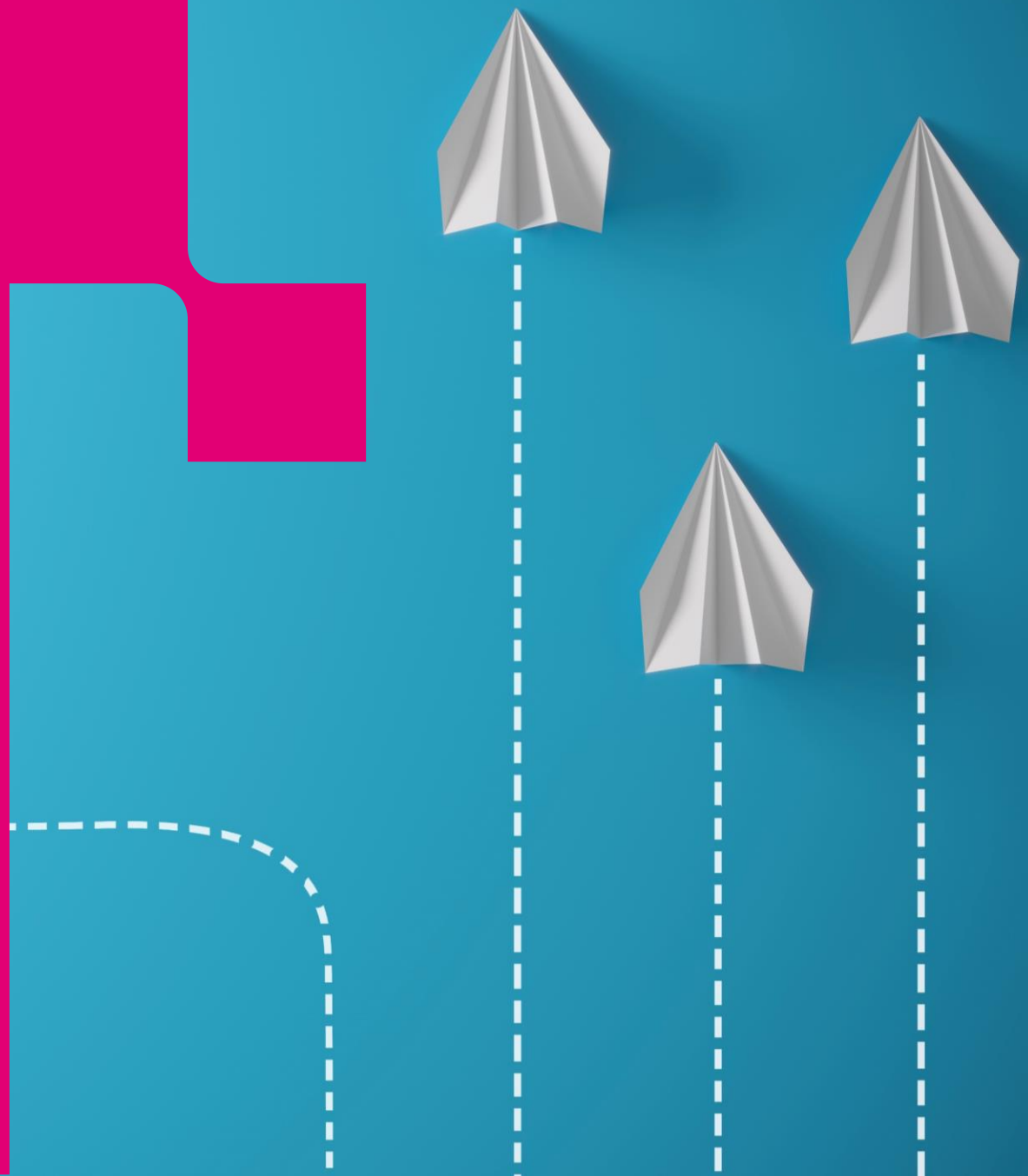
DTGK Classified & Public

MKK FORUM 2030 - Bad Soden-Salmünster

ISMS im Öffentlichen Sektor



Zahlen Daten Fakten.

6,06 Mrd

Malware Angriffe
wurden in 2023
weltweit detektiert.
(National Universty)

194 Tage

Durchschnittliche Zeit zur Identifizierung
einer Datenpanne.
(Varonis)

267 Mrd.

€ Schaden wurden 2023
in der deutschen
Wirtschaft durch
Cyberkriminalität
verursacht. (Bitkom)

81%

aller Unternehmen
waren von analoger und
digitaler
Industriespionage
betroffen. (Bitkom)

Kosten eines Sicherheitsvorfalles
>2,6 Mio EUR

Warum ist der Public Sektor für Cyberkriminelle so attraktiv?

- **Daten-Goldgrube**
  Bürgerakten, Regierungstätigkeiten, Informationen zu kritischen Infrastrukturen
- **Veraltete Technologien** Sicherheitsmaßnahmen
- **Fehlendes Budget**
  Fehlende Kenntnis/ Unterbesetzte Teams
- **Öffentliche Sichtbarkeit**
  als Bonus für Angreifende
- **Geopolitik**
  Cyber-Hybridkrieg

Herausforderung.

- **Komplexe Gesetzeslage & Regulatorik** in Bezug auf IT- und Informations-Sicherheitsniveau (**KRITIS/ NIS2**/ DSGVO)
- **Unklare Verantwortlichkeiten** & Schnittstellen
- Begrenzte **Budgets & Ressourcen**
- **Mangel an Knowhow**
- **Fachkräftemangel** im IT-Sicherheitsbereich
- Aufwändige **Dokumentation & Bürokratie**

„ UNKENNTNIS ERSETZT NICHT VERANTWORTUNG“

Steigende Anforderung & Verantwortung NIS2/ KRITIS.

Die Geschäftsführung ist verantwortlich:

- für die Schaffung einer Cybersicherheitskultur
- Bereitstellung von Ressourcen
- Maßnahmen zur Stärkung der Sicherheit in den Informationssystemen

ZU ERWARTENDE ANFORDERUNGEN:

- **Sicherheitskonzept**
- **Risikomanagement**
- **Störungsbehandlung**
- **Notfallmanagement**
- **Meldewesen**
- **Sicherheit der Lieferkette**
- **Überwachung & Schulung**

Lösung ist ein ISMS.

Etablierung eines Informationssicherheits-Managementsystem

Ziel: Sicherstellung von Informationen bzgl.

- **Vertraulichkeit, Integrität und Verfügbarkeit**

  über

- **Organisation/ Personal/ Prozesse/ Technik & Infrastruktur**

Zwei grundsätzlich etablierte ISMS-Ansätze:

- ISO/IEC 27001: internationaler Standard, flexibel, risikobasiert
- BSI IT-Grundschutz nach ISO 27001: **staatlich empfohlen, detailliert, bausteinbasiert**

Mehrwert durch ein ISMS.

Erhöhung des Sicherheitsniveaus und Resilienz

Erhöhung der Transparenz: Klare Dokumentation von Abläufen, Zuständigkeiten und Sicherheitsmaßnahmen

Förderung einer Sicherheitskultur: Informationssicherheit wird Bestandteil der Organisationskultur

Reputationsschutz: Beitrag zur digitalen Souveränität, Vermeidung von Datenpannen und IT-Ausfällen

Effizientere Ressourcennutzung: Zielgerichteter Einsatz von Budget und Personal

Sichere Basis für Digitalisierung: Grundlage für digitale Dienste

CYBERSECURITY ist der Schlüssel zur Resilienz.

- **Transparenz über Ihre Assets**
- **Proaktive Risikovorsorge**
  systematische Identifikation von IT-Risiken
- **Klare Notfall- und Reaktionspläne**
  strukturierte Krisenbewältigung
- **Sicherstellung des Betriebs im Krisenfall**
  Arbeitsfähigkeit wird schneller hergestellt
- **Kontinuierliche Verbesserung**
  PDCA-Zyklus – Resilienz wächst mit jeder Erfahrung
- **Sensibilisierung der Mitarbeitenden**
  Mensch als Sicherheitsfaktor, nicht als Schwachstelle

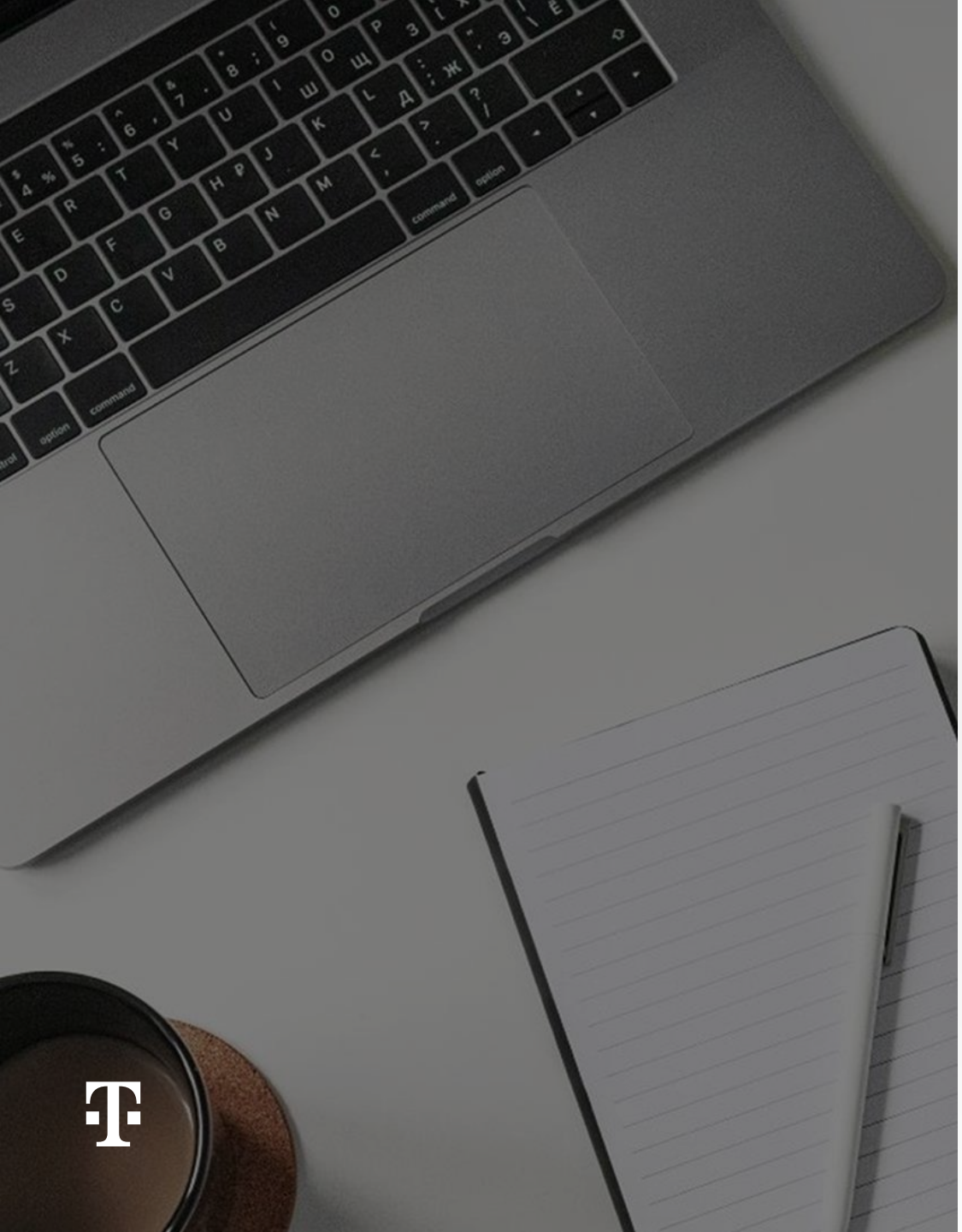
ISMS ist das Werkzeug für mehr Resilienz

STRUKTURIERT, NACHVOLLZIEHBAR, ANPASSUNGSFÄHIG

Ein ISMS schützt nicht nur Ihre Daten,
sondern schützt **VERTRAUEN,**
HANDLUNGSFÄHIGKEIT und **DEMOKRATIE**

Informationssicherheit ist keine Option,
sondern **PFLICHT** und **BASIS** für eine
starke **DIGITALE VERWALTUNG.**

Strukturiert	Netzwerke	Pragmatisch	Zielorientiert	Integrativ	Nachhaltig
▪ Schritt 1: **ISMS Kurzcheck** zur Status-Quo-Bestimmung ▪ Schritt 2: **ISMS-Implementierung** (Framework mit Arbeitspaketen)	▪ Nutzen von Erfahrungen durch **Einbindung ext. Knowhow** ▪ Synergien zwischen Behörden, Ämtern, Kommunen schaffen ▪ **Kontakt/ Austausch mit BSI**	▪ **Kleinere Scope als ALL IN** - Schutz ausgewählter Unternehmensbereiche ▪ „Die Norm ist flexibel“ ▪ **KEINE Überbürokratisierung**	▪ Erhöhung der Informationssicherheit vs. Erreichen der Zertifizierungsreife ▪ Ausschließlich dokumentenbasiert vs. Tool-unterstützt	▪ **Anforderungsmanagement** ▪ Berücksichtigung anderer Managementsysteme (z.B. ISO 9001) ▪ **Berücksichtigung der NIS2/ KRITIS / EU-DSGVO**	▪ Kollaborative Ausarbeitung der Prozesse und Dokumente ▪ Befähigung der Mitarbeiter ▪ Reifegradmodell ▪ PDCA. ▪ **Basis für Digitalisierung**



Alexander Lauth
Leiter Security
Transformation & Control
Classified & Public
Deutsche Telekom
–+49 (0) 160 8861030
alexander.lauth@telekom.de

Wir sind für Sie da.