MATERNA
Information & Communications

Faktor Mensch in IT-Managementsystemen oder *Security-Awareness „nachhaltig und wirksam“: Mit Spannung, Spaß und Spiel zu mehr Sicherheit*

Nadin Ebel, Materna

Agenda.

- **Motivation oder veränderte Rahmenbedingungen**
- Regulatorische Anforderungen
- Awareness: Psychologische Aspekte & Methoden

Ausgangslage.

Schäden durch höhere Gewalt

Angriffe von außen

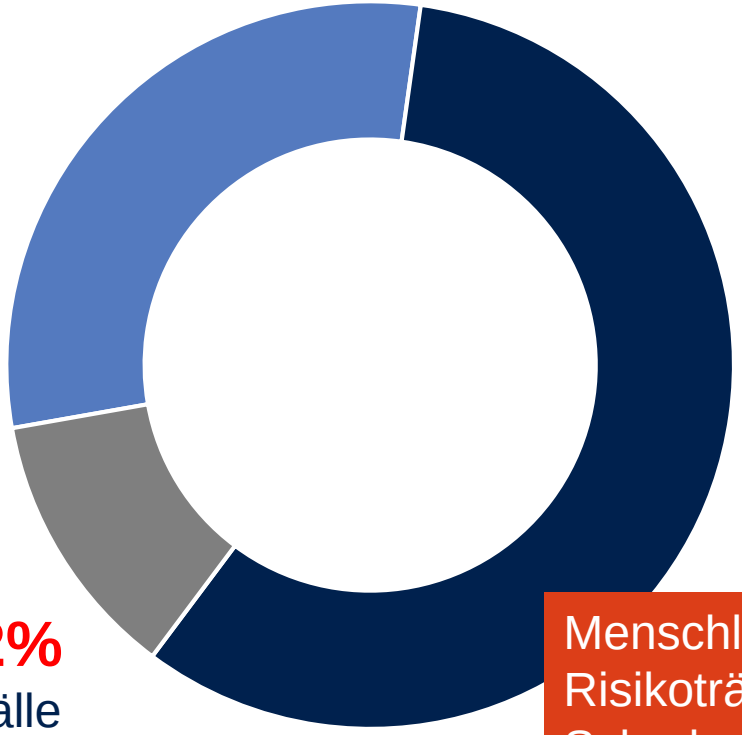
Gefahren von innen

Externer Mail-Verkehr
Unkenntnis
SPAM
Computerviren
BYOD
Abhören
Mitarbeiter
Spionage
Irrtum
Diebstahl
Externes Personal
Notfall
BDSG
Wirtschaftsspionage
Social Engineering
Datenverlust
Hacker
Phishing
Facebook, Twitter, XING, Instagram
Digitalisierung
Industrie 4.0
CFO Fraud
Smart ….
IoT
Datenschutz
Vernetzte Systeme
Digitalisierung
Menschen, Maschinen, Anlagen, Logistik und Produkte

Ignorieren funktioniert nicht!

Die meisten Schäden werden vor Ort verursacht!

Welche IT-Vorfälle gab es in ihrem Unternehmen?



30%
Angriffe über das Internet (z. B. Online-Einbruch, DDOS-Attacken)

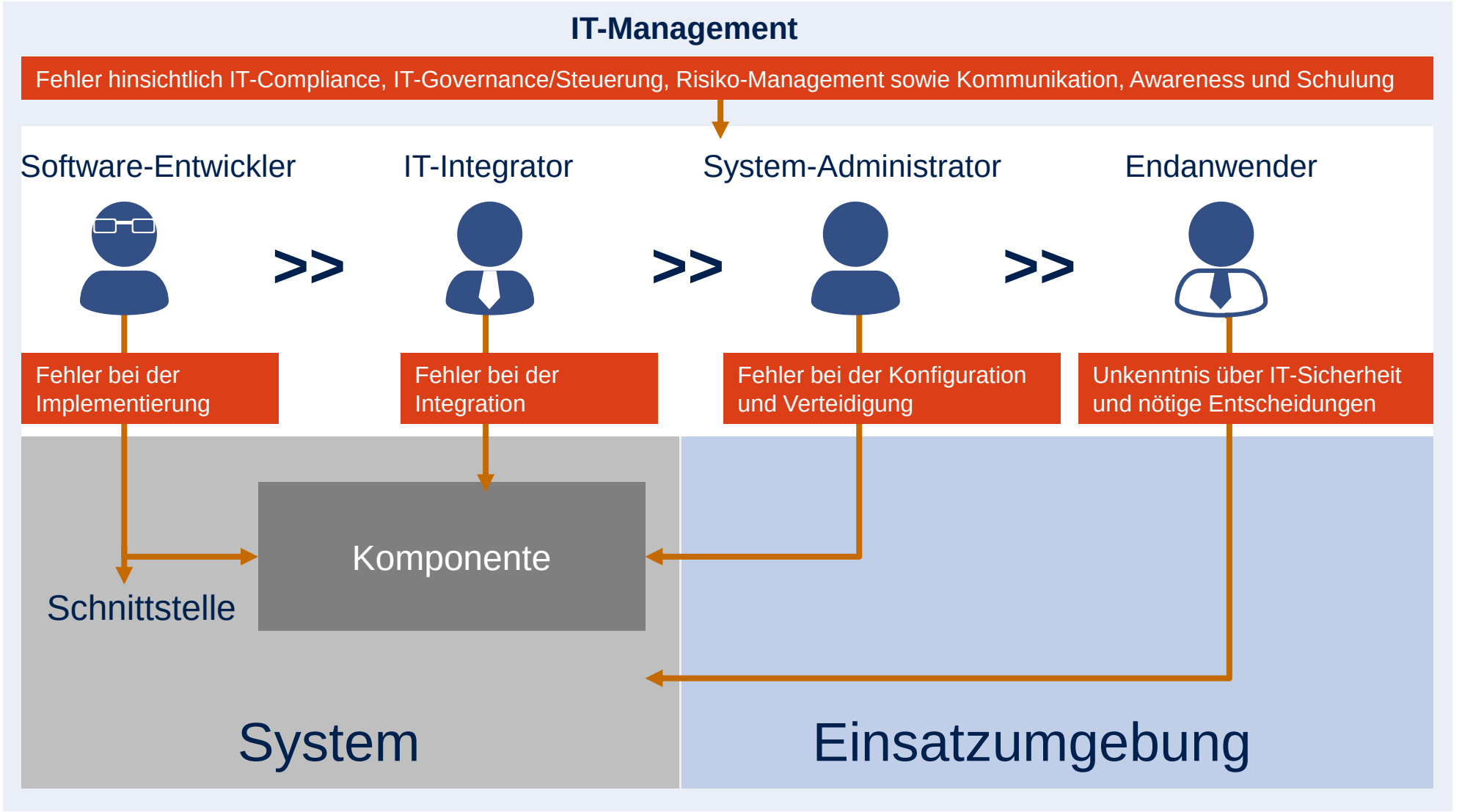
58%
IT-Sicherheitsvorfälle, die „vor Ort“ verursacht wurden (z. B. gezielter Datenklau, Virus über Datenstick…)

12%
Sonstige Vorfälle

Menschliches Verhalten ist Risikoträger und Schadensverursacher Nummer 1 für die IT-Sicherheit.

Quelle: BITKOM

Menschliche Sicherheitsprobleme innerhalb der Wertschöpfungskette



Quelle: Human-Centered Systems Security, IT-Sicherheit von Menschen für Menschen

Ignorieren funktioniert nicht!

Die Zahlen sprechen für sich:

56%
der IT-Entscheider in Deutschland der Ansicht, dass Mitarbeiter über wenig Bewusstsein und Kenntnisse im Bereich IT-Sicherheit verfügen.
(VMware)

11%
der Mitarbeiter würden Sicherheitsrichtlinien des Unternehmens verstoßen, um ihre Arbeit effektiv ausführen zu können.
(VMware)

Laut Medienberichten sind von Mitarbeitern verursachte Fehler für **mehr als die Hälfte** aller Security-Probleme in der IT verantwortlich.

Die Anzahl von Spam-Nachrichten mit Schadsoftware im Anhang ist um **1.270 %** angestiegen.
(BSI)

Agenda.

- Motivation oder veränderte Rahmenbedingungen
- **Regulatorische Anforderungen**
- Awareness: Psychologische Aspekte & Methoden

Informationssicherheit – Die drei Säulen.

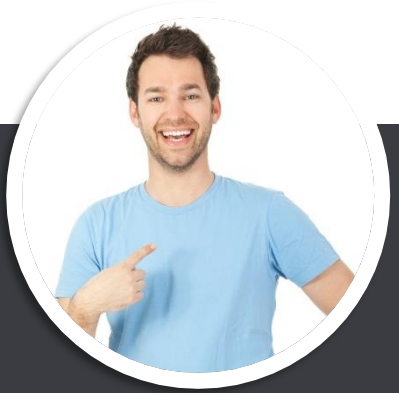
Kundenanforderungen

- Öffentliche Kunden
- Zuverlässige Serviceleistungen
- Wahrung des Datenschutzes
- Sichere Infrastrukturen
- E-Business
- E-Government
- Know-how-Schutz
- **Kunden-/Lieferanten-Compliance**

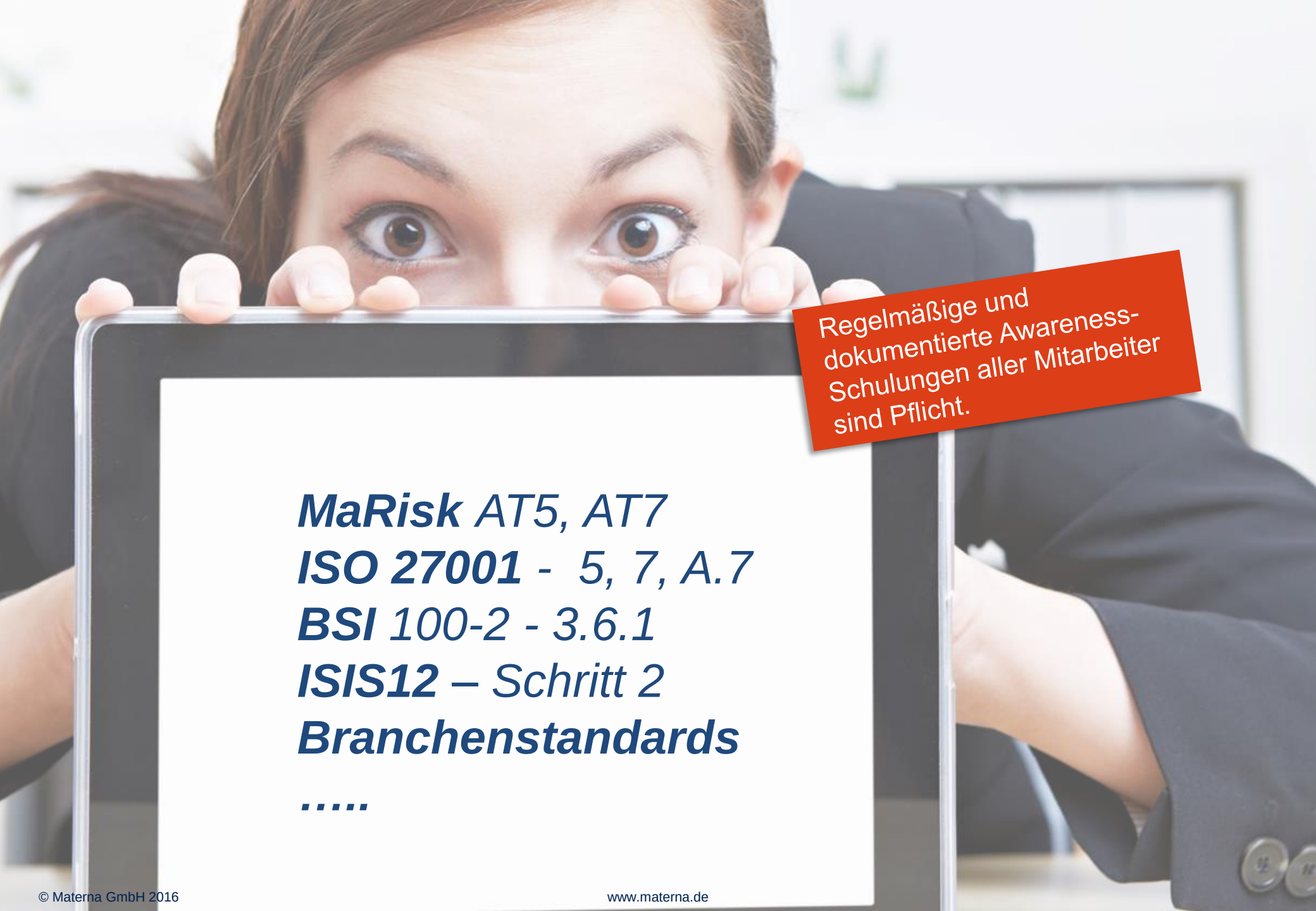
Rechtliche Vorgaben

- Datenschutz (BDSG)
- EU-DSGVO
- Haftungsfragen
- Risikomanagement und Berichtswesen (z. B. SOX, Basel III, MaRISK, KontraG)
- IT-Sicherheitsgesetz
- **Corporate und IT Compliance & Governance**

Eigeninteresse



- Schutz von Informationen und Wissen
- Schutz der Infrastrukturen und der Schnittstellen
- Zusammenarbeit mit externen Mitarbeitern
- Kooperation mit Wettbewerbern und Partnern
- Image in der Öffentlichkeit
- **Vertrauen**



Agenda.

- Motivation oder veränderte Rahmenbedingungen
- Regulatorische Anforderungen
- **Awareness: Psychologische Aspekte & Methoden**

Einführung in die Awareness.

Awareness

Sensibilisierung

Bewusstsein

Gewahrsein

Achtsamkeit

Bewusstheit

Gewahrsein

Aktive, innere Haltung der Aufmerk-samkeit

Ziele der Security-Awareness.

Wie kann man es besser machen?

Auf die **menschlichen** Aspekte eingehen!

Die besonderen Eigenschaften berücksichtigen und fördern.

Schritt 2 aus ISIS12 – Mitarbeiter sensibilisieren

Vorabkommunikation zur Sensibilisierung aller Organisationsebenen

Notwendigkeit darstellen: „Jeder ist für Informationssicher-heit verantwortlich!“

Verschiedene Methoden einsetzen! (Demos, Seminare/ Fachschulungen, E-Learning, Poster, Übungen etc.)

- Entwicklung von speziellen Präsentationen, Schulungen und weiteren Kommunikationsereignissen für verschiedene Zielgruppen (Leitung, Personalrat, interne und externe IT-Mitarbeiter, Endanwender)
- Empfehlungen für die kontinuierliche Sensibilisierung von Mitarbeitern
  - Mitarbeiter als die wichtigste Firewall
  - Mitarbeiter als Sicherheitsschwachstelle

Die Kunst …

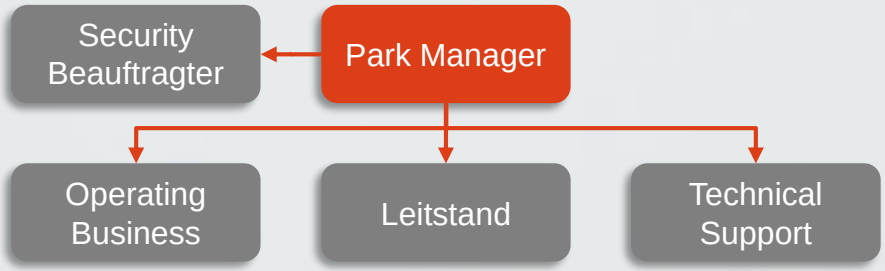
Lernen durch Erleben

Mit Spaß & Spannung
zu mehr Sicherheit!

- … besteht darin, verschiedene Ansätze zu finden und zu verfolgen, um die „Schwachstelle Mensch“ kontinuierlich anwendergruppenspezifisch zu sensibilisieren
- „Gamification“ bietet eine Ergänzung zu klassischen Schulungsformaten und technischen Fachtrainings

Sicherheit im Freizeitpark

- Zwei Teams treten gegeneinander an
- Die Herausforderung:
  - Prozesse für einen reibungslosen Betrieb aufsetzen
  - Sicherheit im Park gewährleisten
  - Besser sein als die Konkurrenz!
- Mehrere Runden mit typischen Szenarien aus der Praxis
- Reflektion der sicherheitsrelevanten und unternehmerischen Aspekte in den Feedbackrunden mit den Trainern



Zusammenfassung.

1. Awareness ist substanziell für erfolgreiche Informationssicherheit.
2. Die Lösungen liegen in der Kultur der Organisation.
3. Die Mitarbeiter brauchen „greifbare“ Vorbilder.
4. Die Methoden der Awareness sind vielfältig.
5. Multipräsente Trainingsinhalte als Vehikel nutzen.
6. Der Erfolg liegt in der Kreativität der Kampagnen.
7. Fokus von Awareness ist die persönliche Integration der Mitarbeiter.
8. Awareness muss in die Köpfe.

Fragen?

MaTA und Dipl.-Kffr.
Nadin Ebel
Master Consultant

BL IT Factory, ITSM Consulting
Materna GmbH

Telefon: 01570/112 2748
E-Mail: nadin.ebel@materna.de