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

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting

Berlin, 14. - 15.11.2017

Sensibilität für Informationssicherheit:
Wie kommen wir vom "ich muss" zum "ich will" ?

Dr. Carsten Gottert

Geschäftsführer etomer GmbH

systemhaus etomer

SECUTAIN

Agenda.

1. Regulatorik und Regelwerke.
2. Informationssicherheit.
3. Sinnbildung.
4. Awareness.

Agenda.

1 **Regulatorik und Regelwerke.**

Warum ist das so schwer?

2 Informationssicherheit.

3 Sinnbildung.

4 Awareness.

Kennen Sie das? Treiber für Regelwerke.

Gesetzliche Regelungen wie die EU-DSGV oder das ITSIG.

Branchenspezifika.

MiFID II / MiFIR

Besicherung OTC-Derivate

BCBS 239 Risk Data Aggregation

Fundamental Review of the Trading Book (FRTB)

EMIR

(…)

Zertifizierungen & Best Practices.

ISO 9001

ISO 14001

ISO 27001

ISO 45001

IT Grundschutz

T.I.S.P.

(…)

Vertragliche Regelungen.

Leiharbeitnehmer

Externe / Freelancer

Subunternehmerschaften

Outtasking

Outsourcing

(…)

Codes of Conduct.

Typische Regelmechanismen.

Typische Regelmechanismen.

Warum haben Organisationen Regeln?
Funktionen organisationaler Regelsysteme:

- bündeln Aufgaben und formulieren Erwartungen
- helfen Organisationen, Risiken für Mitglieder handhabbar zu machen
- liefern den Organisationsmitgliedern Entscheidungsprämissen
  - bieten damit Mitgliedern Sicherheit auf der einen Seite
  - nehmen dabei Mitgliedern Freiraum auf der anderen Seite
  - reduzieren die gesamte Eigenkomplexität des Systems
- sind nicht flexibel veränderbar, erfordern die Änderung der sogenannten Meta-Regeln

Das Problem mit diesen Regeln (1)

1. Regeln haben so ihre Schwächen!

- Unabsichtliches unterschiedliches Auslegen (Latenz)
- Umgehen, Beugen, nur auf dem Papier leben (Anomalien)
- Bewusster Regelbruch, um dem vermeintlichen Wohl der Organisation zu dienen (Brauchbare Illegalität)

- Senken der eigenen Komplexität und damit der Fähigkeit, erhöhter Komplexität von Inhalt und Umwelt zu begegnen
- Anschlussfähigkeit und Orientierungshilfe fehlen, wenn unbekannte Situationen nicht durch regelkonformes Handeln gelöst werden können

Das Problem mit diesen Regeln (2)

2. Regeln wirken in unbekannten Situationen nicht.

„There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don‘t know we don‘t know."

(Rumsfeld, 2002)

Risiko
Eintrittswahrscheinlichkeit bekannt oder schätzbar

Unsicherheit
Eintrittswahrscheinlichkeit unbekannt / unerwartet

Resilienz
Fähigkeit, unter (un)erwarteten Umständen fortbestehen zu können

Was braucht Resilienz?

Organisationale Beidhändigkeit.

EXPLOITATION

Proaktive Robustheit

Nutzbarmachung des Bestehenden / Standards

Verbesserung bestehender Fähigkeiten

Vorbeugung

REGELN !

EXPLORATION

Reaktive Agilität

Entdeckung von Neuem / Neugier

Erlernen neuer Fähigkeiten

Adaption & Innovation

REGELN ?

Agenda.

1 Regulatorik und Regelwerke.

2 **Informationssicherheit.**
Ein Beispiel zum Anfassen.

3 Sinnbildung.

4 Awareness.

Informationssicherheit. Motivation?

Gesetze.

Ich muss!

(Vermeidung von Strafen)

Kunden.

Ich soll!

(Neugeschäft erfordert das)

Märkte.

Ich wachse!

(Zertifizierung als Entré)

Geld & Wissen.

Ich schütze!

(Nachhaltige Existenzsicherung)

Allgemeine Fürsorge.

Ich beschütze!

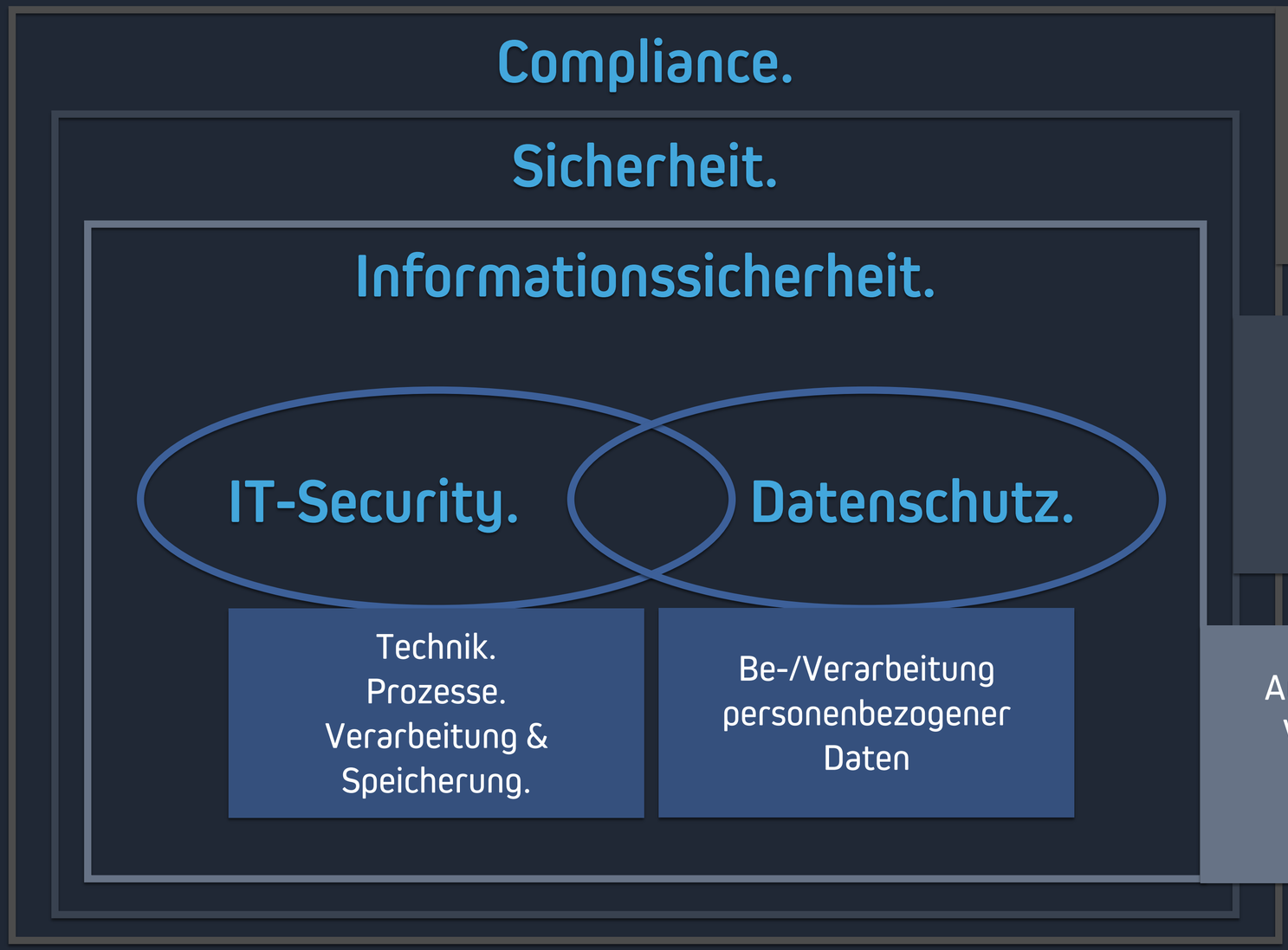
(Gemeinwohl, KRITIS)

Verantwortung.

Ich will!

(Corporate Security Responsibility)

Informationssicherheit.



Verantwortung (des Vorstands) für Einhaltung der gesetzlichen Bestimmungen und unternehmens-internen Richtlinien (DCGK).

Gefahrenfreier Zustand.

Frei von unvertretbaren Risiken.

Aufrechterhaltung (geforderter) Vertraulichkeit, Integrität und Verfügbarkeit aller Art von Informationen.

Informationssicherheit vs. Regeln.

Wie,
wenn die Organisation die Regeln nicht kennt? Nicht versteht? Vergisst?
(Latenzen)

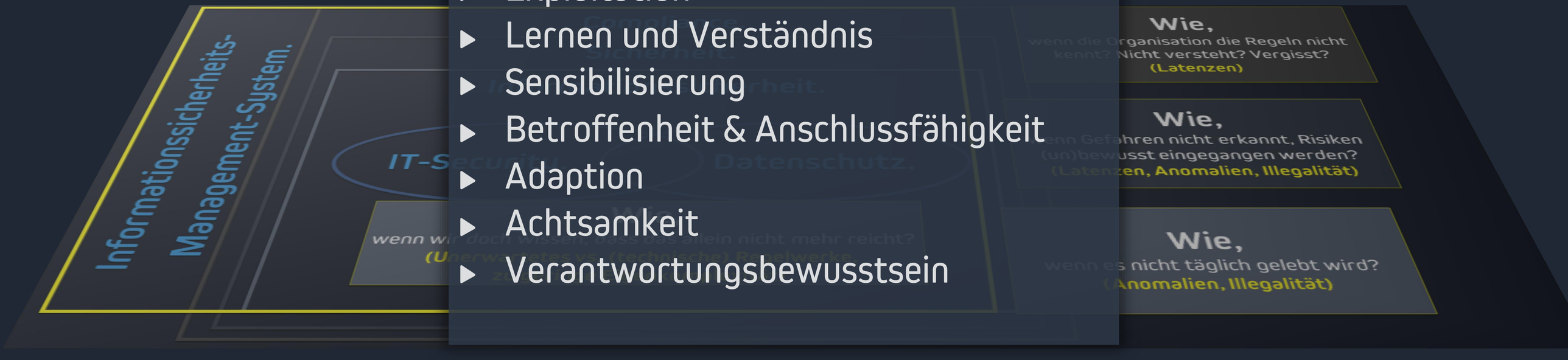
Wie,
wenn Gefahren nicht erkannt, Risiken (un)bewusst eingegangen werden?
(Latenzen, Anomalien, Illegalität)

Wie,
wenn es nicht täglich gelebt wird?
(Anomalien, Illegalität)

Was braucht es demnach?

Informationssicherheit erfordert demnach auch organisationale(s) …

- Exploitation
- Lernen und Verständnis
- Sensibilisierung
- Betroffenheit & Anschlussfähigkeit
- Adaption
- Achtsamkeit
- Verantwortungsbewusstsein



Agenda.

1 Regulatorik und Regelwerke.

2 Informationssicherheit.

3 **Sinnbildung.**

Verstehen. Erkennen. Entwickeln.

4 Awareness.

Sinnstiftend.

"Ah. Das ergibt Sinn. So machen wir das."

Sinnstiftend.

"Sich sinngemäß verhalten."

Sinnbildend.

"Seine Sinne entwickeln."

Sinnbildend.

"Seine Sinne schärfen."

Sinnbildend.

"Sich auf unbekanntem Terrain zurechtfinden."

Sensemaking.

Weick: Das gerade Erlebte in subjektiv sinnvolle Einheiten gliedern

In Konstruktion der Identität verankert

Sinnbildung ist äußerst subjektiv und erzwingt fortwährend neue Positionierung

Retroperspektiv

Erst wird beobachtet, dann ein Sinn konstruiert

Verhalten und Umwelt interagieren

Umwelt beeinflusst Verhalten, das wiederum auf die Umwelt wirkt

Dialog (intern oder mit Umwelt)

Mit sich selbst – mit Kollegen – mit Fremden

Fortlaufend

Konstruktion, Interaktion und Dialog stoßen den Prozess stets neu an

Hervorgestellte Hinweise

Wir konzentrieren uns auf Dinge, die in der Vergangenheit wichtig waren

Plausibilität statt Rationalität

Nicht die genaue Wiedergabe, sondern die Einpassung in die eigene konstruierte Welt ist das Ziel

Agenda.

Regulatorik und Regelwerke.

Informationssicherheit.

Sinnbildung.

Awareness.

Achtsame Organisationen.

Compliance. Sensibilisierung. Awareness.

BSI Grundschutz.

" Sensibilisierung"

B 1.13 / M 2.198 / M 3.5 / M 3.13 / M 3.26 / M 3.47 / M 3.60 / M 3.96

ISO27001 u.a.

"Bewusstsein"/"Awareness"/

ISO27001:2013 ISO27002:2013: Kontrolle A.7.2.2 / PCI DSS 3.2: Anforderung 12.6.1 / ISO22301:2012: 7.3 Awareness

EU-DSGVO

"Sensibilisierung"

Art. 39, (Art. 57)

Compliance vs. Awareness.

BSI Grundschutz.

" Sensibilisierung"

B 1.13 / M 2.198 / M 3.5 / M 3.13 / M 3.26 / M 3.47 / M 3.60 / M 3.96

ISO27001 u.a.

"Bewusstsein"/"Awareness"/

ISO27001:2013 ISO27002:2013: Ko
A.7.2.2 / PCI DSS 3.2: Anforderung 1
ISO22301:2012: 7.3 Awarenes

Gesetze.

Ich muss!

(Vermeidung von Strafen)

Kunden.

Ich soll!

eschäft erfordert das)

Märkte.

Ich wachse!

(Zertifizierung als Entré)

Geld & Wissen.

Ich schütze!

(Nachhaltige Existenzsicherung)

Allgemeine Fürsorge.

Ich beschütze!

(Gemeinwohl, KRITIS)

Verantwortung.

Ich will!

(Corporate Security Responsibility)

Compliance. Awareness. Kultur.

BSI Grundschutz.

" Sensibilisierung"

ISO27001 u.a.

"Bewusstsein"/"Awareness"/

ISO27001:2013 ISO27002:2013: Kc

A.7.2.2 / PCI DSS 3.2: Anforderung 1

ISO22301:2012: 7.3 Awarenes

Allge

(Ge

Geld & Wissen.

Verantwortung.

Ich will!

Awareness

als

Formalkriterium

Awareness

als

Kultur

Awareness-Kultur durch

Exploitation, Lernen und Verständnis, Sensibilisierung, Betroffenheit & Anschlussfähigkeit, Adaption, Achtsamkeit, Verantwortungsbewusstsein

Formalkriterien und Compliance als Abfallprodukt

einer sensibilisierten, achtsamen Organisation, deren Mitglieder zu Informationssicherheit einen Sinn entwickelt haben und auch in unbekannten Situationen besonnen (re)agieren

(V

Fragen?

Gerne.

SECUTAIN

Ihr Partner, wenn es um Awareness geht.