Kommunale IT-UNION

Wie können die Kommunen den Anforderungen an

Informationssicherheit

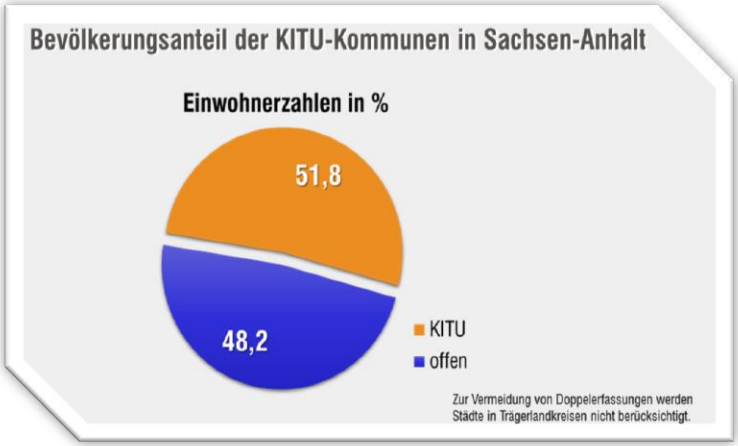
gerecht werden?

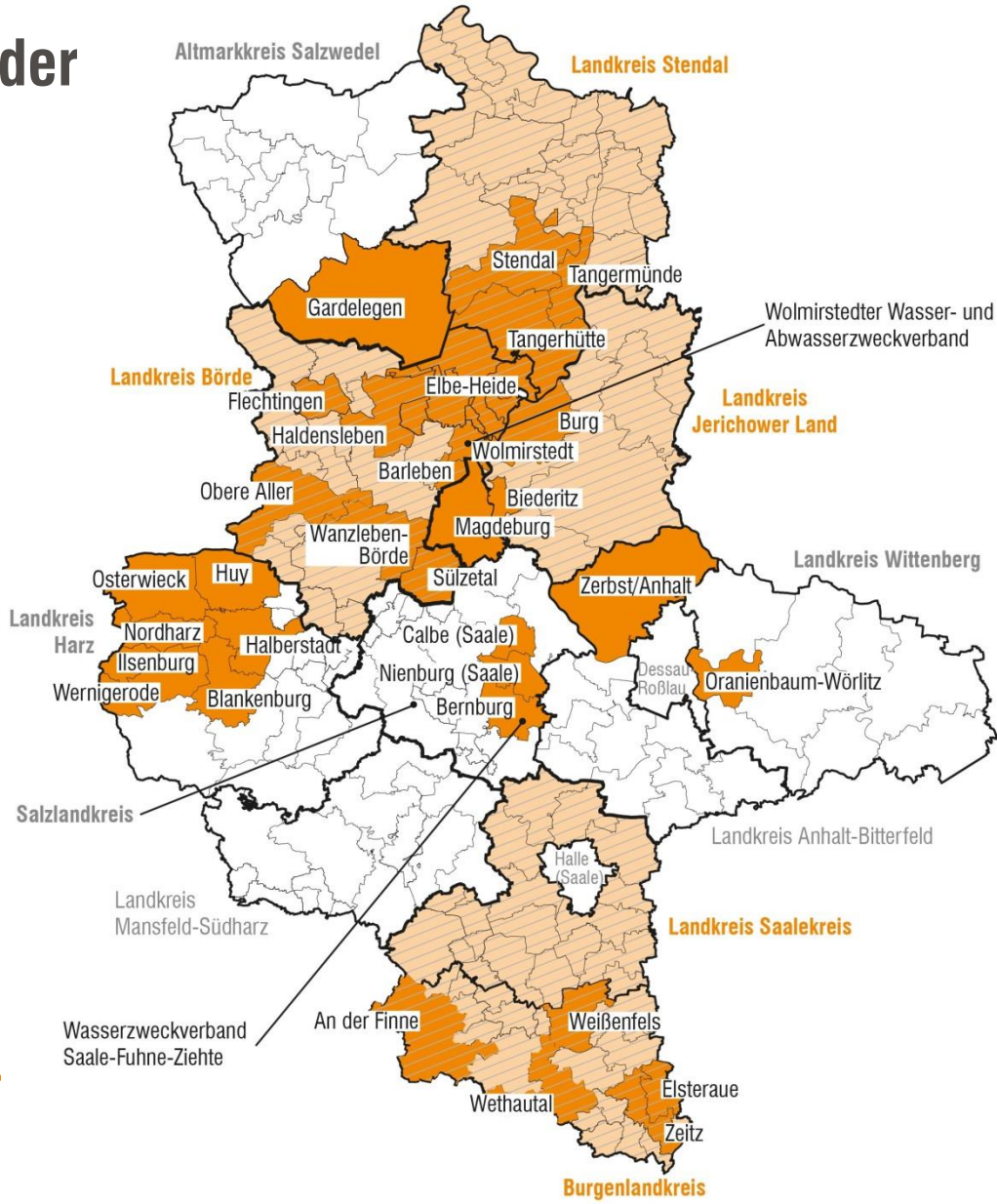
Dr. Michael Wandersleb
Vorstandsvorsitzender KITU
Peter Nehl
Bereichsleiter Technik KID

KITU: Eine starke Gemeinschaft

Aktueller Stand KITU-Mitglieder

5 Landkreise
32 Städte/Gemeinden/VG
2 Zweckverbände
1 Betriebsgesellschaft KID

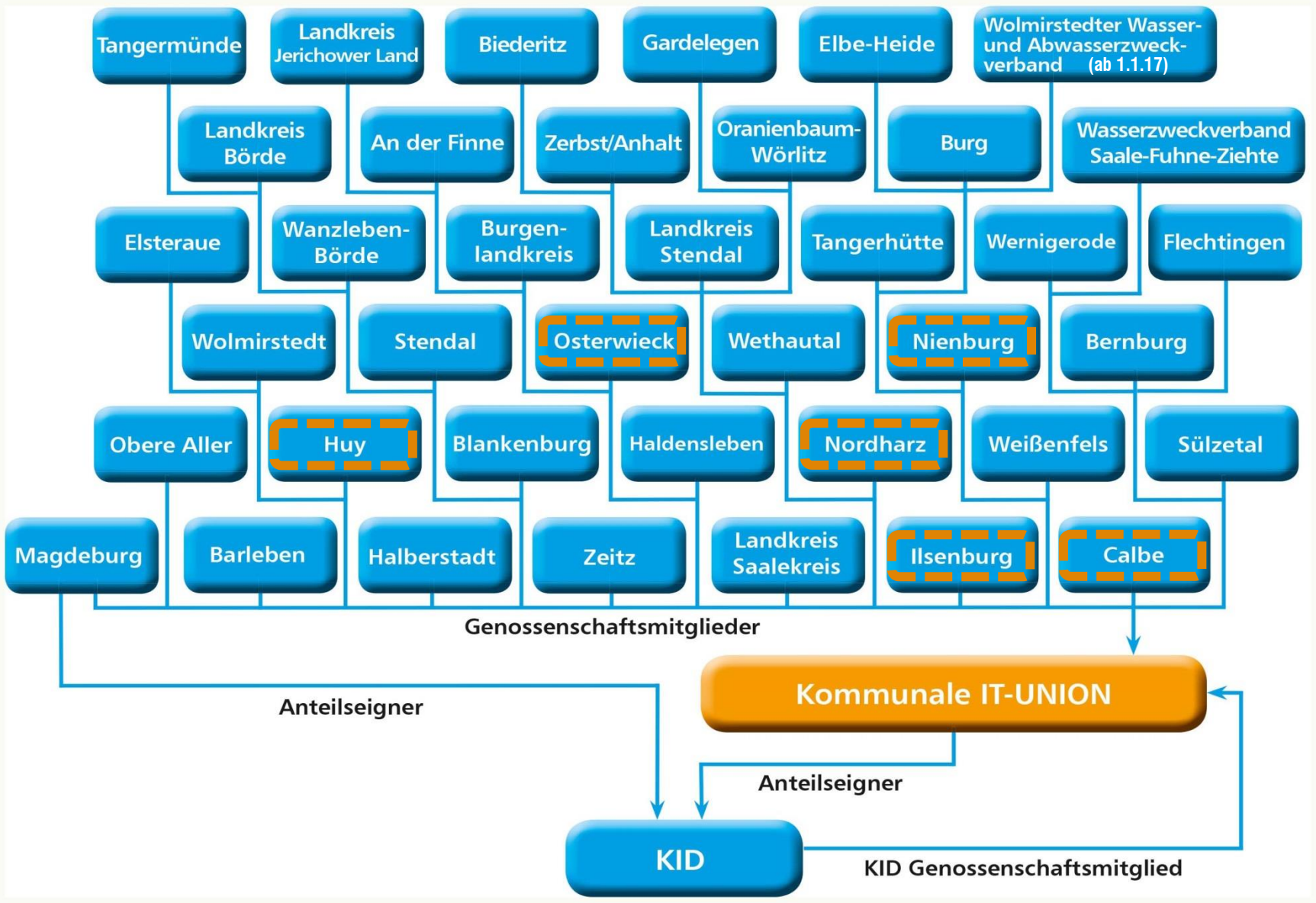




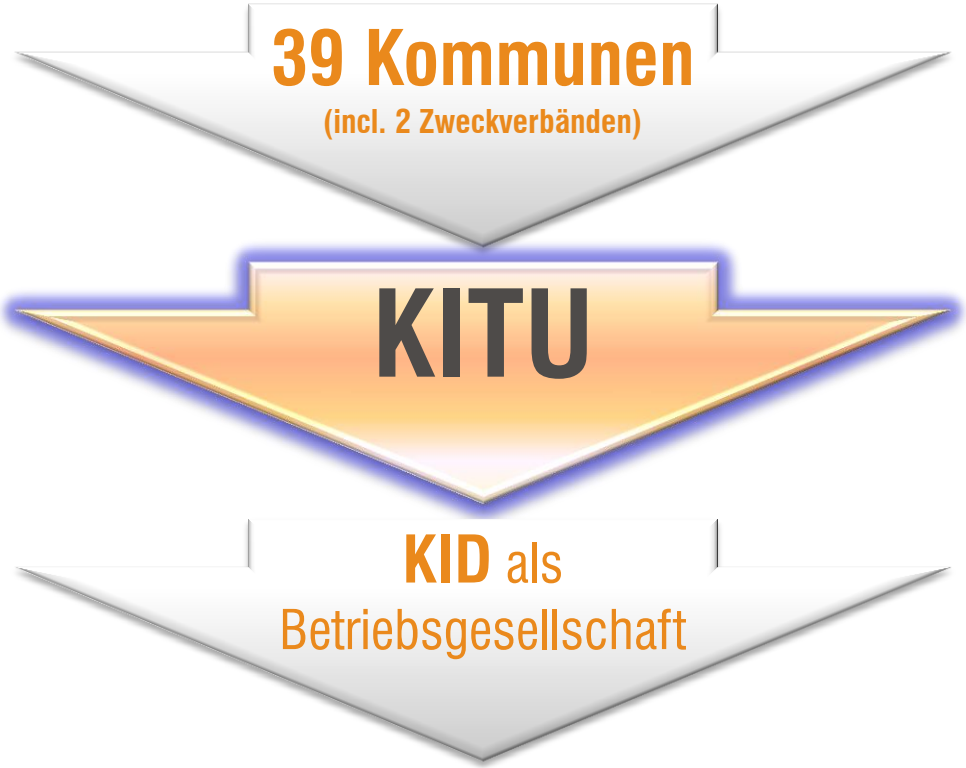
Beteiligungsstruktur

Tangermünde
Landkreis Jerichower Land
Biederitz
Gardelegen
Elbe-Heide
Wolmirstedter Wasser- und Abwasserzweck-verband (ab 1.1.17)
Landkreis Börde
An der Finne
Zerbst/Anhalt
Oranienbaum-Wörlitz
Burg
Wasserzweckverband Saale-Fuhne-Ziehte
Elsteraue
Wanzleben-Börde
Burgen-landkreis
Landkreis Stendal
Tangerhütte
Wernigerode
Flechtingen
Wolmirstedt
Stendal
Osterwieck
Wethautal
Nienburg
Bernburg
Obere Aller
Huy
Blankenburg
Haldensleben
Nordharz
Weißenfels
Sülzetal
Magdeburg
Barleben
Halberstadt
Zeitz
Landkreis Saalekreis
Ilsenburg
Calbe
Genossenschaftsmitglieder
Kommunale IT-UNION
Anteilseigner
Anteilseigner
KID
KID Genossenschaftsmitglied

Beteiligungsstruktur



KITU – eine starke Gemeinschaft aus ganz Sachsen-Anhalt



Aufsichtsrat

- Klaus Zimmermann, Bürgermeister **Magdeburg**, Vorsitzender
- Kerstin Beckmann, Bürgermeisterin **Wethautal**
- Michael Hoffmann, AR-V KID, **Magdeburg**
- Axel Kleefeldt, stv. Oberbürgermeister **Stendal**
- Dennis Loeffke, Bürgermeister **Ilsenburg**
- Robby Risch, Oberbürgermeister **Weißenfels**
- Ingeborg Wagenführ, Bürgermeisterin **Osterwieck**

Vorstand

- Dr. Michael Wandersleb, Vorsitzender, **KID**
- Marcel Pessel, **Barleben**

Vorteile der Genossenschaft

- Einfacher Ein- und Austritt
- Beibehaltung der Entscheidungsfreiheit jedes Mitglieds
- Klare vergaberechtliche Strukturen
- Keine Risiken durch Nachschusspflichten
- Einheitlicher und konstanter Wert des Geschäftsanteils bei Ein- und Austritt (kein Unternehmenswertrisiko)
- Größenunabhängig jedes Mitglied 1 Stimme.

KITU-Leistungen können die Informationssicherheit erhöhen

Erfahrungsaustausch	• Arbeitskreise • Plattformen, bilateral
Beratung	• z.B. Ist-Analyse, Quick-Check
Einkaufsgemeinschaft	• Ausschreibungskompetenz • Skaleneffekte
Einführung und Betreuung Fachverfahren	• z.B. Finanzverfahren • z.B. Dokumentenmanagementsystem
Temporäre Unterstützung	• Projektleitung • Bei gr. Veränderungen (z.B. IT-Infrastruktur)
Betriebsführung vor Ort	• Skalierbar, modular • Bandbreitenabhängig
RZ-Hosting Fachverfahren	• z.T. Software-induziert • z.B. AutiSta, MESO⇨VOIS
RZ-Betrieb	• Höchste Evolutionsstufe • Stand der Technik

Informationssicherheit

Kommunale IT-UNION

Das Trojanische Pferd ist nicht allein in die Stadt gelaufen…

…Schwachstelle Mensch:
freundlich, neugierig, hilfsbereit

[Quelle: Wikimedia]

Kommunale IT-UNION

Beispiel: Datenschutz – 10 typische Fehler …

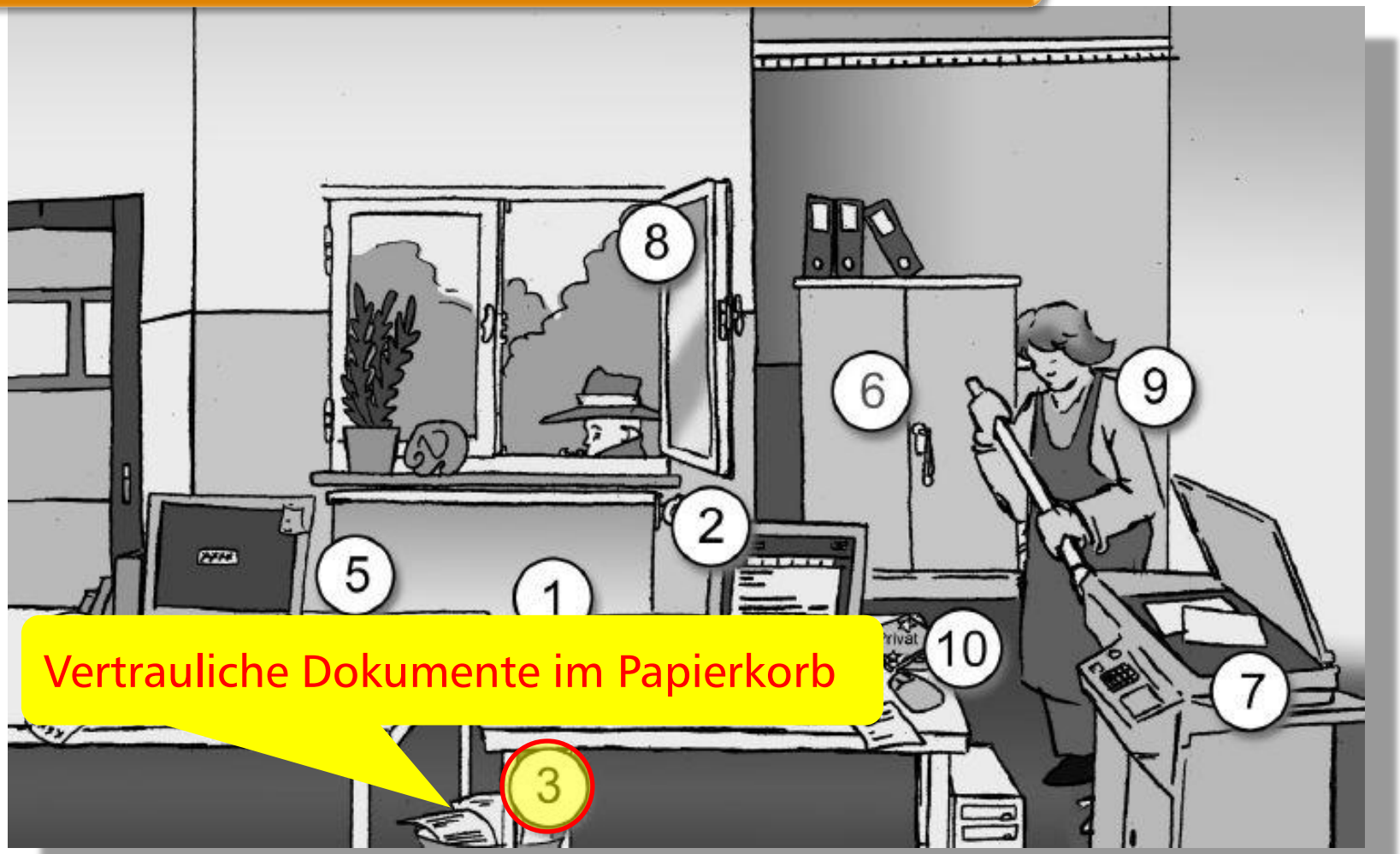
[Quelle: Sabina Siefert UMGT]

Kommunale IT-UNION

Beispiel: Datenschutz – 10 typische Fehler …

[Quelle: Sabina Siefert UMGT]

Beispiel: Datenschutz – 10 typische Fehler …



[Quelle: Sabina Siefert UMGT]

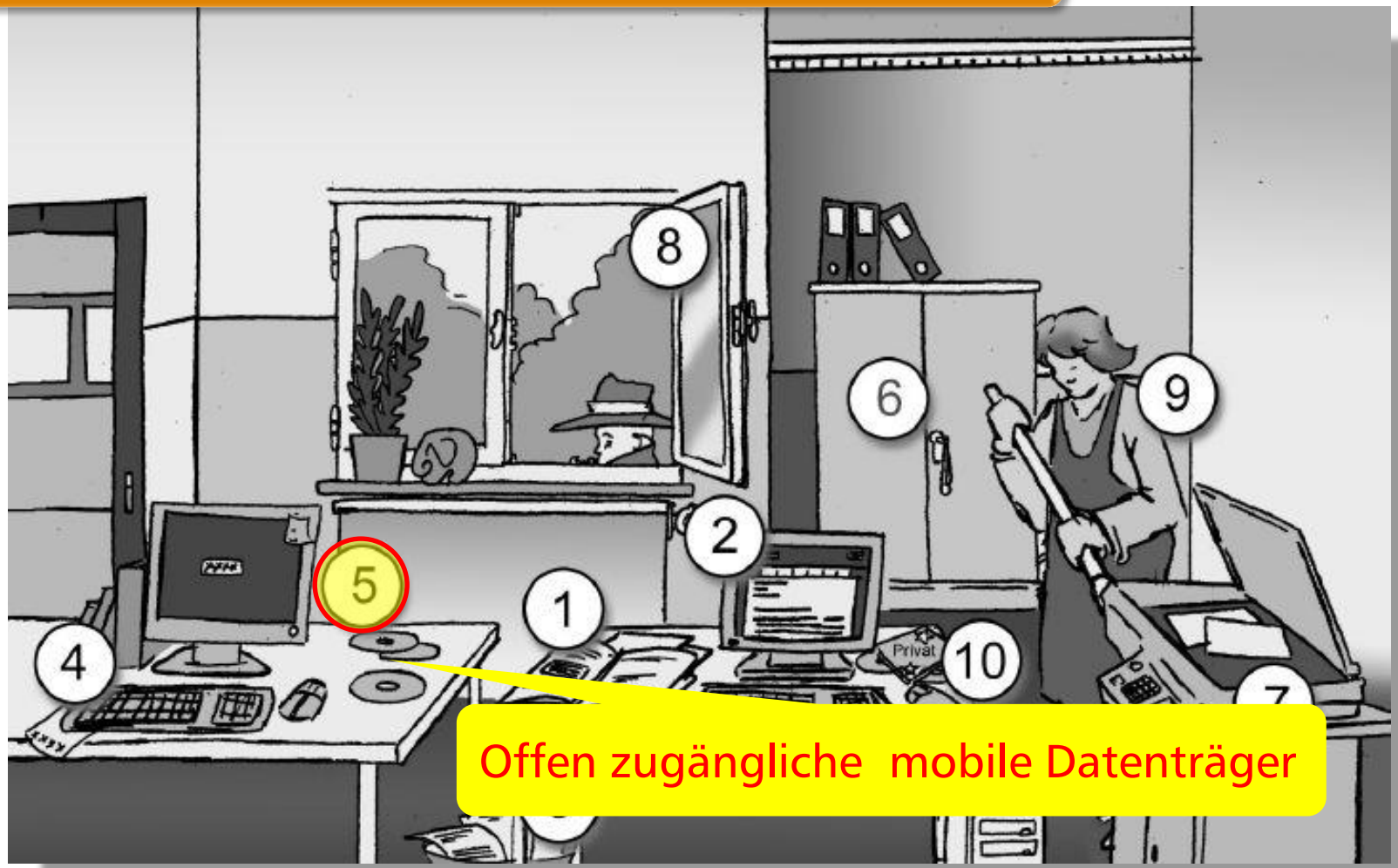
Kommunale IT-UNION

Beispiel: Datenschutz – 10 typische Fehler …

[Quelle: Sabina Siefert UMGT]

Kommunale IT-UNION

Beispiel: Datenschutz – 10 typische Fehler …



[Quelle: Sabina Siefert UMGT]

Kommunale IT-UNION

Beispiel: Datenschutz – 10 typische Fehler …

[Quelle: Sabina Siefert UMGT]

Beispiel: Datenschutz – 10 typische Fehler …

[Quelle: Sabina Siefert UMGT]

Kommunale IT-UNION

Beispiel: Datenschutz – 10 typische Fehler …

[Quelle: Sabina Siefert UMGT]

Kommunale IT-UNION

Beispiel: Datenschutz – 10 typische Fehler …

[Quelle: Sabina Siefert UMGT]

Beispiel: Datenschutz – 10 typische Fehler …

[Quelle: Sabina Siefert UMGT]

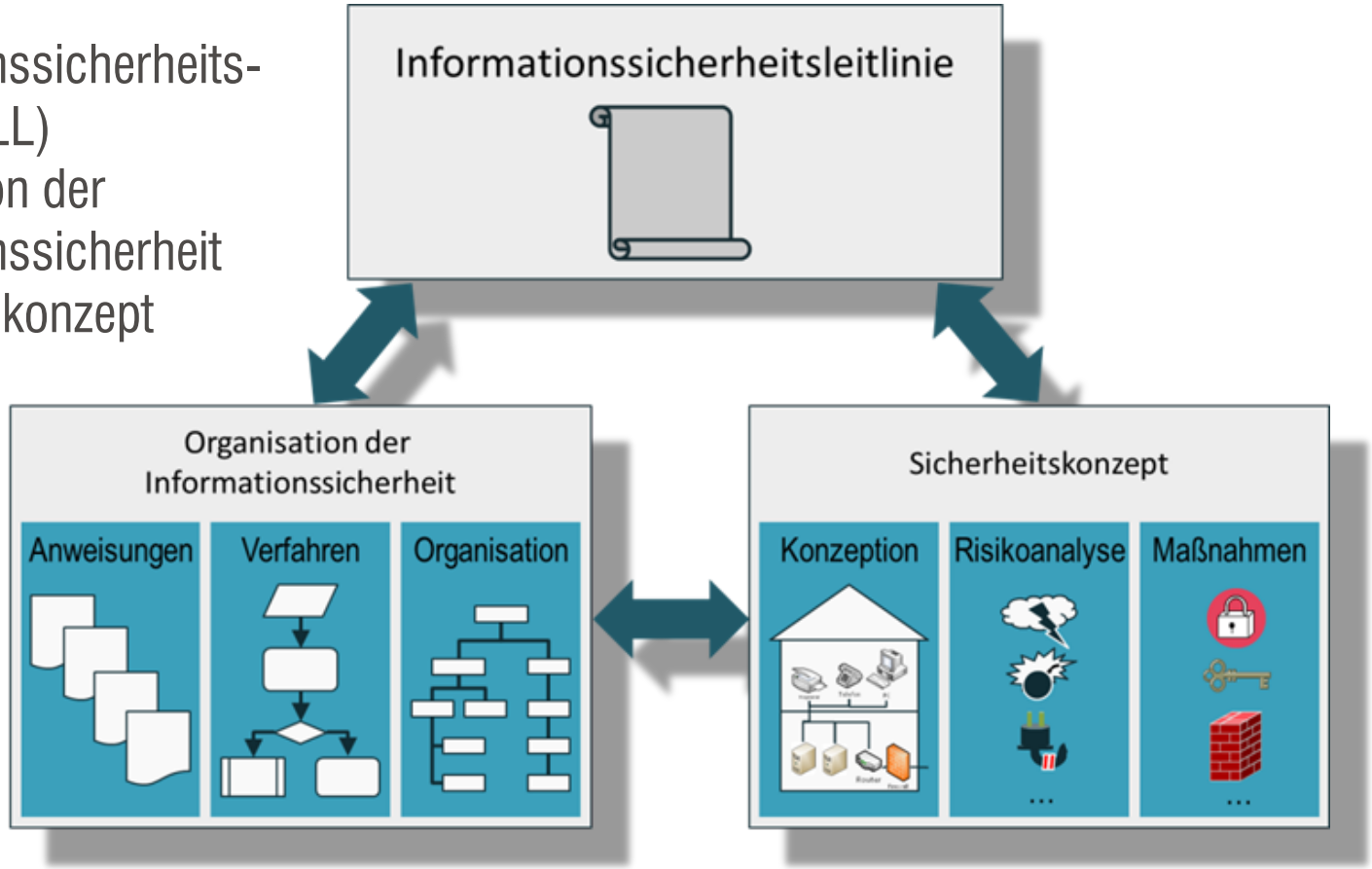
Begriffsbestimmung:
Datenschutz=IT-Sicherheit=Informationssicherheit?

- **Datenschutz** und **IT-Sicherheit** nur Teilmengen von **Informationssicherheit.**
- Informationssicherheit: Sicherung **der Verfügbarkeit, Vertraulichkeit und Integrität** von Informationen, Daten und Systemen.
- Informationssicherheit umfasst stets auch physische Sicherheit, Personal-management, Rechtsschutz, Organisation, Prozesse usw. .
- Ziel: Etablierung eines **Informationssicherheitsmanagementsystems** (ISMS) zur Risikominimierung.
- Anwendung der **Leitlinie für Informationssicherheit** wird den Kommunen seitens IT-Planungsrat empfohlen.

Informationssicherheit: Regelwerk

3 Säulen

- Informationssicherheits-leitlinie (ISLL)
- Organisation der Informationssicherheit
- Sicherheitskonzept



Informationssicherheitsleitlinie (1)

Inhalte/Thesen

- **Ziel**:
  Aufbau eines kommunalen Informationssicherheitsmanagementsystems (ISMS) als **Prozess** auf Basis einer Informationssicherheitsleitlinie (ISLL).

- Berücksichtigung kommunaler Realitäten und Besonderheiten der Gebietskörperschaften; keine pauschalen Empfehlungen.

- Hilfestellung und Mustertexte zur Erarbeitung ISLL.

- **100 % Sicherheit? → gibt es nicht!**

Informationssicherheitsleitlinie (2)

Notwendig

- **Bekenntnis der Verwaltungsleitung** zu Informationssicherheit.
- **Bestandsaufnahme und –analyse** als Voraussetzung für ein ISMS.
- Einbeziehung **aller Beschäftigten** der Verwaltung in den Sicherheits-prozess.

Der entscheidende Faktor: der Mensch

‚. . .
Mit der zunehmenden Verbreitung von Informationstechnik rückt auch der Mensch immer mehr in den Mittelpunkt von IT-Sicherheitsfragen. Einerseits ist er für die IT- und Informations-sicherheit verantwortlich, ***andererseits ist er häufig das schwächste Glied in der Verteidigungskette****.*
Neben technischen und organisatorischen Maß-nahmen sind Sensibilisierung, Awareness sowie ein gesundes Maß an Misstrauen aufseiten der Anwender für die IT-Sicherheit unerlässlich.
. . .‘

Quelle: BSI-Lagebericht zur IT-Sicherheit 2015, S. 14

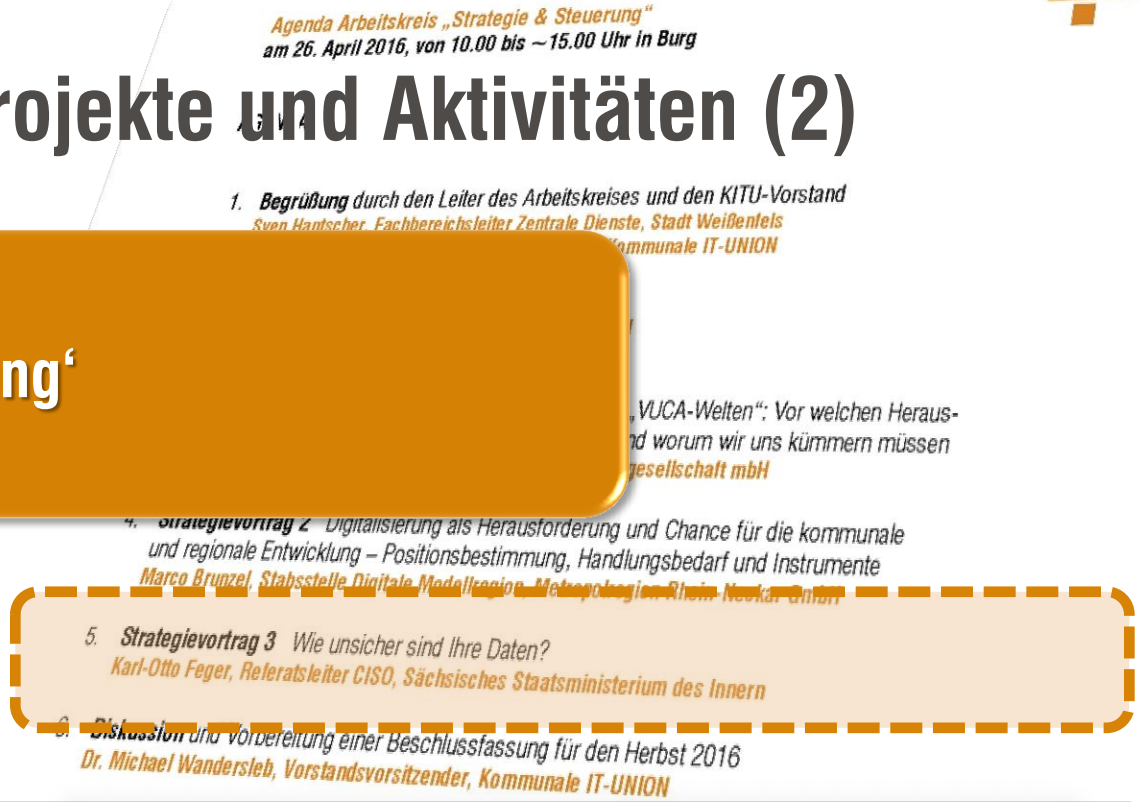
Ausgewählte Projekte und Aktivitäten (1)

KID-Mitwirkung in der Arbeitsgruppe der kommunalen Spitzenverbände

‚Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen‘

Ausgewählte Projekte und Aktivitäten (2)

KITU-Arbeitskreis
‚Strategie & Steuerung'
26.04.2016, Burg



Agenda Arbeitskreis „Strategie & Steuerung"
am 26. April 2016, von 10.00 bis ~15.00 Uhr in Burg

1. **Begrüßung** durch den Leiter des Arbeitskreises und den KITU-Vorstand
   Sven Hantscher, Fachbereichsleiter Zentrale Dienste, Stadt Weißenfels
   Kommunale IT-UNION

„VUCA-Welten": Vor welchen Heraus-
und worum wir uns kümmern müssen
gesellschaft mbH

4. **Strategievortrag 2** Digitalisierung als Herausforderung und Chance für die kommunale und regionale Entwicklung – Positionsbestimmung, Handlungsbedarf und Instrumente
   Marco Brunzel, Stabsstelle Digitale Modellregion Metropolregion Rhein-Neckar GmbH

5. **Strategievortrag 3** Wie unsicher sind Ihre Daten?
   Karl-Otto Feger, Referatsleiter CISO, Sächsisches Staatsministerium des Innern

6. **Diskussion** und Vorbereitung einer Beschlussfassung für den Herbst 2016
   Dr. Michael Wandersleb, Vorstandsvorsitzender, Kommunale IT-UNION

Postdienstleistung

10. **Vorstellung des KITU-Leitfadens** „Intranet-Portale in Kommunen"
    Mitglieder der KITU-Arbeitsgruppe „Intranet in Kommunen"

u.a. …

Hauptverwaltungsbeamte sind direkt für die Informationssicherheit verantwortlich….'

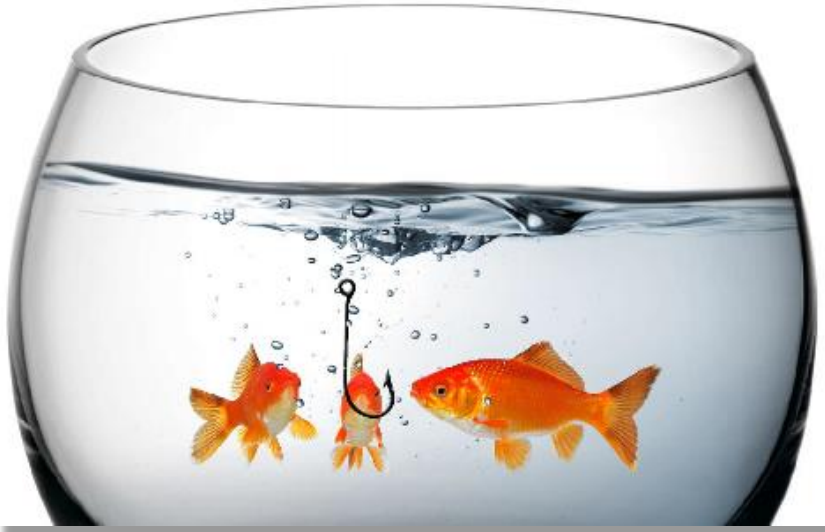
Karl-Otto Feger, Referatsleiter CISO

Sächsisches Staatsministerium des Innern

Ausgewählte Projekte und Aktivitäten (3)

KITU-Workshop
‚IT-Sicherheit in der kommunalen Verwaltung‘
06.07.2016, Magdeburg

.2016 | KID Magdeburg



procilon GROUP

T.I.S.P. TeleTrusT Information Security Professional

ISIS 12

Allianz für Cyber-Sicherheit

Und was geht das uns als Verwaltung an?

…Das Thema betrifft uns als Kommunalverwaltung gar nicht!

…Was wollen ‚die' denn mit unseren Daten?

…Ist doch eher was für die Wirtschaft und Geheimdienste.

...Darum kümmert sich doch unsere IT – oder (etwa nicht)?!

…Ist keine kommunale Pflichtaufgabe, dafür gibts kein Geld!

…Wir sind froh, wenn unsere Computer funktionieren!

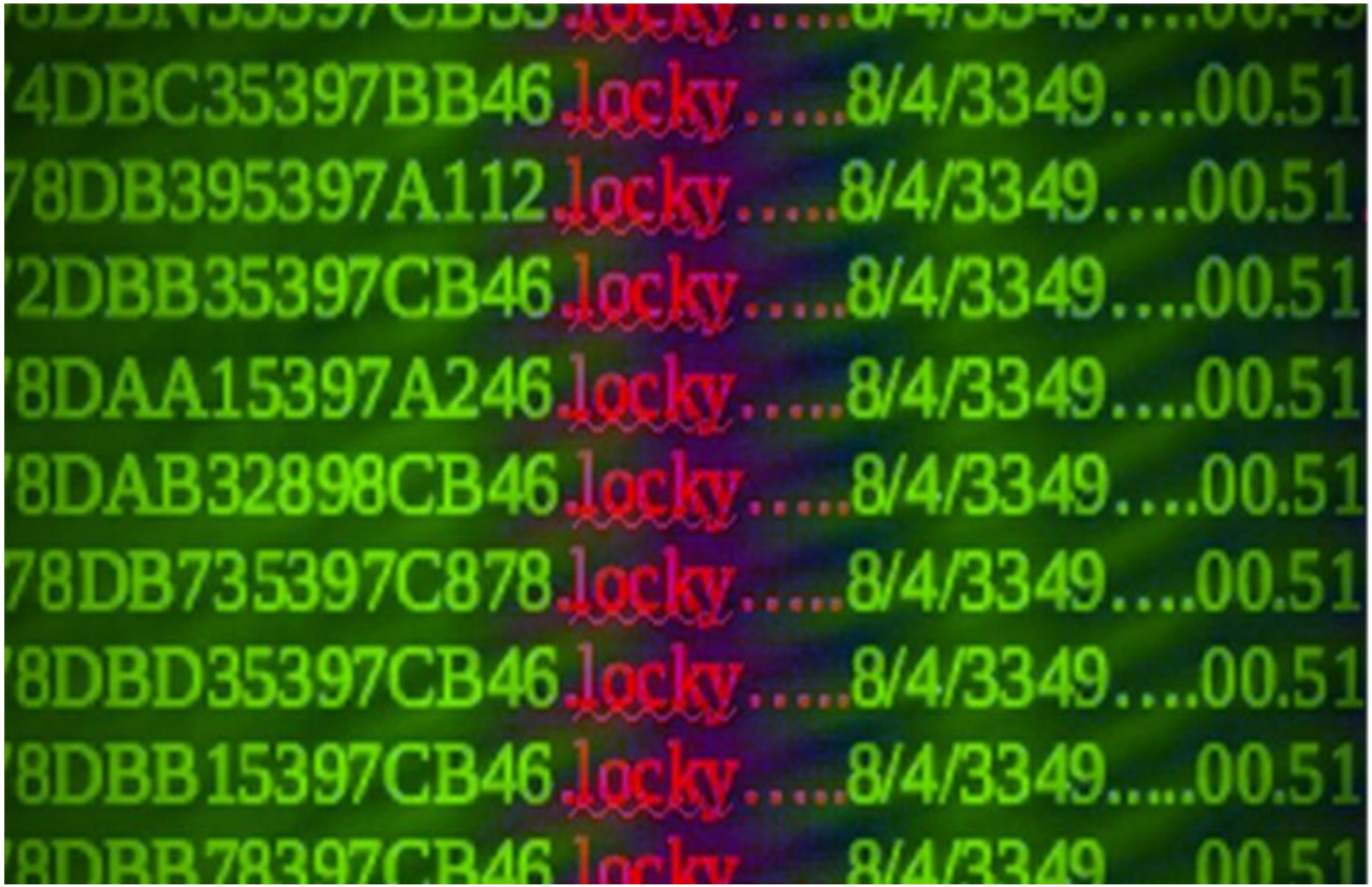
Kommunale IT-UNION

Alles zu abstrakt und theoretisch?

Kleiner Exkurs in die Realität…

Kennen Sie den?

Oder den?


4DBC35397BB46.locky.....8/4/3349....00.51
78DB395397A112.locky.....8/4/3349....00.51
72DBB35397CB46.locky.....8/4/3349....00.51
78DAA15397A246.locky.....8/4/3349....00.51
78DAB32898CB46.locky.....8/4/3349....00.51
78DB735397C878.locky.....8/4/3349....00.51
78DBD35397CB46.locky.....8/4/3349....00.51
78DBB15397CB46.locky.....8/4/3349....00.51

Nicht?!

Na dann: Herzlichen Glückwunsch!
… und weiterhin:
toi, toi, toi!

Praxis-Beispiele

Beispiel 1: Netz des Deutschen Bundestages (Parlakom)

- Angriffsstart: **Ende 2014/Anfang 2015.**
- Kaperung eines(!) einzelnen Abgeordneten-PC durch gewöhnliche Malware.
- **Folgen:**
  - Zentrale IT-Systeme kompromittiert; gesamtes Bundestags-Netz infiziert.
  - Angreifer zwischenzeitlich mit weitreichenden Zugriffsmöglichkeiten.
  - Vermutlich mehrmonatiger Datenabfluss im großen Stil.
- Entdeckung des Angriffs erst 4(!) Monate später (**Anfang Mai 2015**).
- Mehrwöchige Reparaturversuche scheitern; Parlakom muss kplt. offline geschalten und erneuert werden.
- *‚Die IT-Systemtechnik ist wieder hergestellt.‘* **24. August 2015.**
- **Kosten:** keine Angaben…

Praxis-Beispiele

Beispiel 2: Gemeindeverwaltung Dettelbach bei Würzburg

- Angriff: **08. Februar 2016 – 09:40 Uhr,** Erkennung um 10:30 Uhr.
- Aktivierung des eingeschleusten Trojaners Tesla-Crypt durch gewöhnliche Malware (eine Mail mit infiziertem Anhang).
- **Folgen**: Datenverschlüsselung der zentralen Serversysteme mit Lösegeldforderung.

  Weitreichender Totalausfall des Verwaltungssystems nach ‚Fehlentscheidungen bei der Rücksicherung'.
- **Kosten**: 1,3 BitCoins Lösegeldzahlung (ca. **490 EUR**) für die nur teilweise Entschlüsselung der Daten.

  100.000 EUR für Datenrettung durch involvierte IT-Firmen.

  nicht näher spezifizierte Kosten für zusätzliche technische Maßnahmen.

  nicht näher spezifizierte Kosten für städtische Mitarbeiter.

Praxis-Beispiele

Beispiel 3: Stadtverwaltung Rheine/Münsterland

- Angriff: **01.März 2016**.
- Aktivierung des eingeschleusten Trojaners Tesla-Crypt3 über infizierte Internetseite (einmaliges Anklicken).
- **Folgen**: Datenverschlüsselung eines kplt. PC und mehrerer Dateien auf Servern mit Lösegeldforderung.

  Mehrtägiger Totalausfall der Verwaltungs-IT für 500 MA.

  80% der PC erst nach 3 Tagen wieder online.
- *‚Die Folgen der Virus-Attacke auf das Computernetz der Stadtverwaltung in Rheine sind seit Freitagmittag weitgehend behoben.‘* **05. März 2016.**
- **Kosten**: ‚Die durch die Virus-Attacke angerichteten Schäden lassen sich noch nicht beziffern.‘

Diagnosebefund

Studie zur IT-Sicherheitssituation in der öffentlichen Verwaltung

‚Cyberangriffe und Datensicherheit in öffentlichen Netzwerken und Dateninfrastrukturen in Deutschland'

…nur **7%** der befragten IT-Experten der öffentlichen Verwaltung halten kleinere Kommunen für geschützt bzw. umfassend geschützt, bei mittleren Kommunen 15%, bei großen Kommunen 49%...

…Mitarbeiterschulungen zu Datenschutz und Datensicherheit nur bei **40%** der befragten öffentlichen Verwaltungen vorhanden oder vollständig vorhanden….

…bei knapp **50%** gibt es elektronische ID-Zugangskontrollen zur IT-Abteilung, physische Zugangskontrollen liegen bei 60%...

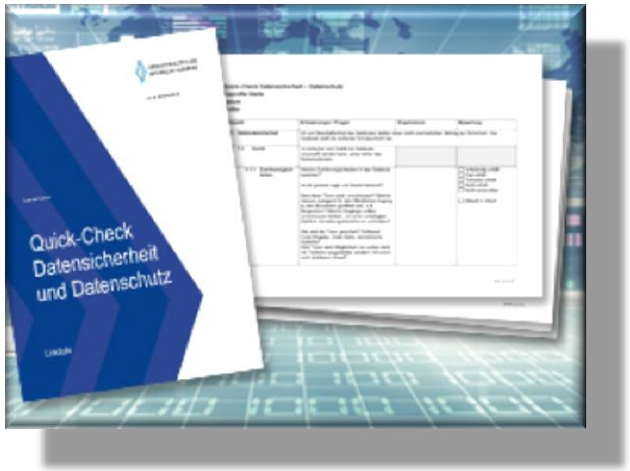
…client- und serverseitige Datenverschlüsselung bei etwa einem **1/4** (bei Server 23%, bei Client 29%) vorhanden bis vollständig vorhanden

…ein schwach ausgeprägtes Notfallmanagement bei knapp **1/3** der öffentlichen Verwaltungen(29%)

…mehr als **3/4** der IT-Experten der öffentlichen Verwaltung sehen einen Mangel an Ressourcenunterstützung im Bereich Datensicherheit durch ihre übergeordnete Behörde (77%) ….

Quellen: Deutsche Universität für Verwaltungswissenschaften in Speyer; eGovernment Computing, 2016

Und nun?



Quick-Check auf Basis ISIS12

Bestandsaufnahme und –analyse Informationssicherheit

ISIS–was?

ISIS12 = Vorgehensmodell in 12 Schritten.

- Aufbau und Betrieb eines kommunalen ISMS.
- Basis:
  BSI IT-Grundschutzkatalog + ISO/IEC 27001.
- Klares Regelwerk unter Berücksichtigung der Verantwortlichkeiten.
- Flankierung technischer durch organisatorische Maßnahmen.

ISMS-Standards (Auswahl)

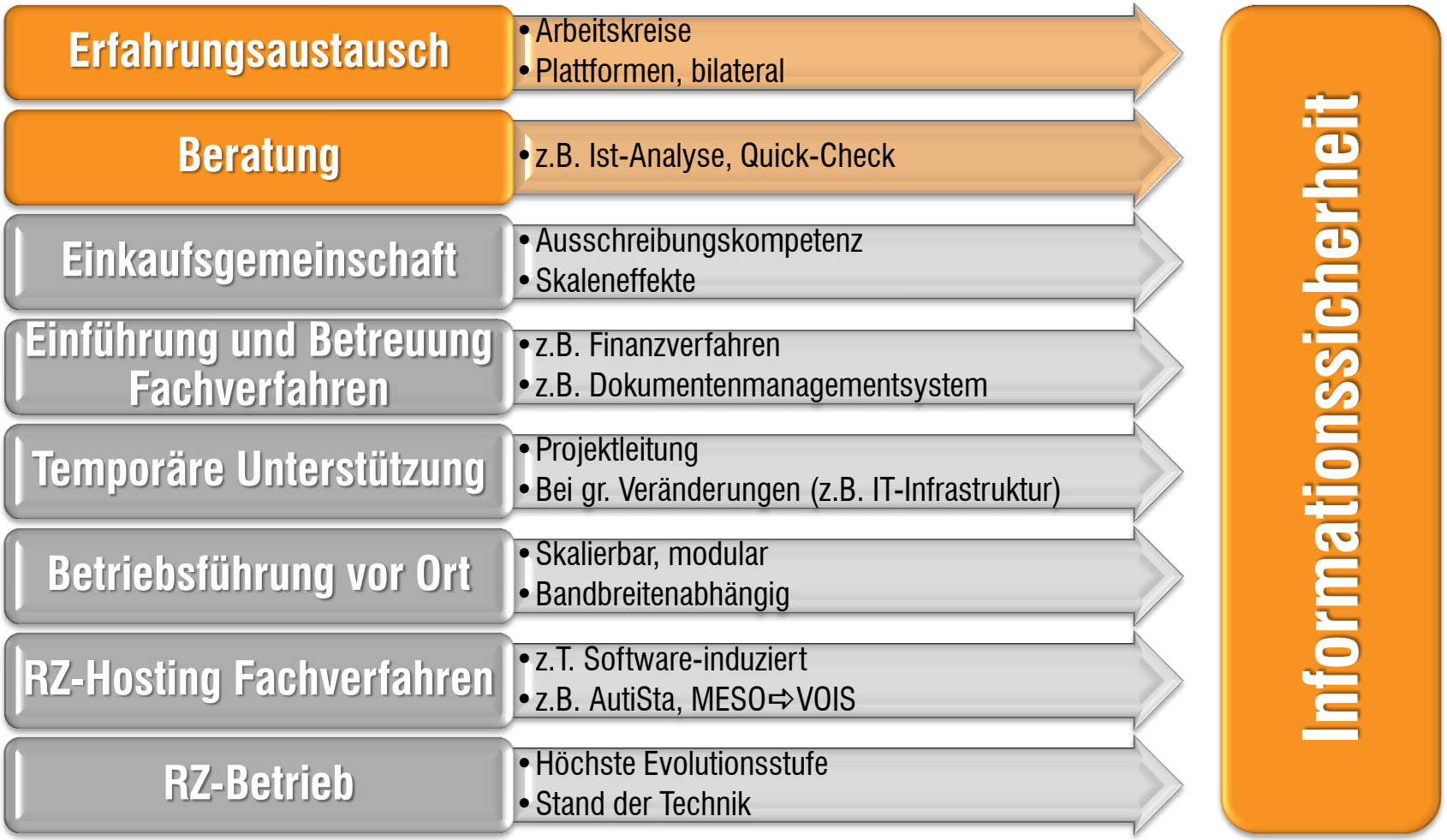
Kriterien	ISIS12	ISO 27000-Reihe	BSI IT-Grundschutz
Herausgeber	Netzwerk Informationssicherheit für den Mittelstand	International Standards Organisation	Bundesamt für Sicherheit in der Informationstechnik
Zielgruppe	Kleine und mittlere Unternehmen	Organisationen jeder Größenordnungen	Organisationen jeder Größenordnungen und öffentliche Verwaltung
Dokumentation	**ca. 170 Seiten**	**ca. 400 Seiten**	**ca. 4.500 Seiten**
Detailierung	Mittel	Minimalistisch abstrakt	Maximal detailliert
Aufbau	Selektierte Bausteine + Maßnahmen	Maßnahmenempfehlungen	Umfassende Bausteine, Gefährdungen + Maßnahmen
Maßnahmenkatalog	**ca. 400 Maßnahmen**	**ca. 150 Maßnahmen**	**ca. 1.100 Maßnahmen**
Risikoanalyse	indirekt	grundsätzlich	ergänzend
Umsetzung	konkret formulierte Maßnahmen umsetzen	allgemeingültig formulierte Maßnahmen umsetzen	konkret formulierte Maßnahmen umsetzen
Mögliche Zertifizierung	DQS-Zertifizierung	ISO-Zertifizierung	ISO-Zertifizierung nach IT-Grundschutz

Methodik und Ergebnisse

- **Bestandsaufnahme und –analyse** Informationssicherheit als Voraussetzung für ein ISMS.
- Grundlage: ISIS12-Checkliste (‚Quick-Check Datensicherheit und Datenschutz' der Innovationsstiftung Bayerische Kommune).
- Transparentes Vorgehen anhand einer Liste mit Schwerpunkten (z.B. Gebäudesicherheit, Zugriffsschutz).
- Status der wichtigsten sicherheitsrelevanten Bereiche.
- Erstbewertung des Schutzniveaus auf Basis vergleichbarer Kriterien.
- Identifikation und Bewertung von Schwachstellen.
- Empfehlung und Priorisierung von Maßnahmen.
- Beratung zur Bewältigung von Sicherheitsrisiken.

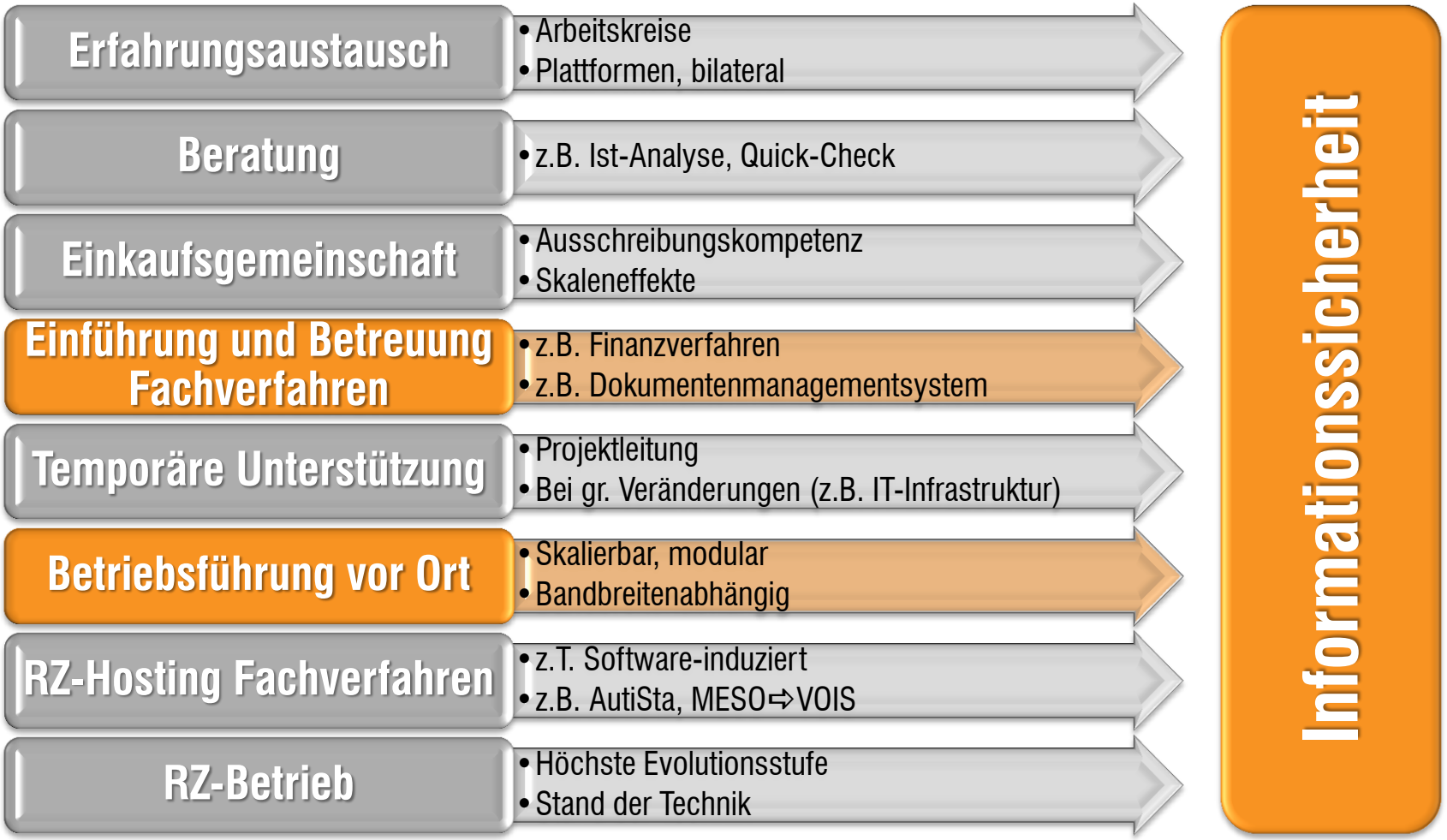
KITU-Leistungen

Entscheidender Beitrag zur Informationssicherheit



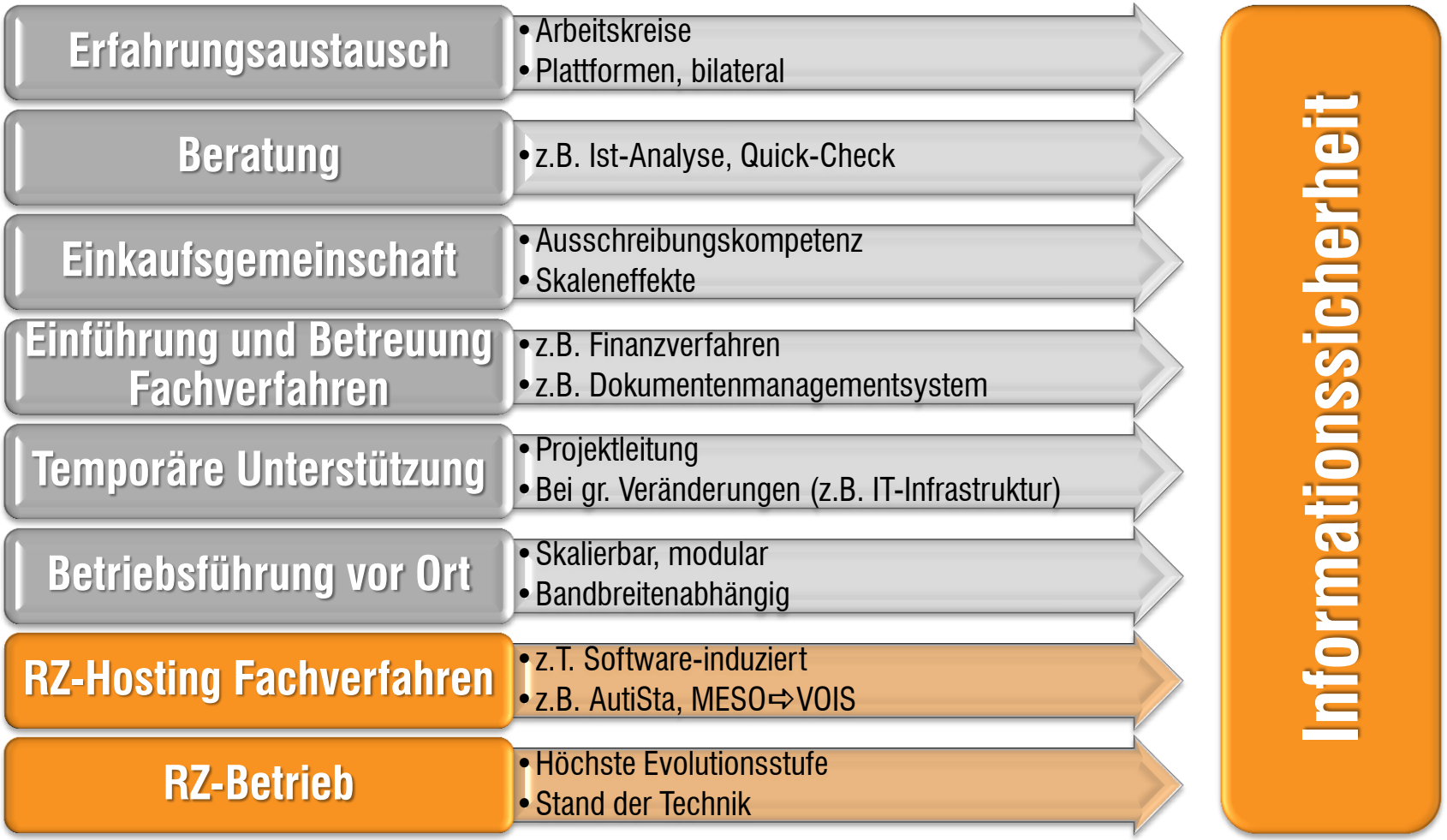
KITU-Leistungen

Entscheidender Beitrag zur Informationssicherheit



KITU-Leistungen

Entscheidender Beitrag zur Informationssicherheit



Herzlichen Dank für Ihre Aufmerksamkeit.

Dr. Michael Wandersleb
Vorstandsvorsitzender

Kommunale IT-UNION eG (KITU)
Alter Markt 15
39104 Magdeburg

Telefon 0391 2 44 64 -440
E-Mail wandersleb@kitu-genossenschaft.de

Peter Nehl
Bereichsleiter TECHNIK

Kommunale Informationsdienste Magdeburg GmbH (KID)
Alter Markt 15
39104 Magdeburg

Telefon 0391 2 44 64 -125
E-Mail peter.nehl@kid-magdeburg.de