
# Informationssicherheit und Notfallmanagement bei Cyberangriffen

## LWL.IT Service Abteilung

# Agenda

**Teil 1 – Methodik und Systematik nach BSI**

1.1 Motivation

1.2 Systematik für Resilienz

1.3 Maßnahmen mit einem ISMS

**Teil 2 - Informationssicherheit bei DiPS.kommunal**

2.1 Maßnahmen für DiPS.kommunal beim LWL

2.2 DiPS.kommunal beim Kunden

2.3 Empfehlungen für sichere Archive

*Foto von Michael Dolnick auf unsplash.com*

# Warum ist Informationssicherheit wichtig?

## Sollte ich mir auch Sorgen machen?

- Zunehmende Digitalisierung macht Behörden und Verwaltung verwundbarer
- „Wir sind für Cyberangriffe uninteressant“ gilt nicht mehr
- Gefahr durch gezielte oder zufällige Kompromittierung

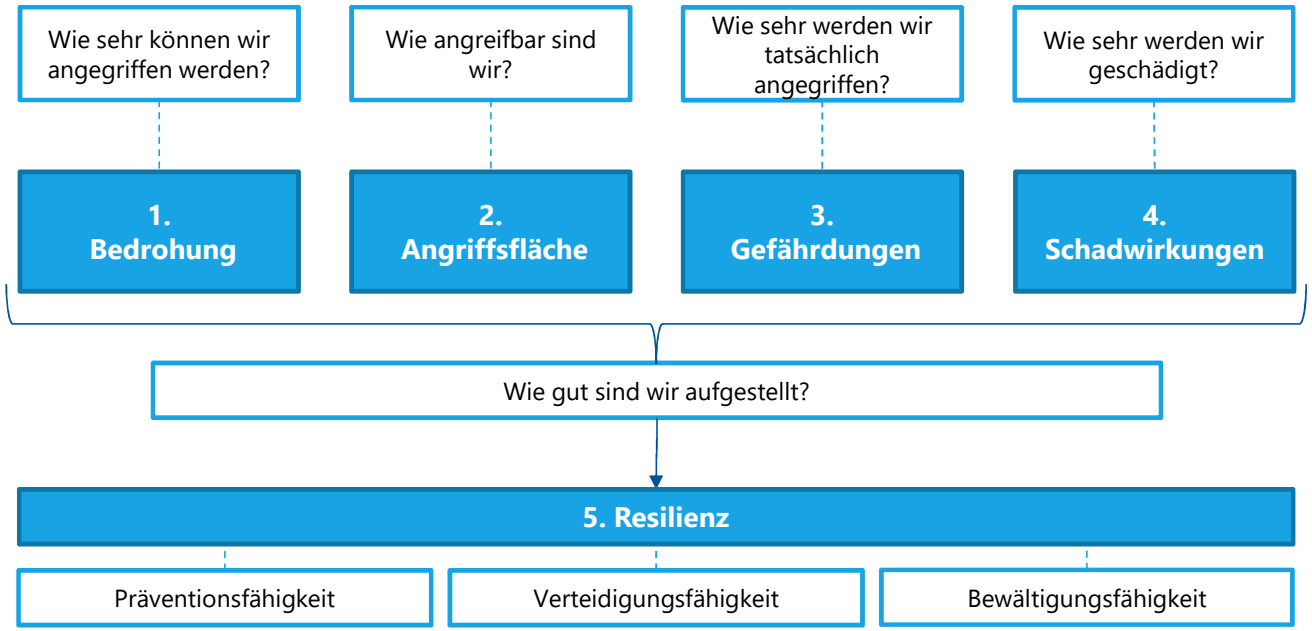
## Was kann passieren?

- Größtes Desaster (aber unwahrscheinlich): Verlust der Primärdaten
- Verlust der Daten, die sich in der Bearbeitung befinden
- Verlust der Daten in der Erschließungssoftware
- Imageschaden, Vertrauensverlust

## Betroffene öffentliche Institutionen in letzter Zeit

- Landkreis Anhalt-Bitterfeld - 6. Juli 2021
- Südwestfalen-IT - 18. Oktober 2023
- Stadtverwaltung Aschaffenburg - 14. November 2024
- Kreis Kitzingen - Oktober 2024
- Heinrich-Heine-Universität Düsseldorf (HHU) - März 2024
- Berliner Hochschule für Technik - 20. Februar 2024
- Gemeinde Petersberg - 7. Februar 2024
- Landratsamt Kelheim - 6. Februar 2024
- Berliner Archiv der DDR-Opposition - 26. August 2024

# Systematik nach BSI

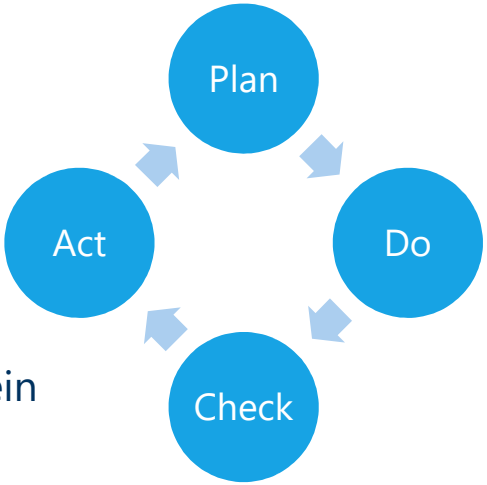


# Beispiele Maßnahmen (TOMs)

| | Präventionsfähigkeit | Verteidigungsfähigkeit | Bewältigungsfähigkeit |
|---|---|---|---|
| Beispiel Feuer | - $O_2$-Reduktion in Serverräumen | - Brandmelde- und Feuerlöschanlage | - Zweiter Serverraum |
| Organisatorisch | - Informationssicherheits-Managementsystem (ISMS)<br>- Patchmanagement<br>- Schulung und Sensibilisierung | - Systematisches Monitoring<br>- Strukturierte Vorfallsbehandlung<br>- Security Operations Center | - Business Continuity Management (BCM)<br>- Definierte Ersatzprozesse<br>- Notfallpläne<br>- Übungen |
| Technisch | - Verschlüsselung<br>- Sichere Konfiguration<br>- Begrenzte Benutzerrechte<br>- Firewall | - Antivirenschutz<br>- Extended Detection and Response | - Redundante Ausführung von Kernkomponenten<br>- Datensicherung |

# Informationssicherheits-Managementsystem (ISMS)

- „Nicht zufällig das Richtige machen“ -




Ein Informationssicherheits-Managementsystem (ISMS) etabliert in einer Organisation ein strukturiertes Vorgehen zur Sicherstellung und kontinuierlichen Weiterentwicklung von Maßnahmen zur Steigerung der Resilienz.

Analog zum Qualitätsmanagement existieren verschiedene Standards, nach denen ein ISMS aufgebaut werden kann:

- ISO 27001: Internationaler, risikoorientierter Standard für die Informationssicherheit
- BSI Grundschutz-Standards 200-1, 200-2 und 200-3 und BSI Standard 200-4 für BCM
- Branchenspezifische Standards (z. B. Gesundheitswesen)

# Informationssicherheit bei DiPS.kommunal

- Welche Rahmenbedingungen bestehen?
- Welche Ziele bestehen seitens des LWL für DiPS.kommunal und welche Maßnahmen werden angewendet?
- Was ist auf Kundenseite zu berücksichtigen?

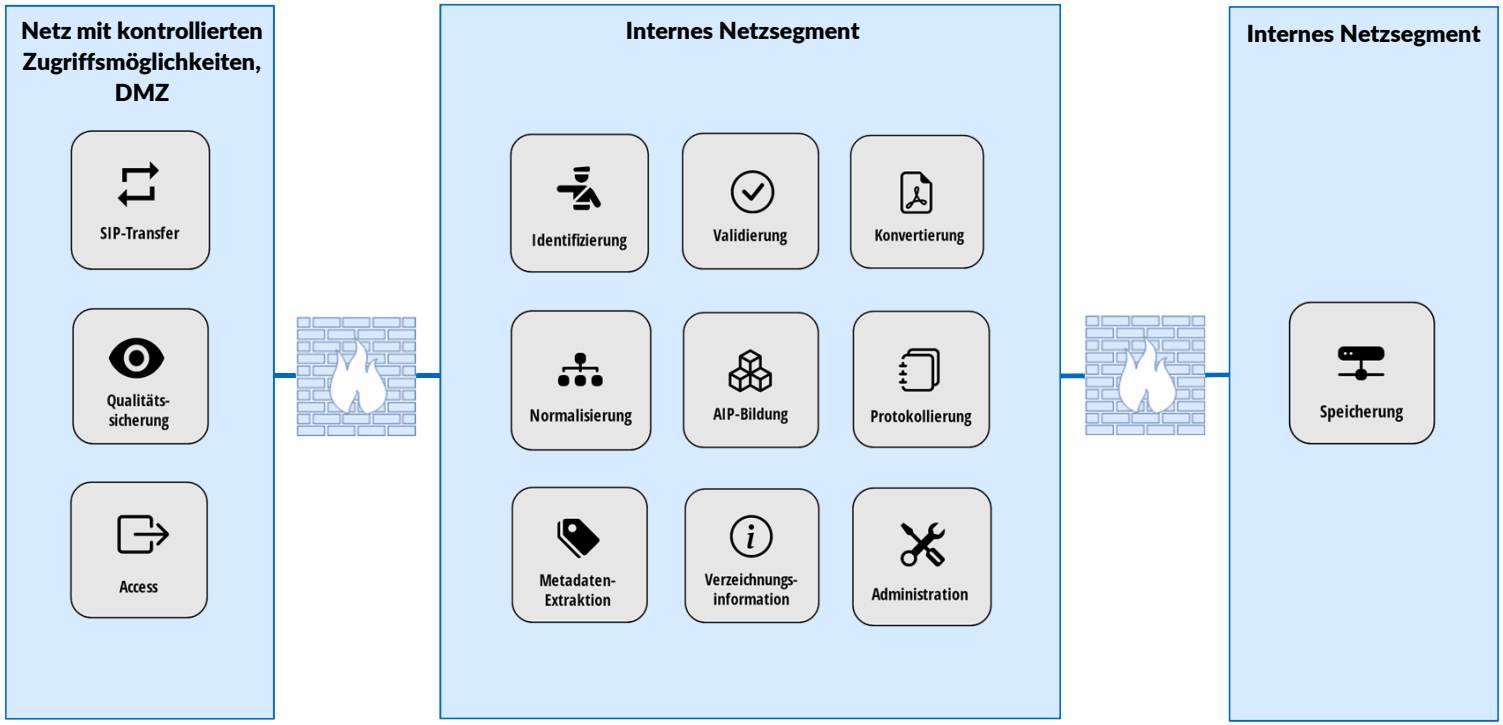
# DiPS.kommunal – Betrieb auf Seite des LWL

## Funktionskomponenten eines digitalen Archivs am Beispiel von DiPS.kommunal

# DiPS.kommunal – Betrieb auf Seite des LWL

**Prävention** (Analogie Feuerschutz: $O_2$-Reduktion, Feuerschutztüren)

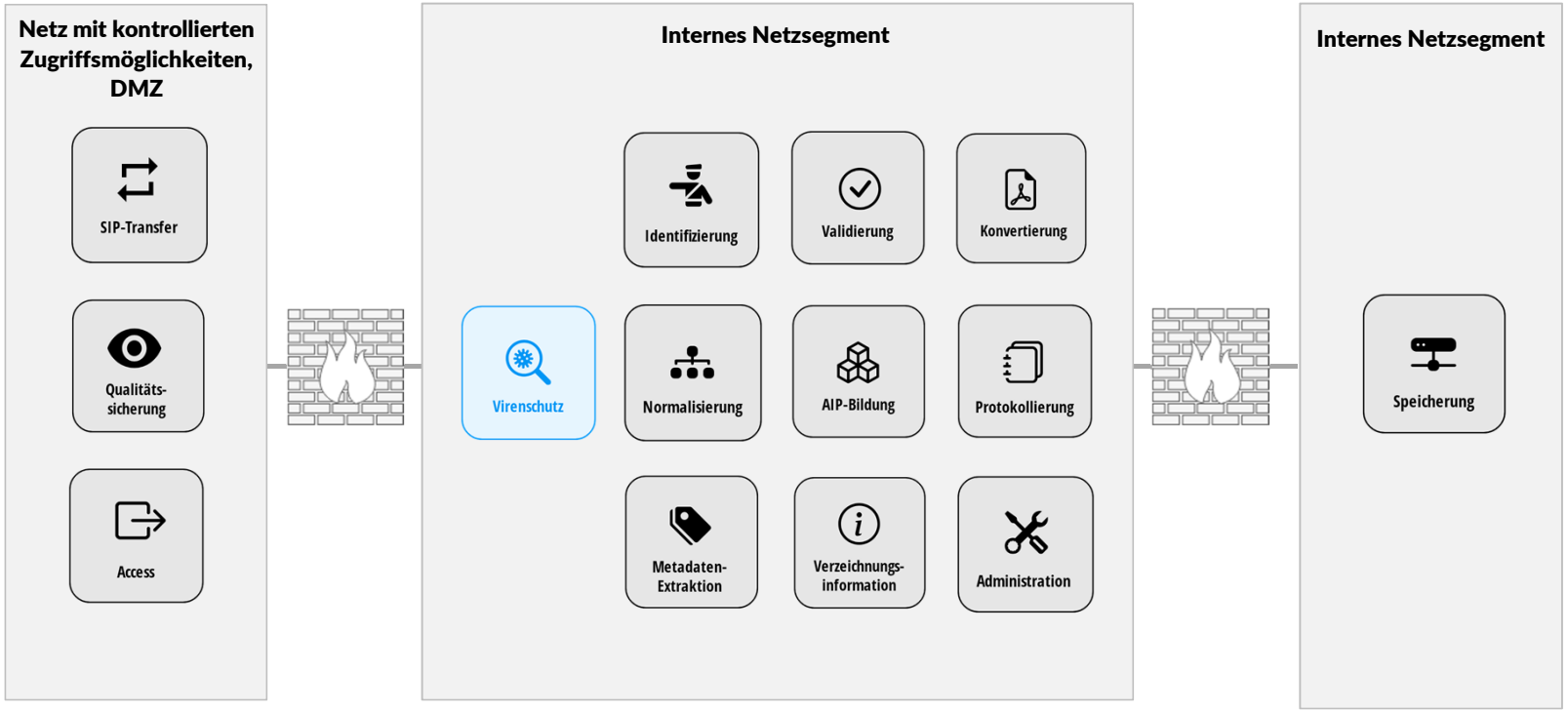
- Netzsegmentierung
- Kommunikation auch intern über TLS
- Komponenten vertrauen sich nur anhand von Zertifikaten
- Systemnutzer mit minimalen Rechten
- Mehrfaktor-Authentisierung für Administratoren



# DiPS.kommunal – Betrieb auf Seite des LWL

**Verteidigung** (Analogie Feuerschutz: Brandmelder, Sprinkleranlage)

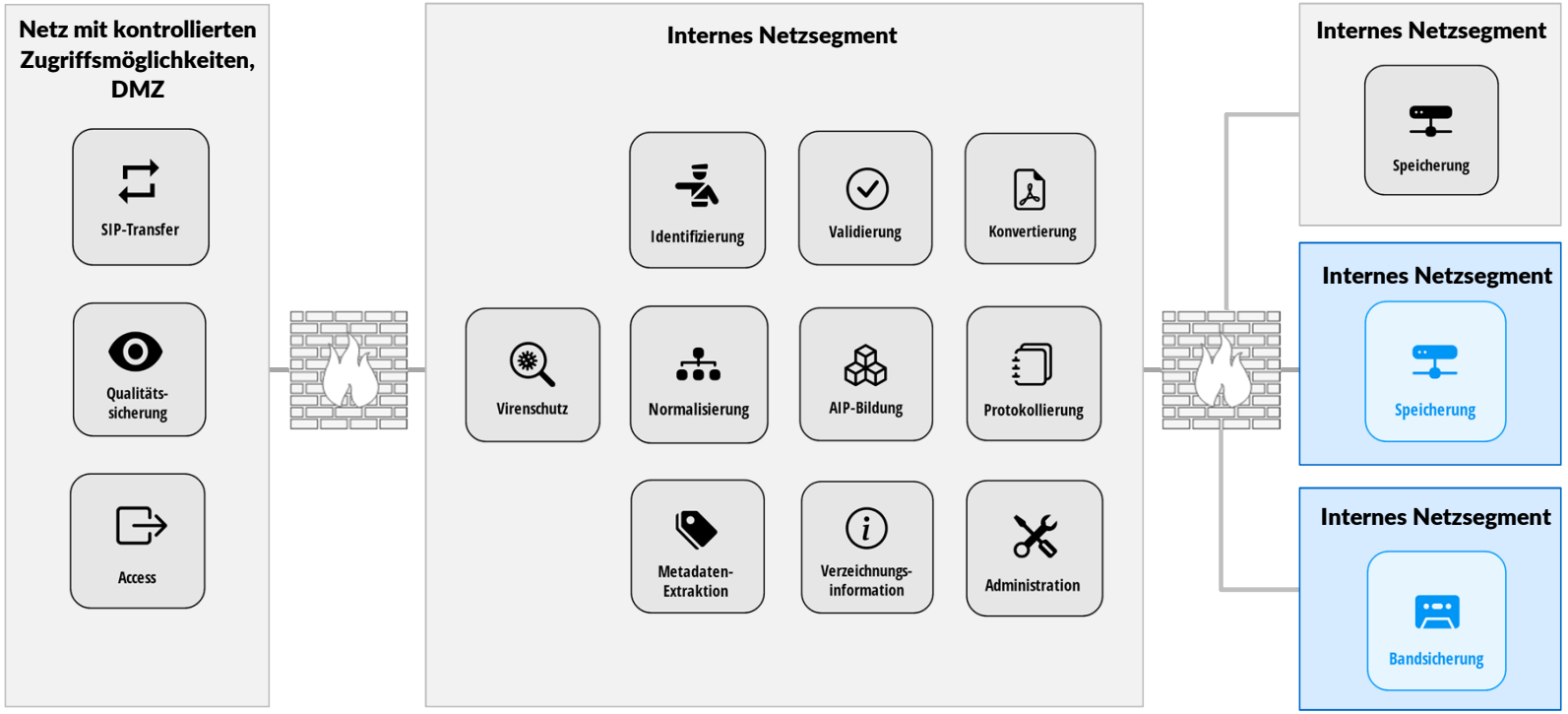
- Virenschutz
- Systemüberwachung
- Log-Analyse



# DiPS.kommunal – Betrieb auf Seite des LWL

**Bewältigung** (Analogie Feuerschutz: Gebäudeteile doppelt auslegen)

- Backup auf Band
- Redundante WORM-Speicher
- Tertiärsicherung im Rechenzentrum der Stadt Köln im Aufbau

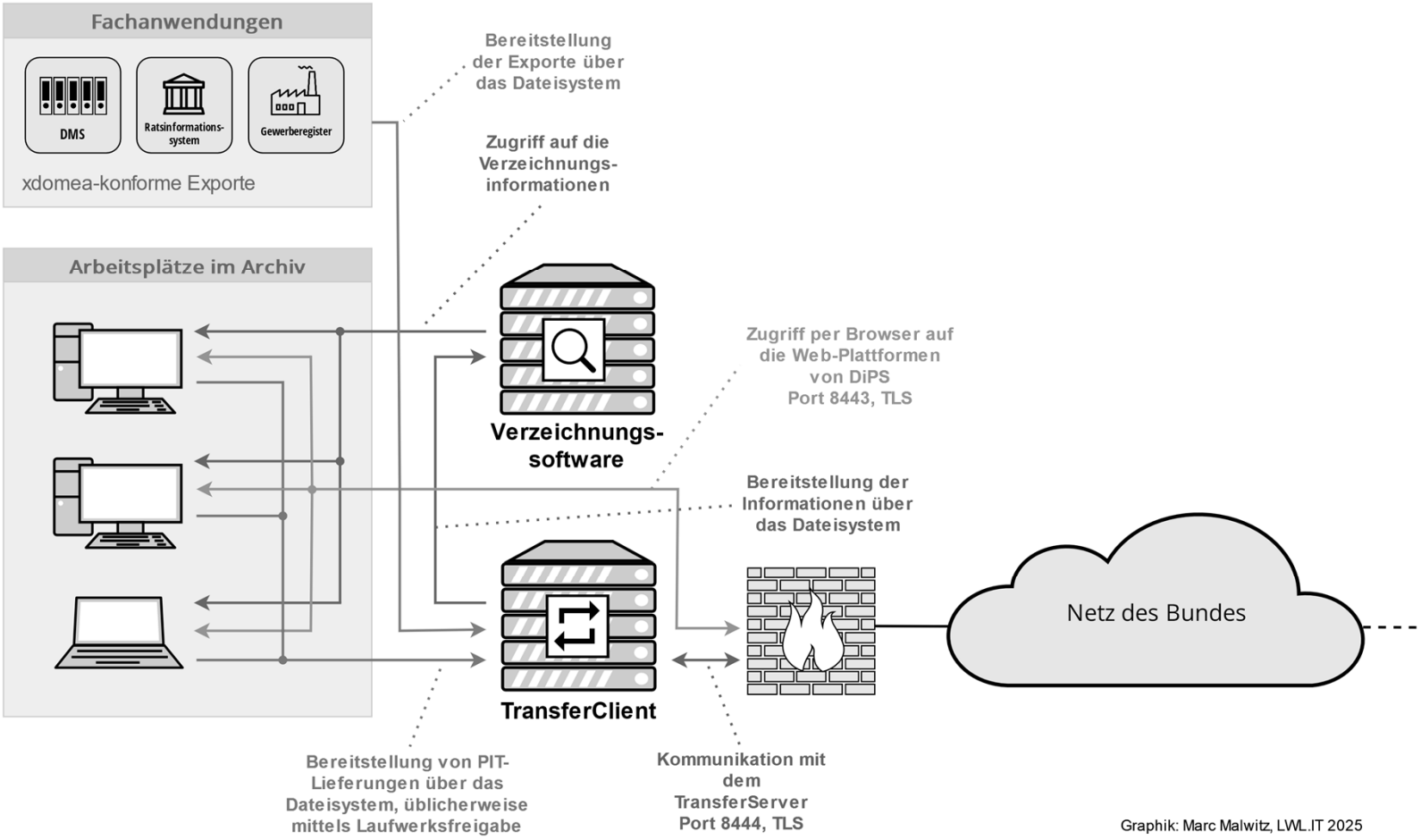


# DiPS.kommunal – Betrieb auf Seite des Kunden

Die Kundenseite kann der LWL nicht absichern!

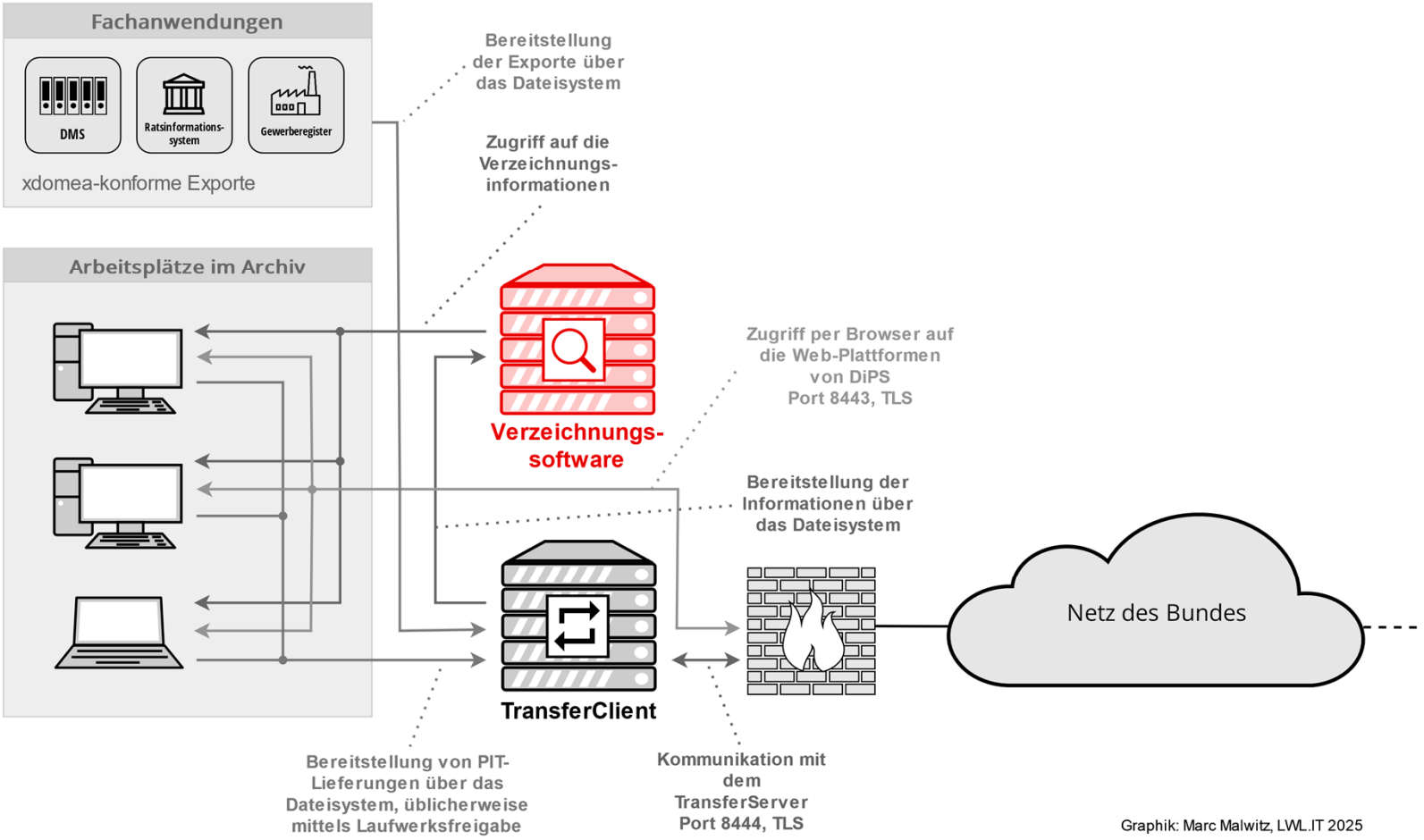
Was ist zu beachten?

# DiPS.kommunal – Betrieb auf Seite des Kunden




Graphik: Marc Malwitz, LWL.IT 2025

# DiPS.kommunal – Betrieb auf Seite des Kunden




Graphik: Marc Malwitz, LWL.IT 2025

# DiPS.kommunal – Betrieb auf Seite des Kunden

**Empfehlungen, um die Resilienz zu steigern**

- Orientierung an Standards
- Informationssicherheits-Managementsystem etablieren, Maßnahmen entwickeln, fortschreiben
- Ressourceneinsatz: Bedrohungslagen prüfen, aber auch Wirtschaftlichkeit berücksichtigen
- Archivische Assets beurteilen, Risikoschätzung
- IT-Sicherheit ist Querschnittsaufgabe: Kooperation aus Archivaren und IT-Mitarbeitern bilden
- Digitalen Notfallplan erstellen und auf Funktion prüfen, Maßnahmen zur Wiederaufnahme des Betriebs nach Problemen berücksichtigen
- Größtes Einfallstor ist der Benutzer - Berechtigungen restriktiv vergeben, auch wenn es unbequem ist
- Bewusstsein und Expertise aufbauen! Ransomware kommt da rein, wo Angreifer das System besser verstehen als der Betreiber

# Vielen Dank für Ihre Aufmerksamkeit.

Jannes Riffert, Marc Malwitz

**Landschaftsverband**
**Westfalen-Lippe (LWL)**
**LWL.IT Service-Abteilung**

Besuchen Sie uns im Internet: **https://www.lwl.it/**