# Der Inhouse-Lawyer als Krisenmanager im Datenschutz

Dr. Tobias Hemler
General Counsel DACH/TT
Amadeus Germany GmbH

amadeus
Your technology partner

”You can't defend.
You can't prevent.

The only thing you can do
is detect and respond.“

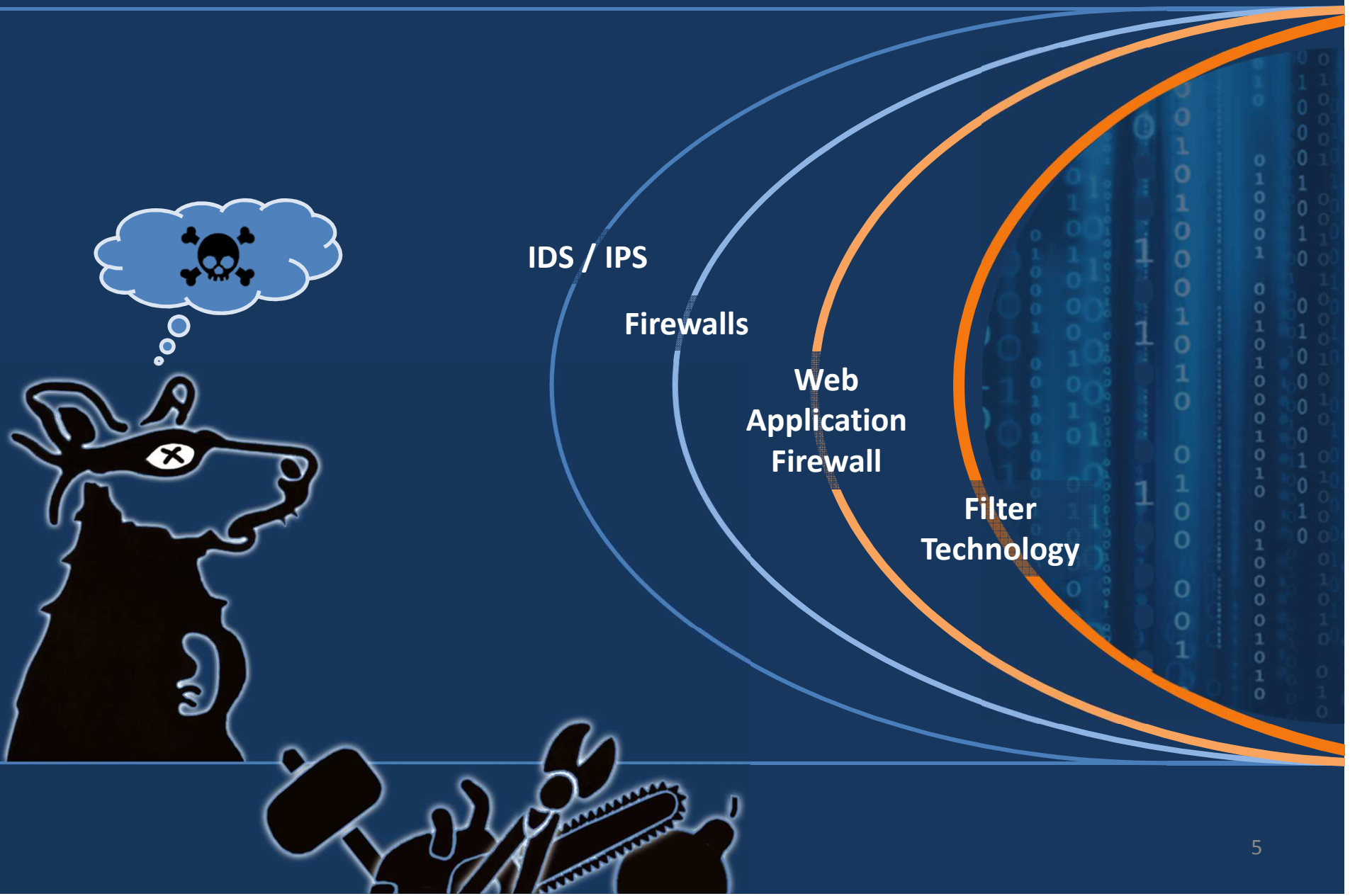
Bruce Schneier (*1963)

American cryptographer & computer security specialist

# Cat & Mouse Game

# The Hackers Motivation

# Ruin the Hackers Business Case!



# Ablauf

**Unmittelbare, schnelle Information an die Rechtsabteilung notwendig!**

**Panne nach der Panne: Information kommt bei der Rechtsabteilung erst Tage später an**

**Können Informations- und Reaktionsfristen noch eingehalten werden?**

**Test: Sind Sie im Unternehmen richtig aufgestellt?**

# Planung und Ablauf der Kundenkommunikation

- Klärung so schnell wie möglich
- Krisenstab bilden
- Kommunikation
- Verträge prüfen (welche Zusicherungen gibt es? SLA?)
- Checkliste für Informationen der Aufsichtsbehörden

# Klärung so schnell wie möglich:

1. **Was ist passiert? Von wem?**
2. **Seit wann?**
3. **Welche Daten sind betroffen?**
4. **Sind personenbezogene Daten dabei?**
5. **Sind Kreditkarten betroffen?**
6. **Wer betreibt das Rechenzentrum?**
7. **Wie hat das Unternehmen davon erfahren?**
8. **Besteht die Gefahrenlage weiter? Wie? Von Wem?**
9. **Maßnahmen zur Minderung negativer Folgen?**

# Planung und Ablauf der Kundenkommunikation

- Klärung so schnell wie möglich
- Krisenstab bilden
- Kommunikation
- Verträge prüfen (welche Zusicherungen gibt es? SLA?)
- Checkliste für Informationen der Aufsichtsbehörden

# Krisenstab bilden

- **Geschäftsführung**
- **Operations**
- **Development**
- **Legal**
  - **Externer Support notwendig: Kanzlei / forensisches Unternehmen**
- **Public Relationship (ggf. externe Krisenprofis hinzuziehen)**
- **IT Security**
- **Datenschutzbeauftragter**
  - **Notfall/Krisenplan gemäß BDSG (Teil der sog. Organisatorisch Technische Maßnahmen)**

# Planung und Ablauf der Kundenkommunikation

- Klärung so schnell wie möglich
- Krisenstab bilden
- Kommunikation
- Verträge prüfen (welche Zusicherungen gibt es? SLA?)
- Checkliste für Informationen der Aufsichtsbehörden

# Kommunikation

## Wichtig:

1. **Keine Korrespondenz, Pressemitteilung, offiziellen Telefonate mit betrieblichen Datenschutzbeauftragten von Kunden oder Behörden ohne Beteiligung der Rechtsabteilung/Datenschutzbeauftragten.**

2. **Abstimmung von „Krisen Q & A“**

   - **Aufklärung soweit möglich + sinnvoll**
   - **Vertrauen schaffen (Message wenn möglich: Situation ist unter Kontrolle)**
   - **Hilfestellung geben**
     - **z. B. wenn § 11-Verhältnis: Musterschreiben für die Auftraggeber zur Erfüllung der Informationspflicht**
   - **Deeskalierung (Shit Storm vermeiden!!!)**
   - **Beruhigung der Öffentlichkeit**

# Kommunikation

- **Presse – Briefing**
  - **Kanalisierung, Meinungsführerschaft übernehmen**
  - **Kernbotschaften übermitteln**
    - **Situation ist im Griff**
    - **Kreis der Betroffenen ist klein**
    - **etc.**
- **Ziel der Pressearbeit**
  - **Raus aus der Presse**
  - **Management von Selbstdarstellung abhalten, sofern Neigung besteht!**
  - **Nur gravierende Fehler korrigieren (Rechtsabt. sollte presserechtlichen Maßnahmen nur als „ultima ratio“ ergreifen, meist folgt sonst der Shit Storm).**

# Kommunikation

**3. Klären wer zu informieren ist:**

**a) Polizei (Cyber Crime – Abteilungen der LKA, nicht lokale Kripo)**

- **Zusammenarbeit erhöht Chance der Schadensminderung, Ergreifung –**

  **„Polizei, Dein Freund und Helfer“!**

- **Strafanzeige stellen**

**b) Aufsichtsbehörden**

- **Personenbezogene Daten? (§42a BDSG; TMG, TKG, EU-VO)**

**c) Interne Stellen**

- **Konzernabteilungen**
- **Aufsichtsrat**
- **Investoren**

**d) Kreditkartengesellschaften**

- **Kreditkartendaten betroffen**

# Kommunikation

**4. Informationspflicht wann:**

**a) besondere Art personenbezogener Daten (§3 IX BDSG)**

- **Rasse, ethnische Herkunft, politische Überzeugung, Gesundheit, Sexualleben**

**b) Berufsgeheimnisse**

**c) Daten über Straftaten, Ordnungswidrigkeit**

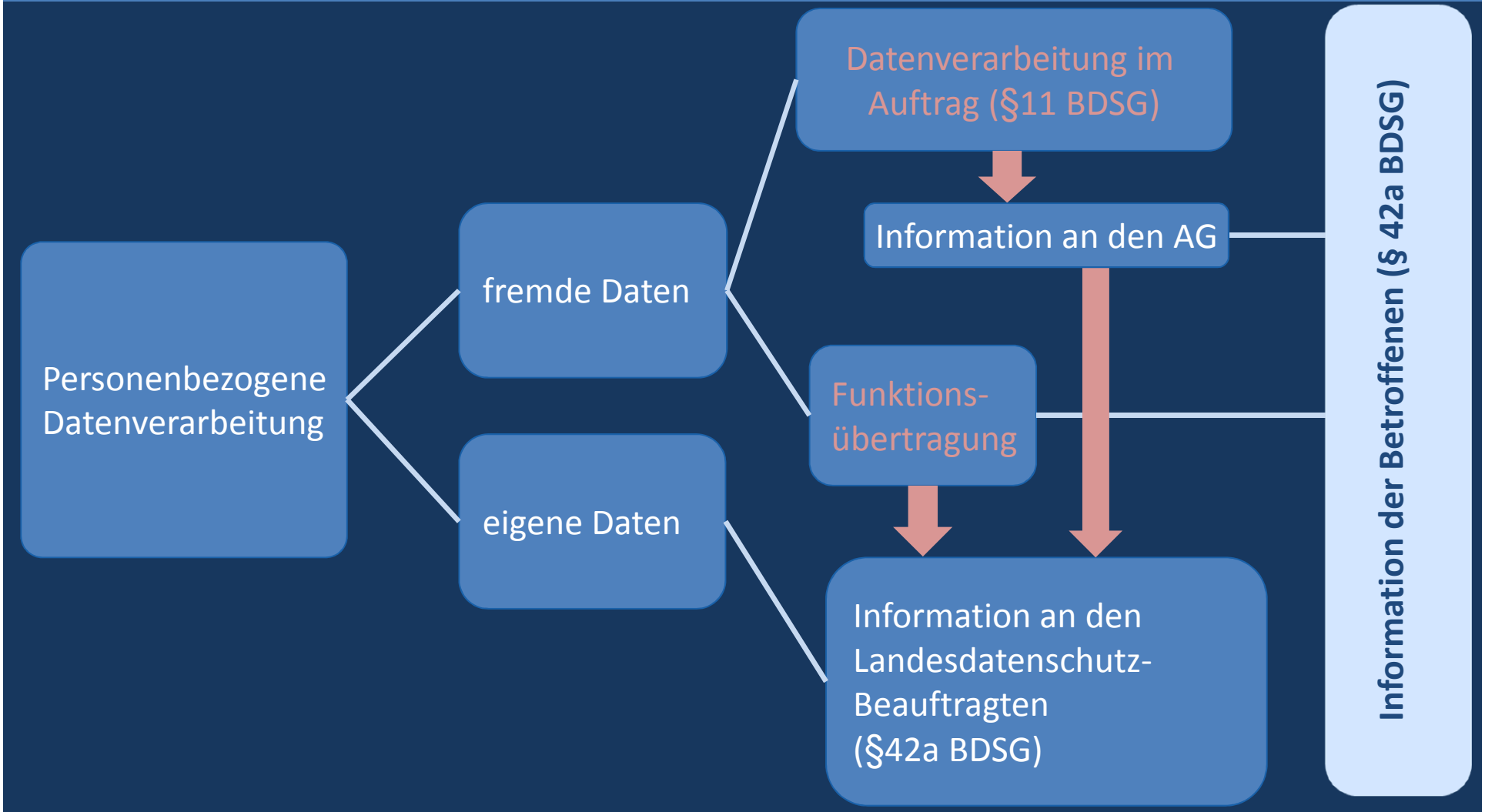
**d) Bank-/Kreditdaten**

**5. Wenn zahlreiche Kunden betroffen sind:**

**a) Prüfen, ob eine Callcenter-Nummer geschaltet wird**

**b) Einrichten einer Sonderseite i.R. des Internetauftritts**

# Kommunikation



# Kommunikation

**6. Form der Information der Betroffenen:**

**a) Direkt per eMail, Anruf, Brief**

**<u>oder</u>**

**b) Halbseitige Anzeige in zwei überregionalen Tageszeitungen**

**Frist der Benachrichtigung**

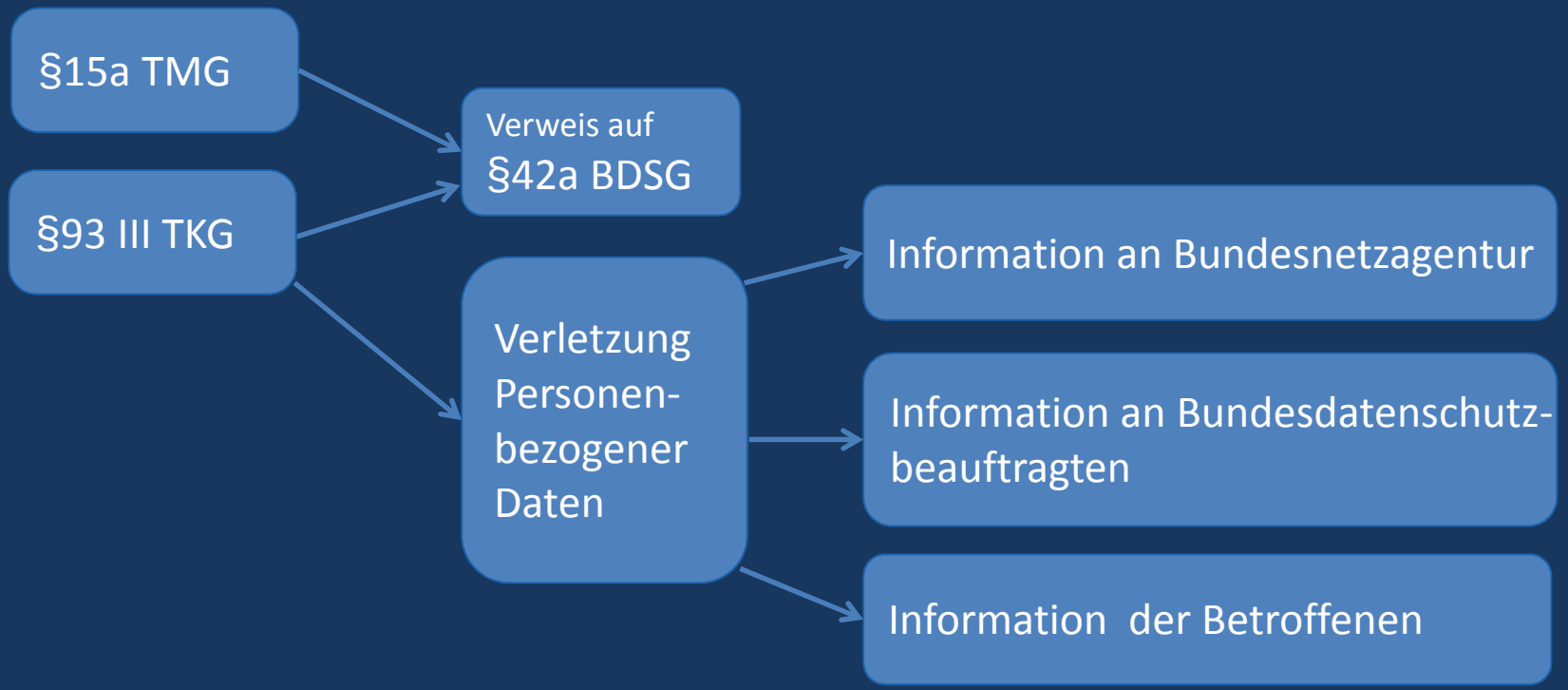
- **Unverzüglich**
- **Einzelfallabhängig i. d. R. nicht länger als 2 Wochen**

**<u>Verstoß:</u> Bußgeld bis zu 300.000 Euro (§42II, Nr. 7 Abs. 3 BDSG)**

# Kommunikation

## Besondere Vorschriften für TK-Unternehmen:

### 1) Deutschland:



# Kommunikation

## Besondere Vorschriften für TK-Unternehmen:

### 2) EU

Seit 25.8.2013 unmittelbar für öffentlich zugängliche Betreiber von Telekommunikationsdiensten gilt:

VO (EU) 611/2013:

- 24 Stunden Meldepflicht
  - Zuständige nationale Datenschutzbehörde = Landesdatenschutzbeauftragter
  - Form: Online-Standardformular
  - Betroffene: Wenn nachteilige Beeinträchtigung der Privatsphäre zu befürchten (nicht der Fall bei Verschlüsselung und wenn diese noch intakt).
    - Vorteil wenn PCI-DSS eingehalten.

  Beeinträchtigung ist gegeben, wenn kompromittierte Daten:

    - Finanzielle Information enthalten
    - Standort-/Adressdaten betreffen
    - zu Rufschädigung oder
    - Physischer Schädigung führen könnten

# Planung und Ablauf der Kundenkommunikation

- Klärung so schnell wie möglich
- Krisenstab bilden
- Kommunikation
- Verträge prüfen (welche Zusicherungen gibt es? SLA?)
- Checkliste für Informationen der Aufsichtsbehörden

# Vertragsprüfung

- **Schadenersatz**
  - **Vertraglich geregelt?**
  - **Gesetzliche Regelung**

- **Versicherungen ggf. informieren**
  - **Policen prüfen**
  - **Fristen beachten**

# Planung und Ablauf der Kundenkommunikation

- Klärung so schnell wie möglich
- Krisenstab bilden
- Kommunikation
- Verträge prüfen (welche Zusicherungen gibt es? SLA?)
- Checkliste für Informationen der Aufsichtsbehörden

# Checkliste für Information der Aufsichtsbehörden

1. **Wer hat was getan?**
2. **Welche Daten sind wem zur Kenntnis gelangt?**
3. **Wie ist die unrechtmäßige Übermittlung/Kenntniserlangung der Daten erfolgt?**
4. **Wie und wann hat die verantwortliche Stelle Kenntnis erlangt (interner oder externer Hinweis?)**
5. **Auswirkungen für Betroffene**
6. **Empfehlungen für Maßnahmen zur Minderung nachteiliger Folgen**
7. **Darstellung der bisherigen Schutzmaßnahmen**

# The day after… Chancen nutzen!!

Sofern Rechtsabteilung nicht optimal aufgestellt war

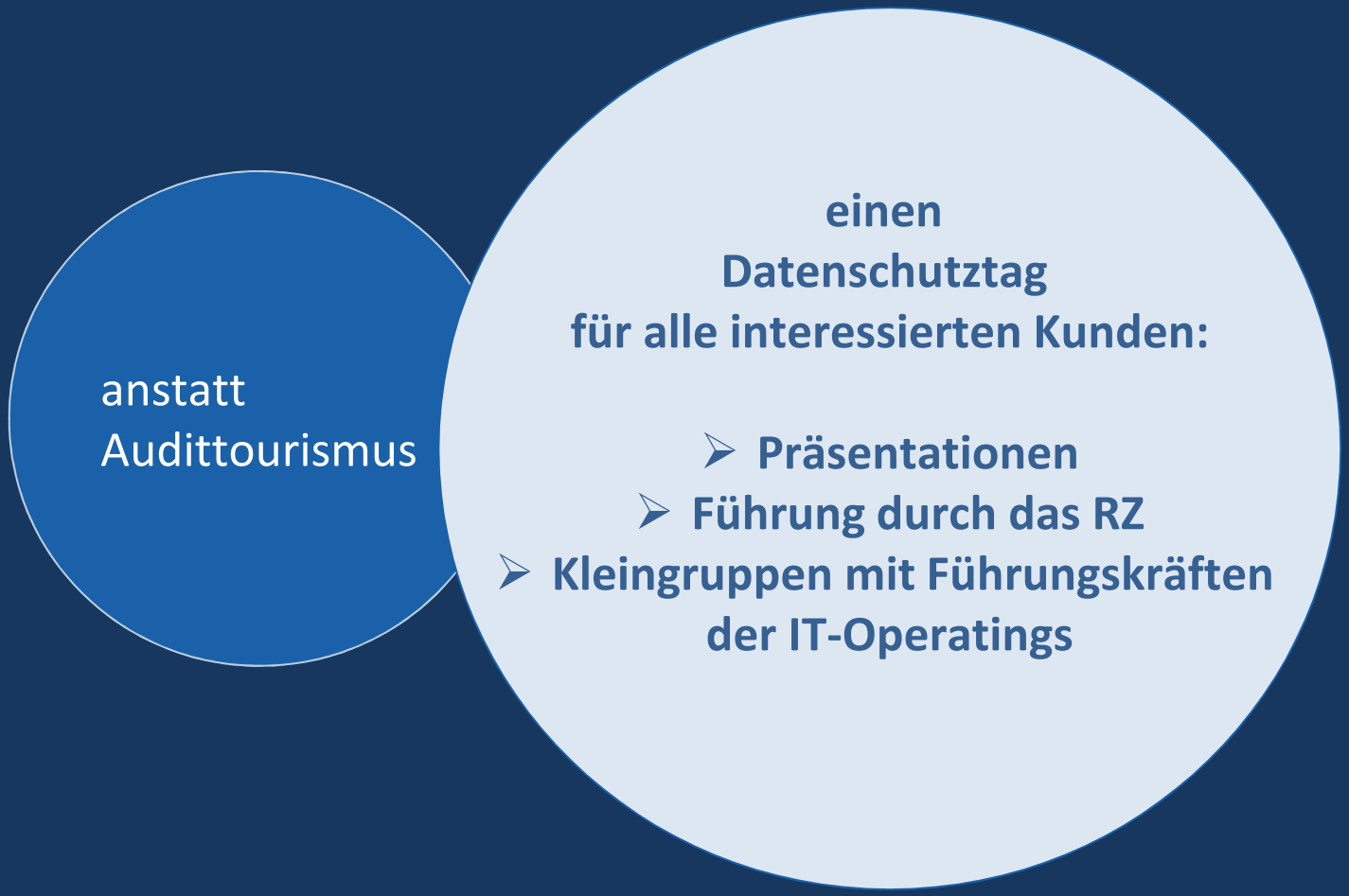
Chance nutzen

Bereitschaft Verbesserungen von Datenschutz und Datensicherheit zu finanzieren ist jetzt besonders hoch

Gefahr, dass die Aufsichtsbehörde den Hackerangriff zum Anlass eines Audits nimmt, ist gegeben

Überprüfung der organisatorisch, technischen Maßnahmen (OTMs)

# Kundenaudits anlässlich des Hackerangriffs



# Conclusion

**there will always be mice!**

**we constantly improve.**

**we are well prepared.**

# Questions