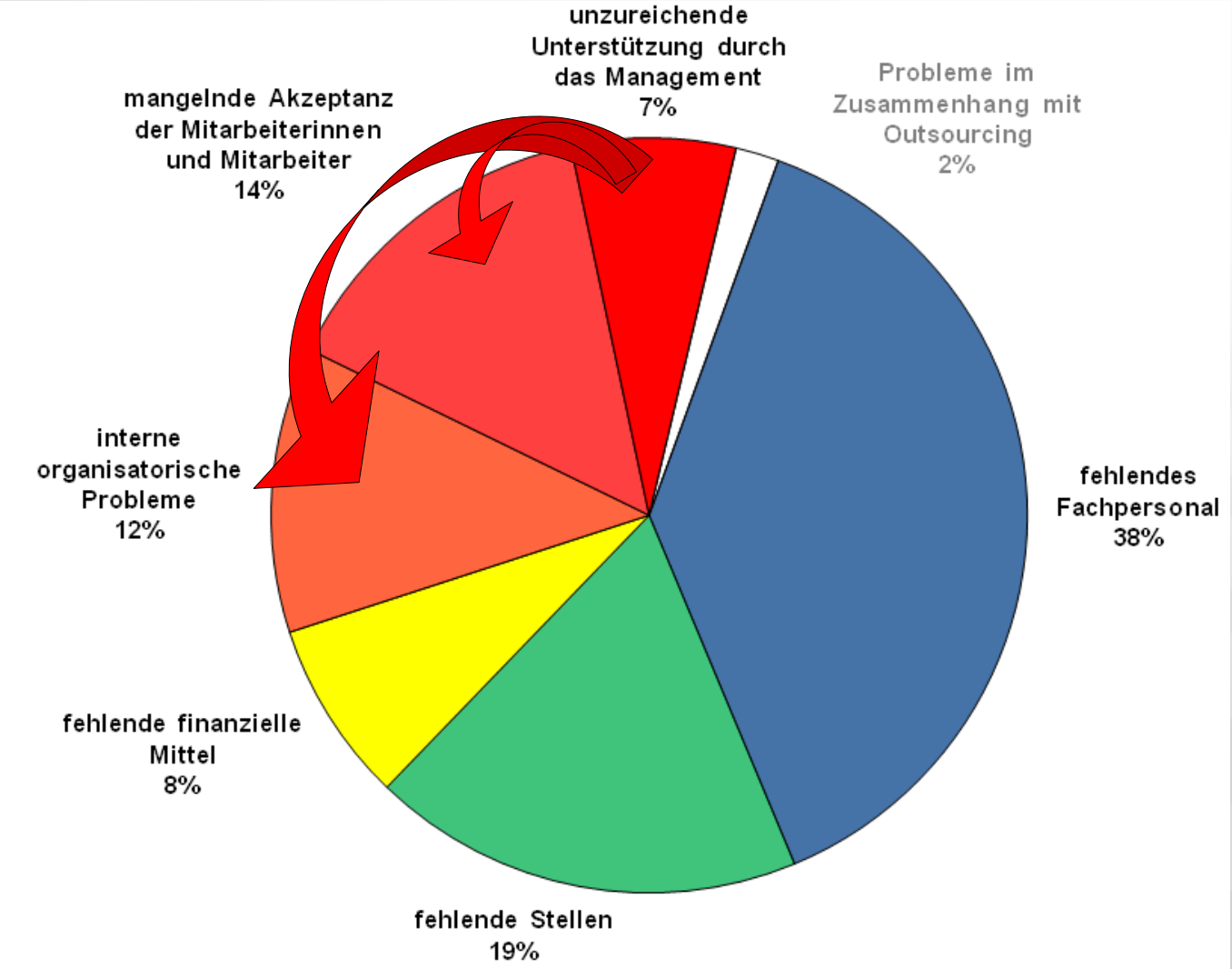
Informationssicherheit in Kommunen

Was sind die wichtigsten Hemmnisse?

„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



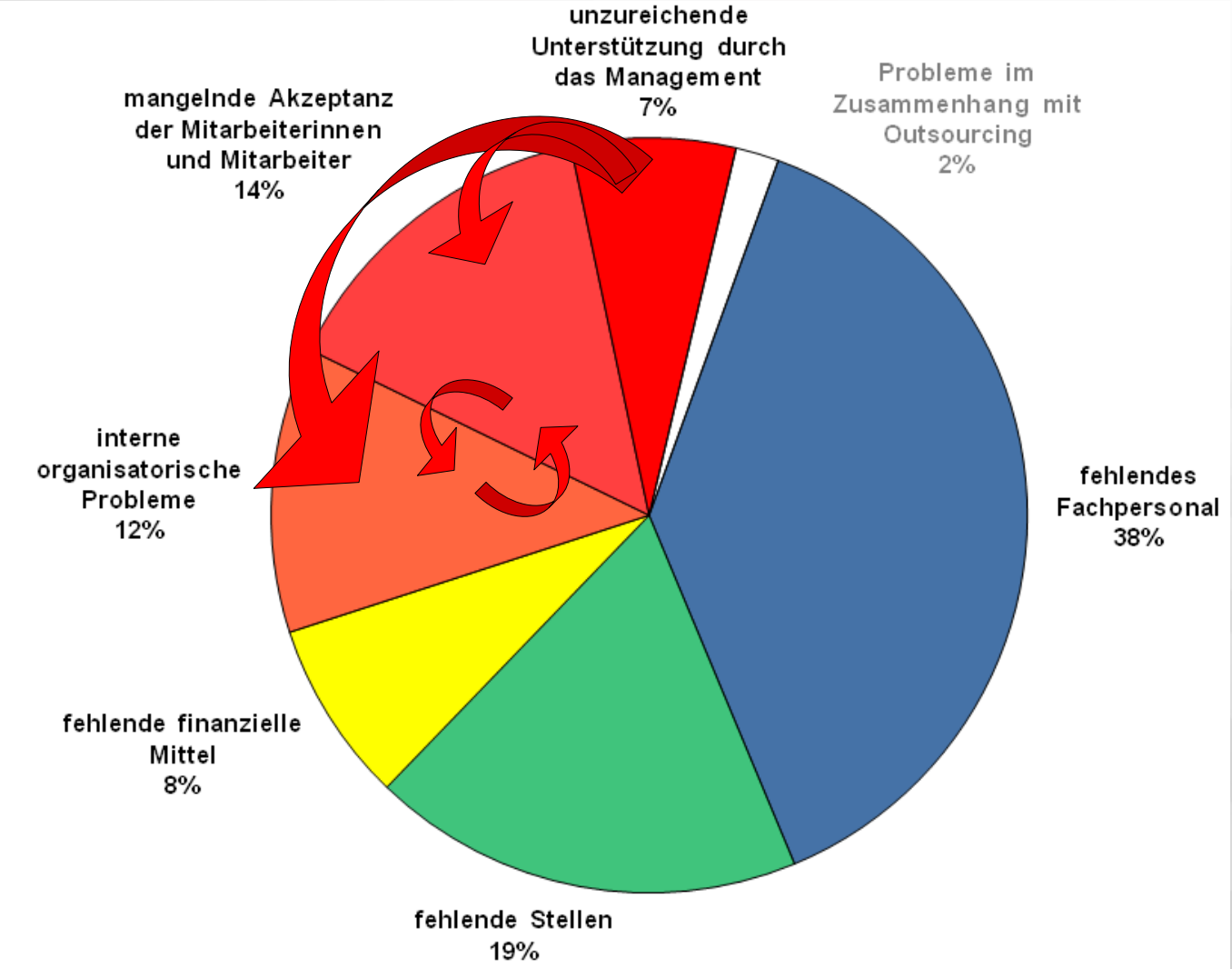
Informationssicherheit in Kommunen

Was sind die wichtigsten Hemmnisse?

„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



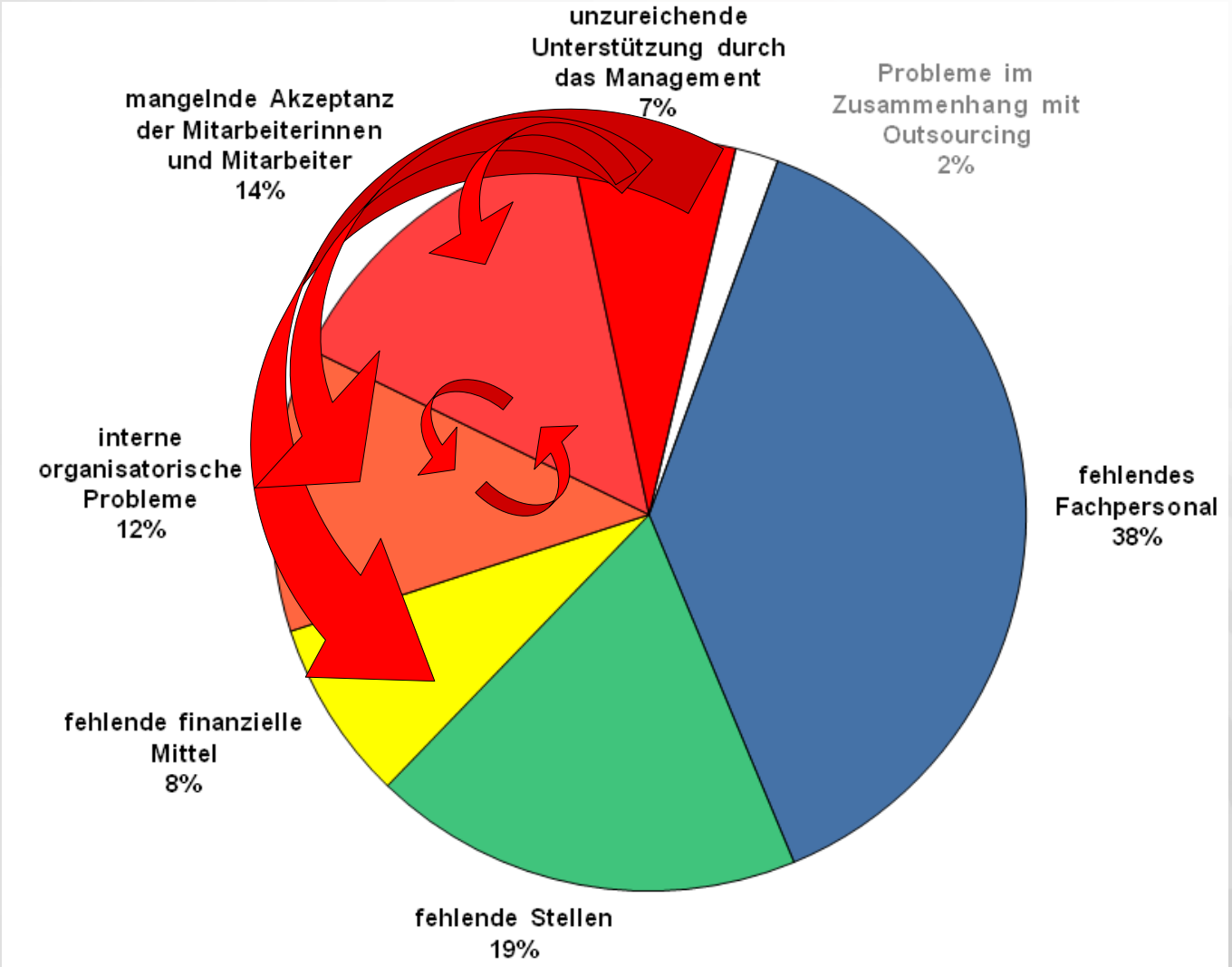
Informationssicherheit in Kommunen

Was sind die wichtigsten Hemmnisse?

„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



Informationssicherheit in Kommunen

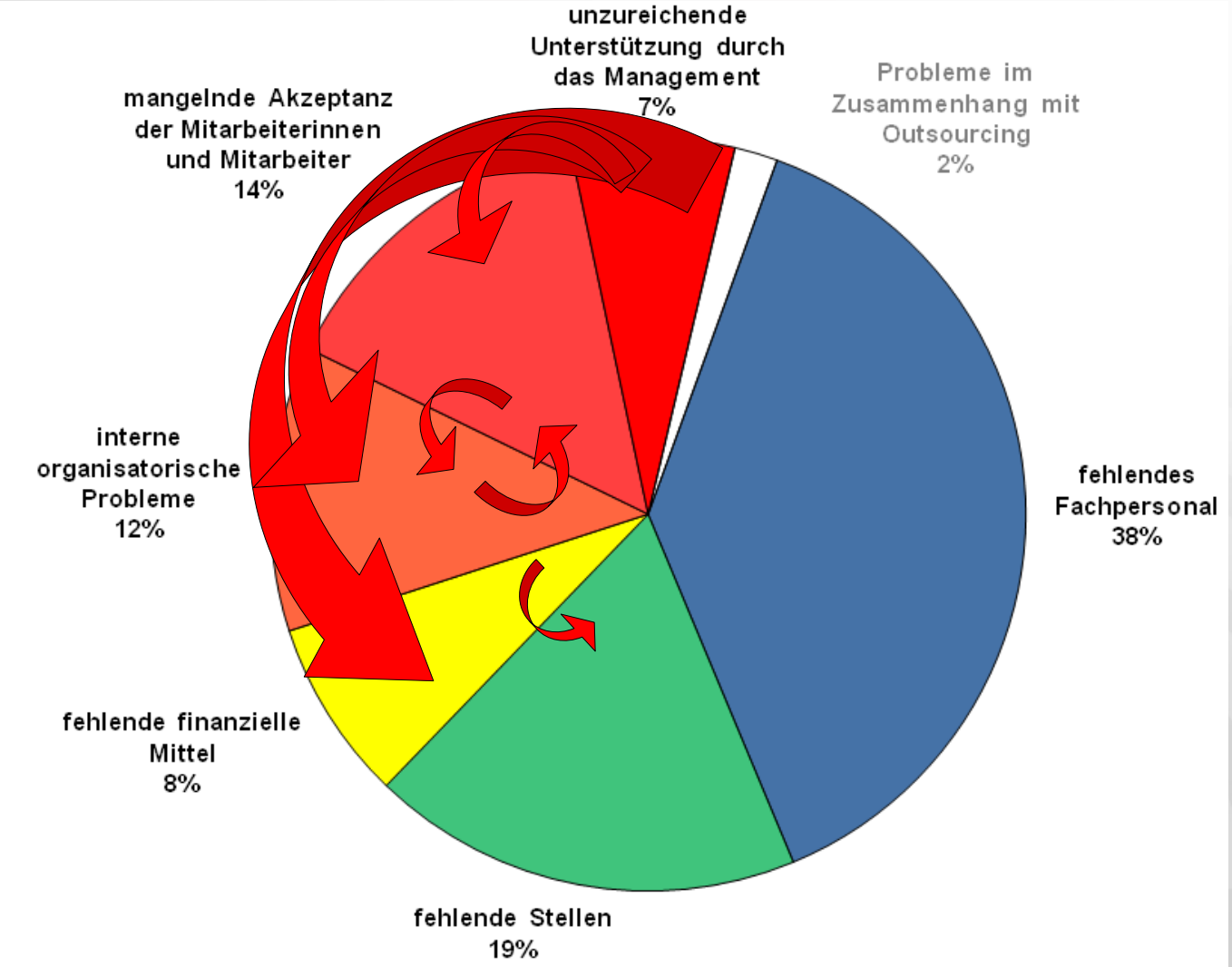
Was sind die wichtigsten Hemmnisse?

„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

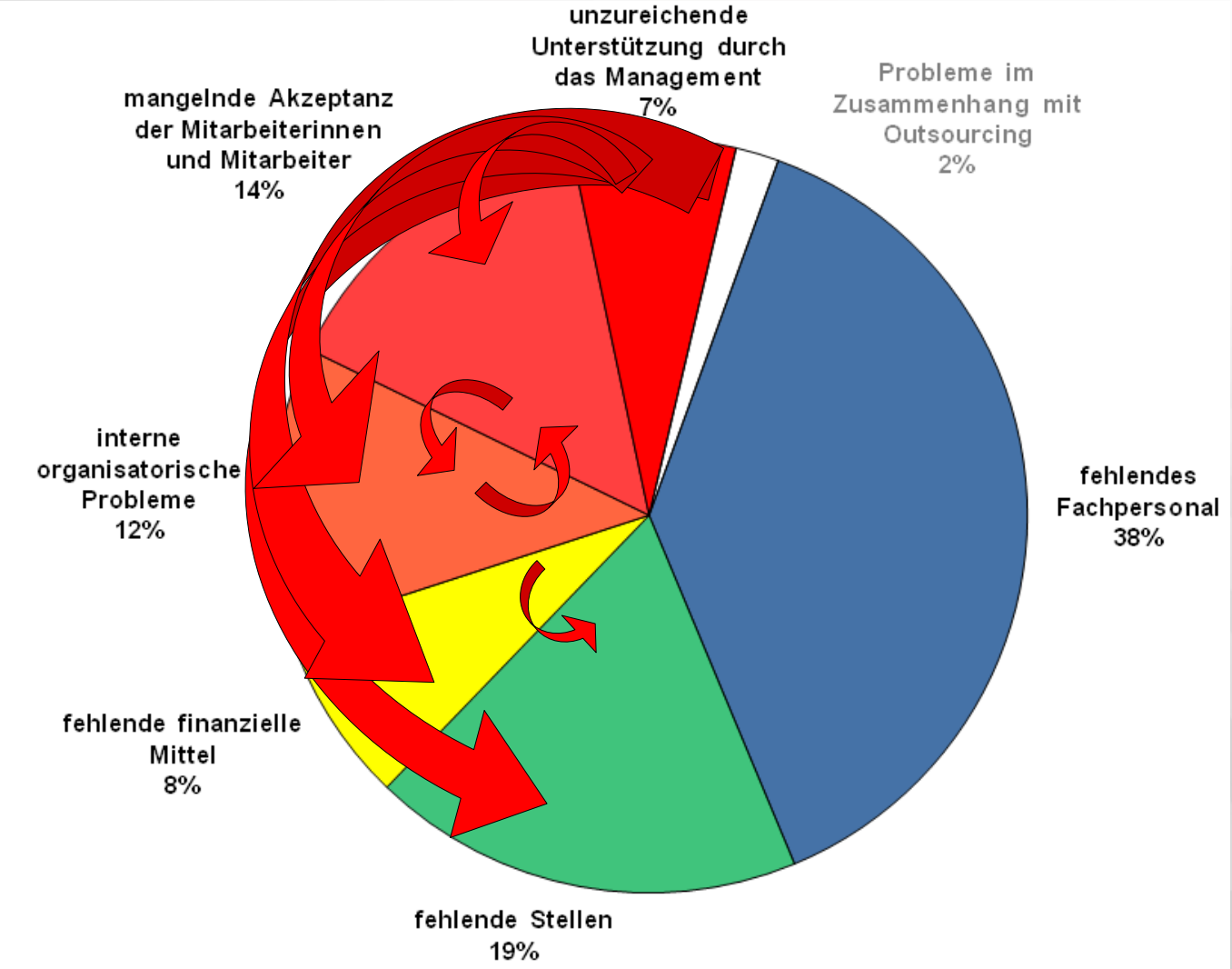


Informationssicherheit in Kommunen

Was sind die wichtigsten Hemmnisse?

„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



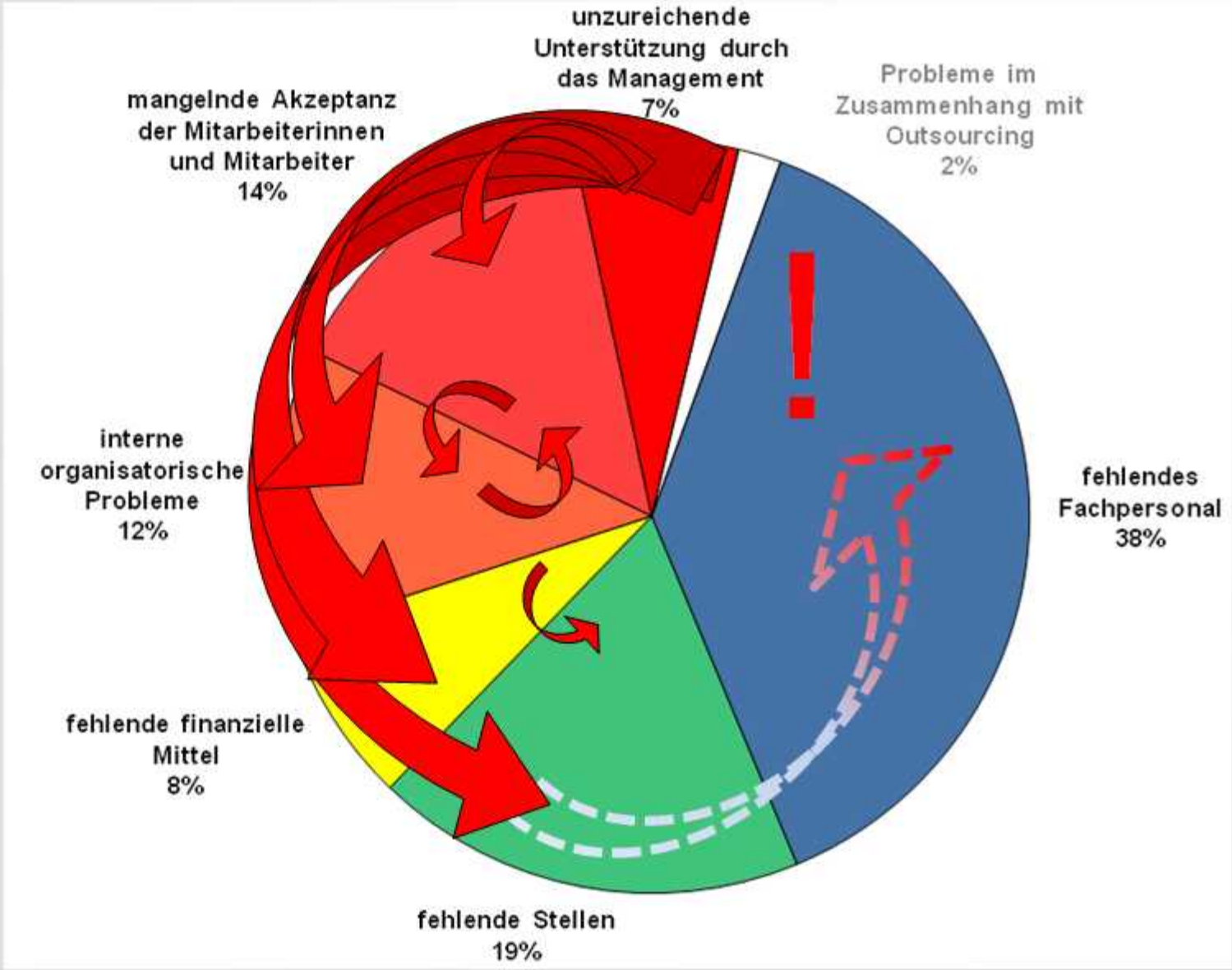
Informationssicherheit in Kommunen

Was sind die wichtigsten Hemmnisse?

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.



<ironie>

Was kann man gegen lästige Informationssicherheitsbeauftragte (ISB) tun?

Eigentlich sind die IT-Leute doch schon schlimm genug. Sie haben offensichtlich den ganzen Tag nichts zu tun, weil die Arbeit sowieso von den vielen Computern erledigt wird. Trotzdem schaffen sie es immer wieder, mit Wartungsarbeiten und anderen Schikanen auf sich aufmerksam zu machen.

Und nun tauchen auch noch diese Informationssicherheitsbeauftragten auf, die immer öfter allen Mitarbeitern - einschließlich der IT-Abteilung - zur Last fallen und nicht einmal vor der Leitungsebene zurückschrecken. Diese paranoiden Nervensägen mischen sich in bewährte Arbeitsabläufe ein, wollen bequeme Verhaltensweisen ändern und malen ständig den Teufel an die Wand. Was früher bequem und einfach war, machen sie kompliziert oder unmöglich.

Zum Schutz vor dem Einfluss dieser Störenfriede habe ich für die Leitungsebene

„10 Goldene Regeln gegen lästige Informationssicherheitsbeauftragte (ISB)“

zusammengestellt:

</ironie>

<ironie>

10 Goldene Regeln gegen lästige Informationssicherheitsbeauftragte (ISB)

1. Im Idealfall setzen Sie keinen Informationssicherheitsbeauftragten ein, so kann er weder die gewohnten Abläufe stören noch Folgekosten verursachen.

</ironie>

<ironie>

10 Goldene Regeln gegen lästige Informationssicherheitsbeauftragte (ISB)

1. Im Idealfall setzen Sie keinen Informationssicherheitsbeauftragten ein, so kann er weder die gewohnten Abläufe stören noch Folgekosten verursachen.
2. Wenn Sie es nicht völlig verhindern können, wählen Sie eine inkompetente, überforderte Person aus, die möglichst frei von Empathie und Verantwortungsbewusstsein ist.

</ironie>

<ironie>

10 Goldene Regeln gegen lästige Informationssicherheitsbeauftragte (ISB)

1. Im Idealfall setzen Sie keinen Informationssicherheitsbeauftragten ein, so kann er weder die gewohnten Abläufe stören noch Folgekosten verursachen.
2. Wenn Sie es nicht völlig verhindern können, wählen Sie eine inkompetente, überforderte Person aus, die möglichst frei von Empathie und Verantwortungsbewusstsein ist.
3. Etablieren Sie möglichst mehrere Hierarchieebenen zwischen Behördenleitung und ISB.

</ironie>

<ironie>

10 Goldene Regeln gegen lästige Informationssicherheitsbeauftragte (ISB)

1. Im Idealfall setzen Sie keinen Informationssicherheitsbeauftragten ein, so kann er weder die gewohnten Abläufe stören noch Folgekosten verursachen.
2. Wenn Sie es nicht völlig verhindern können, wählen Sie eine inkompetente, überforderte Person aus, die möglichst frei von Empathie und Verantwortungsbewusstsein ist.
3. Etablieren Sie möglichst mehrere Hierarchieebenen zwischen Behördenleitung und ISB.
4. Vermeiden Sie den Kontakt der Leitung mit dem ISB.

</ironie>

<ironie>

10 Goldene Regeln gegen lästige Informationssicherheitsbeauftragte (ISB)

1. Im Idealfall setzen Sie keinen Informationssicherheitsbeauftragten ein, so kann er weder die gewohnten Abläufe stören noch Folgekosten verursachen.
2. Wenn Sie es nicht völlig verhindern können, wählen Sie eine inkompetente, überforderte Person aus, die möglichst frei von Empathie und Verantwortungsbewusstsein ist.
3. Etablieren Sie möglichst mehrere Hierarchieebenen zwischen Behördenleitung und ISB.
4. Vermeiden Sie den Kontakt der Leitung mit dem ISB.
5. Geben Sie Ihrem ISB weder Rechte noch Ressourcen.

</ironie>

<ironie>

10 Goldene Regeln gegen lästige Informationssicherheitsbeauftragte (ISB)

1. Im Idealfall setzen Sie keinen Informationssicherheitsbeauftragten ein, so kann er weder die gewohnten Abläufe stören noch Folgekosten verursachen.
2. Wenn Sie es nicht völlig verhindern können, wählen Sie eine inkompetente, überforderte Person aus, die möglichst frei von Empathie und Verantwortungsbewusstsein ist.
3. Etablieren Sie möglichst mehrere Hierarchieebenen zwischen Behördenleitung und ISB.
4. Vermeiden Sie den Kontakt der Leitung mit dem ISB.
5. Geben Sie Ihrem ISB weder Rechte noch Ressourcen.
6. Weisen Sie dem ISB max. 10% der Arbeitszeit für die Wahrnehmung der ISB-Tätigkeit zu.

</ironie>

<ironie>

10 Goldene Regeln gegen lästige Informationssicherheitsbeauftragte (ISB)

1. Im Idealfall setzen Sie keinen Informationssicherheitsbeauftragten ein, so kann er weder die gewohnten Abläufe stören noch Folgekosten verursachen.
2. Wenn Sie es nicht völlig verhindern können, wählen Sie eine inkompetente, überforderte Person aus, die möglichst frei von Empathie und Verantwortungsbewusstsein ist.
3. Etablieren Sie möglichst mehrere Hierarchieebenen zwischen Behördenleitung und ISB.
4. Vermeiden Sie den Kontakt der Leitung mit dem ISB.
5. Geben Sie Ihrem ISB weder Rechte noch Ressourcen.
6. Weisen Sie dem ISB max. 10% der Arbeitszeit für die Wahrnehmung der ISB-Tätigkeit zu.
7. Sollte Ihr 10%-ISB aktiv werden und bewährte Abläufe stören, ist die Belastung der anderen 90% des Arbeitszeitanteils zu erhöhen, bis wieder Ruhe einkehrt.

</ironie>

<ironie>

10 Goldene Regeln gegen lästige Informationssicherheitsbeauftragte (ISB)

1. Im Idealfall setzen Sie keinen Informationssicherheitsbeauftragten ein, so kann er weder die gewohnten Abläufe stören noch Folgekosten verursachen.
2. Wenn Sie es nicht völlig verhindern können, wählen Sie eine inkompetente, überforderte Person aus, die möglichst frei von Empathie und Verantwortungsbewusstsein ist.
3. Etablieren Sie möglichst mehrere Hierarchieebenen zwischen Behördenleitung und ISB.
4. Vermeiden Sie den Kontakt der Leitung mit dem ISB.
5. Geben Sie Ihrem ISB weder Rechte noch Ressourcen.
6. Weisen Sie dem ISB max. 10% der Arbeitszeit für die Wahrnehmung der ISB-Tätigkeit zu.
7. Sollte Ihr 10%-ISB aktiv werden und bewährte Abläufe stören, ist die Belastung der anderen 90% des Arbeitszeitanteils zu erhöhen, bis wieder Ruhe einkehrt.
8. Qualifizierung ist überbewertet. Sie kostet Zeit und Geld und es ist nicht auszuschließen, dass der ISB vom Lehrgang irgendwelche Ideen mitbringt.

</ironie>

<ironie>

10 Goldene Regeln gegen lästige Informationssicherheitsbeauftragte (ISB)

1. Im Idealfall setzen Sie keinen Informationssicherheitsbeauftragten ein, so kann er weder die gewohnten Abläufe stören noch Folgekosten verursachen.
2. Wenn Sie es nicht völlig verhindern können, wählen Sie eine inkompetente, überforderte Person aus, die möglichst frei von Empathie und Verantwortungsbewusstsein ist.
3. Etablieren Sie möglichst mehrere Hierarchieebenen zwischen Behördenleitung und ISB.
4. Vermeiden Sie den Kontakt der Leitung mit dem ISB.
5. Geben Sie Ihrem ISB weder Rechte noch Ressourcen.
6. Weisen Sie dem ISB max. 10% der Arbeitszeit für die Wahrnehmung der ISB-Tätigkeit zu.
7. Sollte Ihr 10%-ISB aktiv werden und bewährte Abläufe stören, ist die Belastung der anderen 90% des Arbeitszeitanteils zu erhöhen, bis wieder Ruhe einkehrt.
8. Qualifizierung ist überbewertet. Sie kostet Zeit und Geld und es ist nicht auszuschließen, dass der ISB vom Lehrgang irgendwelche Ideen mitbringt.
9. Jeder Kontakt des ISB mit anderen ISB ist unbedingt zu verhindern. Das gilt insbesondere für das IT-SiBe-Forum! (http://info.it-sibe-forum.de/)

</ironie>

<ironie>

10 Goldene Regeln gegen lästige Informationssicherheitsbeauftragte (ISB)

1. Im Idealfall setzen Sie keinen Informationssicherheitsbeauftragten ein, so kann er weder die gewohnten Abläufe stören noch Folgekosten verursachen.
2. Wenn Sie es nicht völlig verhindern können, wählen Sie eine inkompetente, überforderte Person aus, die möglichst frei von Empathie und Verantwortungsbewusstsein ist.
3. Etablieren Sie möglichst mehrere Hierarchieebenen zwischen Behördenleitung und ISB.
4. Vermeiden Sie den Kontakt der Leitung mit dem ISB.
5. Geben Sie Ihrem ISB weder Rechte noch Ressourcen.
6. Weisen Sie dem ISB max. 10% der Arbeitszeit für die Wahrnehmung der ISB-Tätigkeit zu.
7. Sollte Ihr 10%-ISB aktiv werden und bewährte Abläufe stören, ist die Belastung der anderen 90% des Arbeitszeitanteils zu erhöhen, bis wieder Ruhe einkehrt.
8. Qualifizierung ist überbewertet. Sie kostet Zeit und Geld und es ist nicht auszuschließen, dass der ISB vom Lehrgang irgendwelche Ideen mitbringt.
9. Jeder Kontakt des ISB mit anderen ISB ist unbedingt zu verhindern. Das gilt insbesondere für das IT-SiBe-Forum! (http://info.it-sibe-forum.de/)
10. Lassen Sie sich nicht durch ängstliches Awareness-Gerede dieser paranoiden Looser verunsichern. Sie selbst haben die ultimativen Erfahrung im Umgang mit Risiken und die Nerds der IT-Abteilung werden schon dafür sorgen, dass - wie immer - nichts passiert.

</ironie>

<ironie>

10 Goldene Regeln gegen lästige Informationssicherheitsbeauftragte (ISB)

1. Im Idealfall setzen Sie keinen Informationssicherheitsbeauftragten ein, so kann er weder die gewohnten Abläufe stören noch Folgekosten verursachen.
2. Wenn Sie es nicht völlig verhindern können, wählen Sie eine inkompetente, überforderte Person aus, die möglichst frei von Empathie und Verantwortungsbewusstsein ist.
3. Etablieren Sie möglichst mehrere Hierarchieebenen zwischen Behördenleitung und ISB.
4. Vermeiden Sie den Kontakt der Leitung mit dem ISB.
5. Geben Sie Ihrem ISB weder Rechte noch Ressourcen.
6. Weisen Sie dem ISB max. 10% der Arbeitszeit für die Wahrnehmung der ISB-Tätigkeit zu.
7. Sollte Ihr 10%-ISB aktiv werden und bewährte Abläufe stören, ist die Belastung der anderen 90% des Arbeitszeitanteils zu erhöhen, bis wieder Ruhe einkehrt.
8. Qualifizierung ist überbewertet. Sie kostet Zeit und Geld und es ist nicht auszuschließen, dass der ISB vom Lehrgang irgendwelche Ideen mitbringt.
9. Jeder Kontakt des ISB mit anderen ISB ist unbedingt zu verhindern. Das gilt insbesondere für das IT-SiBe-Forum! (http://info.it-sibe-forum.de/)
10. Lassen Sie sich nicht durch ängstliches Awareness-Gerede dieser paranoiden Looser verunsichern. Sie selbst haben die ultimativen Erfahrung im Umgang mit Risiken und die Nerds der IT-Abteilung werden schon dafür sorgen, dass - wie immer - nichts passiert.

Ich wünsche Ihnen viel Glück! Sie werden es brauchen.

</ironie>

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

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