Love, Peace & Compliance

19.06.2024 | IT4B Digital Summit

19.06.2024 | IT4B Digital Summit

Love, Peace & Compliance

Mit dem etwas anderen Ansatz Datenschutz und Informationssicherheit pragmatisch umsetzen

Tim Hoffmann

UIMC

Berater für Datenschutz und Informationssicherheit

- Wirtschaftswissenschaften an der Universität-GH Essen
- Studien-Schwerpunkte; u. a.
  - » Organisation
  - » Informationsmanagement
- Seit 2002 als Berater mit den Schwerpunkten
  - » Datenschutz und
  - » Informationssicherheit / IT-Sicherheit

Wer wir sind

pragmatisch.erfahren.verständlich.

UIMC

Datenschutz

Externe Datenschutzbeauftragung, E-Learning, Audits, Dienstleister-Auditierung etc.

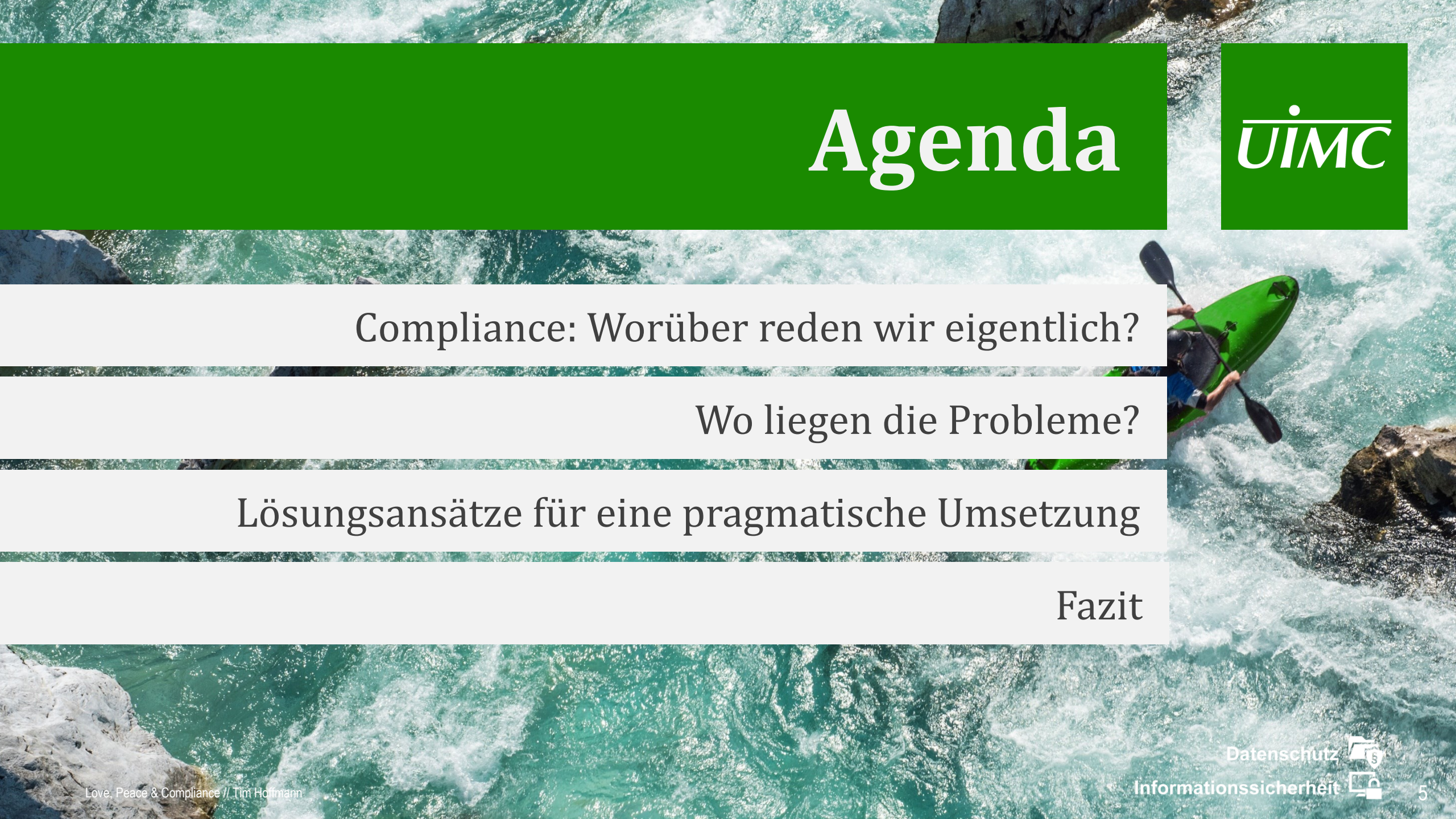
Informationssicherheit

Aufbau eines ISMS bis zur Zertifizierung, Informationssicherheitsbeauftragter etc.

Organisation / Strategie

Beratungsleistungen bei konzeptionellen und strategischen Fragestellungen

Agenda



- Compliance: Worüber reden wir eigentlich?
- Wo liegen die Probleme?
- Lösungsansätze für eine pragmatische Umsetzung
- Fazit

Agenda

UIMC

Compliance: Worüber reden wir eigentlich?

Wo liegen die Probleme?

Lösungsansätze für eine pragmatische Umsetzung

Fazit

Compliance

UIMC

Compliance ist die betriebswirtschaftliche und rechtswissenschaftliche Umschreibung für die Regeltreue von Unternehmen, also die **Einhaltung von Gesetzen, Richtlinien und freiwilligen Kodizes.**

Die Gesamtheit der Grundsätze und Maßnahmen eines Unternehmens zur Einhaltung bestimmter Regeln und damit zur Vermeidung von Regelverstößen wird als „Compliance Management System“ bezeichnet.

Steigende Anforderungen

- Datenschutz
  - » DSGVO und weitere Datenschutzgesetze
  - » Anforderungen durch Kunden (z. B. Auftragsverarbeitung)
- Informationssicherheit
  - » Gesetzgeber (z. B. NIS2UmsuCG)
  - » Kunden (z. B. TISAX, ISO, Grundschutz)
  - » Schutz des Unternehmens

Steigende Digitalisierung

UIMC

- Prozesse werden digitaler
  - » Vereinfachung der Verfahren
  - » Kostenreduktion
  - » Flexibilisierung
  - » Große Vorteile und Nutzen für die Unternehmen

Steigende Abhängigkeiten

- Prozesse werden digitaler
  - » Vereinfachung der Verfahren
  - » Kostenreduktion
  - » Flexibilisierung
  - » Große Vorteile und Nutzen für die Unternehmen
- …aber:
  - » Abhängigkeit von IT-Systemen
  - » fehlende Wahrnehmung von Risiken (Fokus auf Nutzen)

Steigende Bedrohungslage

ÜiMC

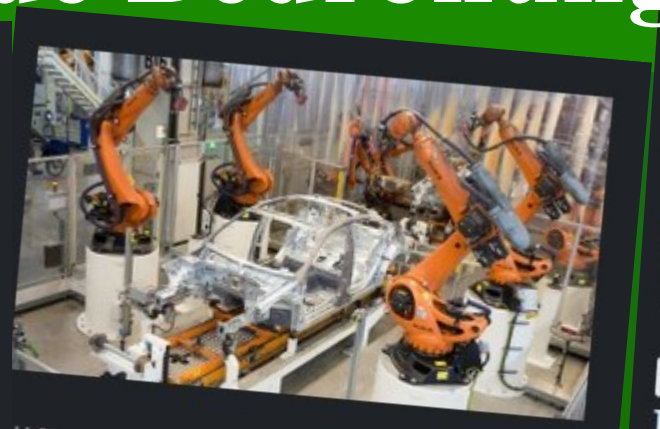
AUCH KLEINE GEMEINDE BETROFFEN

Hackerangriff legt Website von Flughafen Kopenhagen lahm

Die Website des Flughafens in der dänischen Hauptstadt ist derzeit nicht

EVENTIM STOPPT WEITERVERKAUF

Hacker-Angriff auf Konzerttickets von Taylor Swift



HACKERANGRIFFE

Tausende Dateien von Volkswagen gestohlen

F+ SCHUTZ VOR HACKERANGRIFFEN

Freitags werden Regeln für Cybersicherheit öfter missachtet

Wenn der Arbeitstag zu E

DATENSCHÜTZER ALARMIERT

Mehr Cyberattacken in Hessen

CHIP

Gefahr für Telekom-Kunden: Ver… Fake-Rechnungen - CHIP

Der… war…

Security-Insider

Spear Phishing und KI – Eine gefährliche Kom…

Während Künstliche Intelligenz immer leichter einzusetzen und da… gebräuchlicher wird, müssen Organisationen mit einer neuen Gen…

Kopierer-Fehlfunktion

Xerox schaltet Zahlendreher-Funktion ab

In hunderttausenden Xerox-Multifunktionsdruckern steckt ein Software-Bug, der Zahlendreher verursachen kann. Nun hat der Konzern das verantwortliche

Neue Spam-Welle mit Bewerbungsschreiben wird erwartet – ACHTUNG: dahinter verbirgt sich Ransomware

Art der Bedrohung

Verschlüsselung von Privat- und Firmendaten und anschließende Erpressung zur Bezahlung eines…

Cybersecurity

UIMC

Eins ist (eigentlich) Allen klar:

Es ist keine Frage, ob man Opfer eines Cyberangriffs wird, sondern wann!

Was ist zu tun?

- Wer schreibt, der bleibt!
- oder: Aufbau eines Managementsystems, u.a.
  - » Aufbau eines Risikomanagements zur Priorisierung
  - » Vorgaben durch Richtlinien (Prävention und Notfallmaßnahmen)
  - » Organisationsstruktur und Besetzung der notwendigen Rollen
  - » Schulungen / Sensibilisierung
  - » Kontrolle der Umsetzung und Wirksamkeit

Agenda

UIMC

Compliance: Worüber reden wir eigentlich?

Wo liegen die Probleme?

Lösungsansätze für eine pragmatische Umsetzung

Fazit

Hindernisse


Et hätt nochmal allet joot gegange

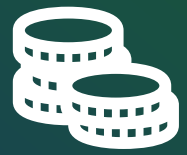

keine Zeit / personelle Ressourcen


Unwissenheit


Themen nicht sexy


Problem nicht sehen (wollen)


behindert Business


kein Geld / finanzielle Ressourcen


widersprüchliche Ziele

Faktor Mensch

- Durch das Verhalten von Beteiligten entstehen Gefahren für die Compliance (z. B. Datenpannen, Gesetzesverstöße)
- Viele Beteiligte verhalten sich nicht zielkonform*
  - » Frage: Kennen alle Beteiligten die Ziele und verstehen diese?
- Oftmals werden den Beteiligten „falsche“ Anreize gegeben
  - » Frage: Welche Ziele lebt die Geschäftsleitung vor?

*) im Sinne der Compliance

Agenda

Compliance: Worüber reden wir eigentlich?

Wo liegen die Probleme in der Umsetzung?

Lösungsansätze für eine pragmatische Umsetzung

Fazit

Umsetzung von Compliance

Schritt zurück:

Kultur-Änderung

Neue Kultur

- Commitment der Geschäftsführung
  - » Bedeutung für das Geschäft darstellen (Tipp: „Kaufmännische Bedeutung“ betrachten)
  - » Strategie definieren
  - » Ziele und Maßnahmen ableiten
  - » wichtig: durch Geschäftsleitung vorleben

Neue Kultur

- Commitment der Geschäftsführung
- Alle Beteiligten mitnehmen
  - » Ideen berücksichtigen
  - » Fehlerkultur schaffen
  - » Sensibilisierung / Schulung / Fortbildung
  - » Ziele der Mitarbeiter:innen von Unternehmenszielen ableiten

Neue Kultur

- Commitment der Geschäftsführung
- Alle Beteiligten mitnehmen
- Gemeinsamkeiten entdecken
  - » Synergien generieren
  - » Mehrwerte schaffen
  - » *Miteinander* kommunizieren (nicht *übereinander*)
  - » Compliance-Ansprechpartner als *Helfer* etablieren (nicht als „Störer“)

Neue Kultur

- Commitment der Geschäftsführung
- Alle Beteiligten mitnehmen
- Gemeinsamkeiten entdecken
- Compliance integrieren
  - » keine autarken Prozesse, sondern Business-Prozesse mit Compliance-Bausteinen
  - » Operationalisierung durch Berücksichtigung in den Zielen/KPI der Mitarbeiter:innen

In die Bewegung kommen

- Zusammenbringen der wichtigsten Beteiligten
  - » Fachbereiche/Business und Compliance-Experten (DSB, ISB etc.)
  - » Gemeinsame Ziele formulieren
  - » Kommunikationskonzept entwickeln
  - » Gemeinsame Vorgehensweise vereinbaren (Commitment schaffen)
- *…und natürlich auch:* Klassische Herangehensweise
  - » Audit, Maßnahmenplanung, Umsetzung, Schulung, Kontrolle …
  - » idealerweise natürlich integriert

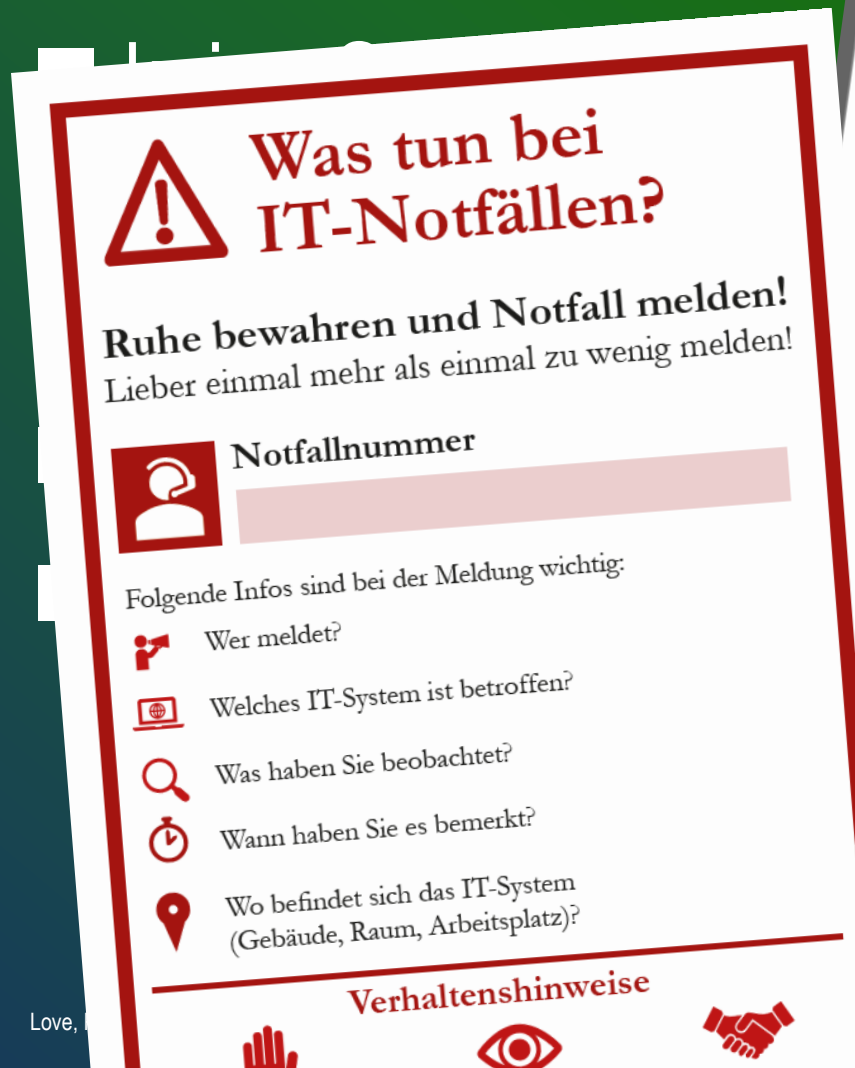
Und doch noch ein Prozess

Akut-Maßnahmen

- keine Schnellschüsse
- Sensibilisierung der Belegschaft
  - » Auch jener Mitarbeiter:innen, die nicht mit PC arbeiten
- Etablierung eines Meldesystems
- Prüfung der aktuellen Sicherheitsmaßnahmen
  - » Backups
  - » Updates / Sicherheits-Patches etc.
  - » Virenscanner, Firewalls etc.

Akut-Maßnahmen

UIMC



Was tun bei IT-Notfällen?

Ruhe bewahren und Notfall melden!
Lieber einmal mehr als einmal zu wenig melden!

Notfallnummer

Folgende Infos sind bei der Meldung wichtig:

- Wer meldet?
- Welches IT-System ist betroffen?
- Was haben Sie beobachtet?
- Wann haben Sie es bemerkt?
- Wo befindet sich das IT-System (Gebäude, Raum, Arbeitsplatz)?

Verhaltenshinweise

Unternehmens- und Informations-Management Consultants

UIMC®

Klassifikationsstufe	Beschreibung	Beispiel	Schutzmaßnahmen (Auszug)
Hochsensibel	Informationen, deren Missbrauch die gesellschaftliche Stellung und/oder die wirtschaftlichen Verhältnisse » des Mitarbeiters, » des Kunden und/oder » des Unternehmens *erheblich* beeinträchtigen kann. **[Existenz-Bedrohung]**	» durch vertragliche Reglungen (NDA) geschützte Informationen » kritische Geschäftsinformationen (z. B. Verluste, Schulden, geplante Personalmaßnahmen wie betriebsbedingte Kündigungen oder Kurzarbeit) » besondere Arten personenbezogener Daten (z. B. Krankheits-/Gesundheitsinformationen der Mitarbeiter)	*Zusätzlich zu Maßnahmen für sensible Informationen:* » explizite Kennzeichnung als „hochsensibel" » Übermittlung und Speicherung auf mobilen Datenträgern nur verschlüsselt » Hohe Komplexität der Passworte (ggf. zweiter Faktor) » Aufbewahrung von Unterlagen unter Verschluss » Sichere Vernichtung mit Datentonne / Shredder (Stufe 5) » Weitergabe nur nach Freigabe durch die GL » Nutzung des „vertraulichen Druckens" » Kein Zutritt in Bereiche für Bereichsfremde » Automatischer Türschließer (inkl. Knauf von Außen) » Striktes Fotografierverbot
sensibel	Informationen, deren Missbrauch die gesellschaftliche Stellung und/oder die wirtschaftlichen Verhältnisse » des Mitarbeiters, » des Kunden und/oder » des Unternehmens beeinträchtigen kann. **[Verlust des Ansehens]**	» kaufmännische Informationen (Umsatz, Gewinn/Verlust) » personenbezogener Daten von Mitarbeitern und Geschäftspartnern » Informationen über Kunden- und Lieferanten-Beziehungen » Individuelle Kundenangebote inkl. Preise	» Übermittlung und Speicherung auf mobilen Datenträgern mindestens passwortgeschützt » Normale Komplexität der Passworte » Weitergabe nur durch berechtige Personen an berechtigte Personen » Sicherstellung einer hohen Verfügbarkeit » Sichere Vernichtung mit Datentonne / Shredder (Stufe 3) » Aufbewahrung von Unterlagen unter Verschluss » Verschluss der Räume, wenn unbesetzt » Zutritt für Besucher nur unter Aufsicht
n	Informationen, deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse der Einsichtnehmenden gebunden sein sollte.	» Organigramm » Mitarbeiter-Listen (dienstliche Kontaktdaten) » Veröffentlichung von Personalveränderungen	
	Informationen, die frei zugänglich sind. Der Einsichtnehmende muss dabei kein berechtigtes Interesse geltend machen		» Weitergabe nur bei Erforderlichkeit

nsmatrix und Schutzmaßnahmen [Version 01/2019]

Agenda

UIMC

Compliance: Worüber reden wir eigentlich?

Wo liegen die Probleme?

Lösungsansätze für eine pragmatische Umsetzung

Fazit

Fazit: Kultur-Änderungen sinnvoll

- Richtige Kultur ist zunächst wichtiger als der Prozess selbst
- Kommunikation ist das A und O
- Ganzheitliche Umsetzung
  - » Umsetzung von Compliance ist interdisziplinär
  - » Akzeptanz schaffen
  - » Fachleute und Business zusammenbringen
- Integration in die Gesamt-Strategie
  - » keine Insel-Lösungen

Fazit: Argumente für den Wandel

- **Effektivität**
  - » Umsetzung auf (fast) allen Ebenen: Technik, Organisation und Mensch
- **Effizienz**
  - » keine/weniger gegenläufige Aktivitäten und Nachbesserungen
- **Zufriedenheit**
  - » (fast) alle ziehen an einem Strang und erreichen gemeinsam Ziele
- **oftmals tatsächlicher Mehrwert**
  - » Vereinfachung bei (anderen) Zertifizierungen (z. B. QM)
  - » Notwendigkeit im Vertrieb (z. B. DSGVO oder TISAX)
  - » Compliance wird als Teil des Business verstanden

Losgelöst von Kulturwandel: To(p)Do10

1. Festlegung von **Verantwortlichkeiten** (u. a. DSB, CISO)
2. Durchführung einer **Risikobewertung**
3. Aufbau eines funktionierenden **Meldewegs**
4. Durchführung einer **Bestandsaufnahme** („Fangen Sie an“)
5. Erstellung eines **Sicherheitskonzepts**
6. Prüfung der **Datentransfers**
7. Beachtung der Rechenschaftspflicht (u. a. **Dokumentation**)
8. Schaffen Sie **Transparenz**: Reden Sie darüber, was Sie tun.
9. **Revision** der „kritischen“ Bereiche
10. Last, not least: Schulung und **Sensibilisierung** ist das A und O

Love, Peace & Compliance

Fragen??

UIMC

Mancher ertrinkt lieber,
als daß er um Hilfe ruft.
– Wilhelm Busch

thoffmann[at]uimc.de

Folgen Sie uns auf LinkedIn:
www.linkedIn.com/company/uimc

weitere Vorträge

UIMC

- **Nicht der Apfel hat Schneewittchen vergiftet,** sondern ihr blindes Vertrauen oder: Die Bedeutung von Sensibilisierung
- **You can't stop the waves, but you can learn to surf**
  oder: Der richtige Umgang mit dem unvermeidlichen Sicherheitsvorfall
- **Datenschutz ist nicht sexy, aber…**
  Gesetzliche Anforderungen und aktuelle Problemstellungen im Datenschutz pragmatisch lösen

www.uimc.de/webecollege

Kontaktdaten

UIMC Dr. Vossbein GmbH & Co. KG
Otto-Hausmann-Ring 113
42115 Wuppertal
Telefon: +49 202 946 7726 200
E-Mail: consultants@uimc.de
Internet: www.UIMC.de

UIMCert GmbH
Otto-Hausmann-Ring 113
42115 Wuppertal
Telefon: +49 202 946 7726 300
E-Mail: certification@uimcert.de
Internet: www.UIMCert.de

Wuppertal

Saarbrücken

Berlin

Wien

IT-Sicherheit mit System

Aufbau eines Informationssicherheits-Managementsystem

Schulung der Mitarbeiter

Auditierung der IT-Sicherheit

Risiko-Workshop

u. v. m.

… bis hin zur Zertifizierungsreife

Datenschutz von A bis Z

UIMC®

Externe Datenschutzbeauftragung

Schulung der Mitarbeiter

Datenschutz-Checkup / Auditierung

Datenschutz-Management / -Organisation

u. v. m.

Pragmatischer Datenschutz weiterhin möglich

„Superman braucht keinen Gurt!“

(Muhammed Ali zur Flugbegleiterin)

„Superman braucht auch kein Flugzeug!“

(Die Antwort der Flugbegleiterin)