

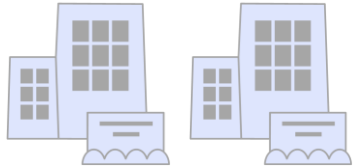
Anwendbarkeit der TeleTrust Handreichung zum „Stand der Technik“ in der Praxis

Workshop LSZ Security & Risk Management Kongress

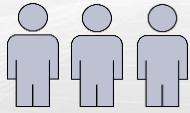
www.uninet.at | info@uninet.at | Büro: Business Campus One, Softwarepark 32/1, 4232 Hagenberg



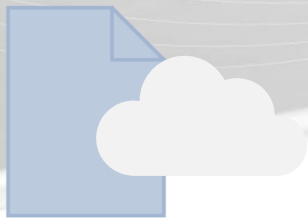
Musterunternehmen GmbH



- Produktionsunternehmen mit zwei Standorten
- Hauptsitz in Musterstadt, Produktionsstätte in Beispielhausen
- Beide Standorte sind vernetzt

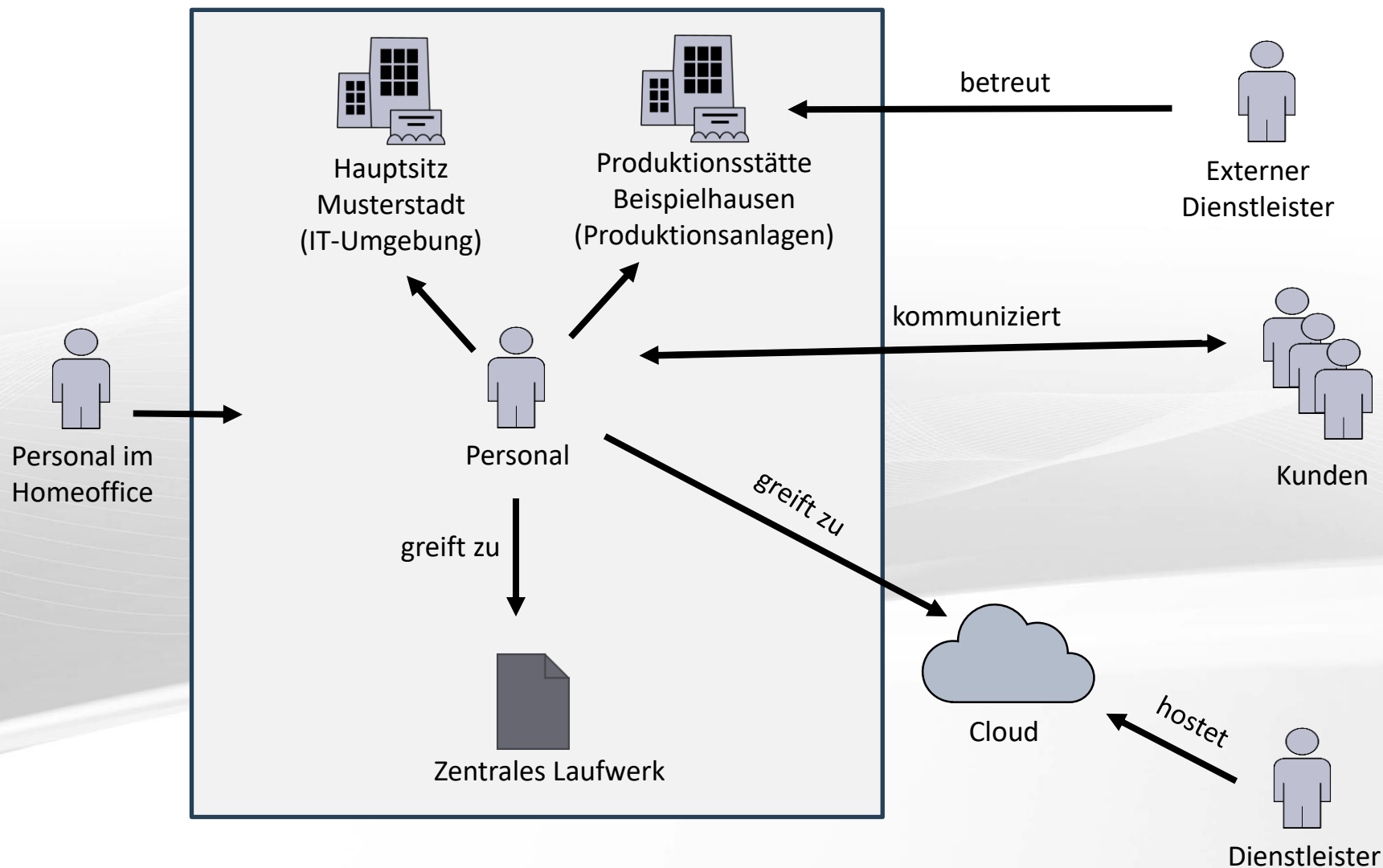


- Herstellung von Elektronikkomponenten für die Automobil- und Industriebranche
- 56 Mitarbeitende
- IT-Abteilung mit 2 Mitarbeitern, kümmern sich um alle technischen Systeme (Produktionsanlagen, Büro-PCs etc.)



- Mitarbeitende greifen auch von zuhause aus auf Unternehmensdaten zu
- Produktionsdaten werden auf einem zentralen Laufwerk im Unternehmensnetzwerk gespeichert
- Kundendaten werden in der Cloud verwaltet
- Kommunikation mit Kunden und Lieferanten erfolgt hauptsächlich per E-Mail

Musterunternehmen GmbH



Aufgabenstellung für Teilnehmer:innen

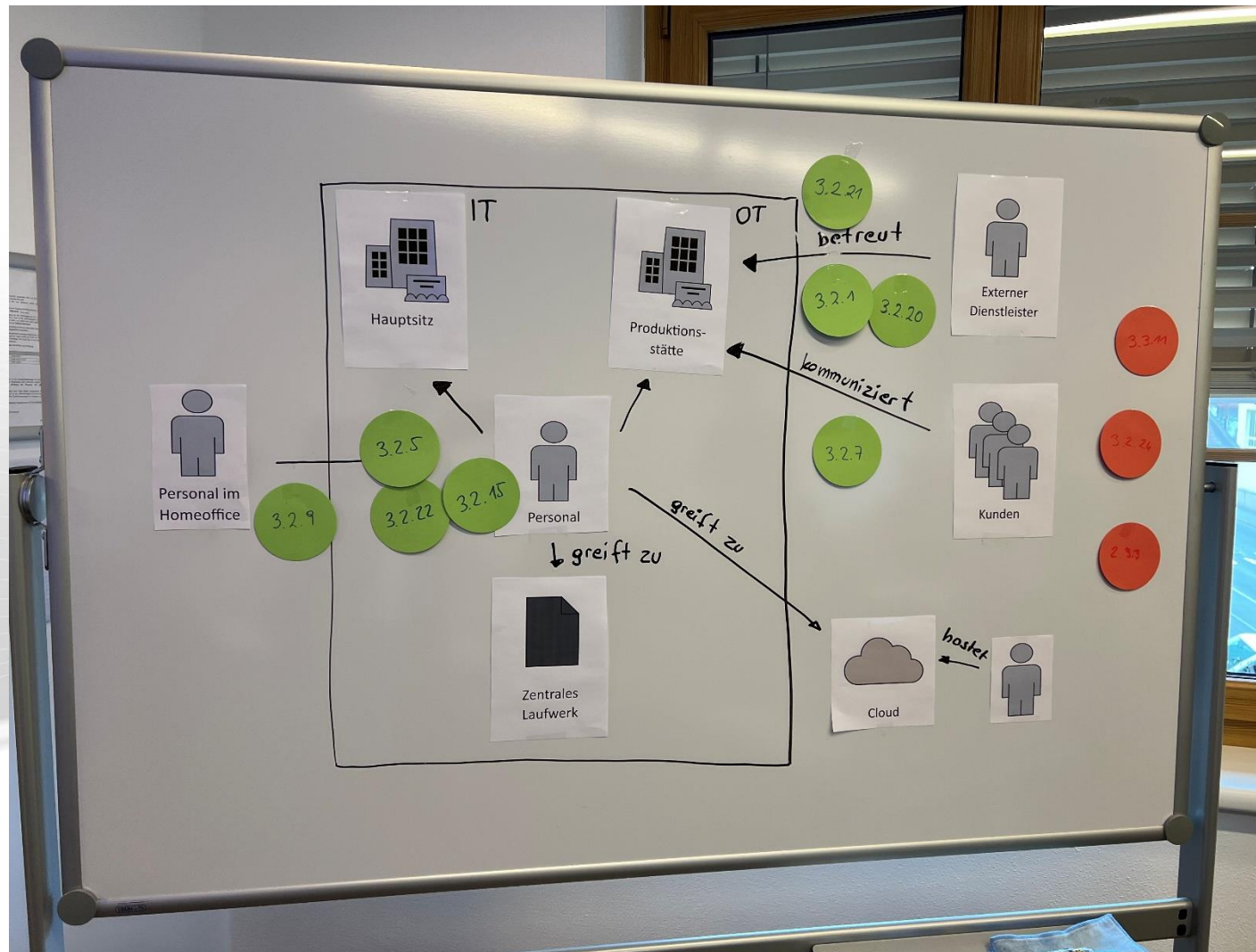
- Pro Gruppe ist ein:e Sicherheitsverantwortliche:r zu bestimmen, der:die im Anschluss die jeweilige Ausgangslage und entsprechende Ausarbeitung präsentiert
- Je Gruppe gibt es eine ausgedruckte Handreichung (kann aufgeteilt werden oder digital gelesen werden – siehe QR-Code), Kärtchen zum Beschriften der Kapitelnummern aus der Handreichung und eine Beschreibung der Szenarien

Konkrete Aufgabenstellung:

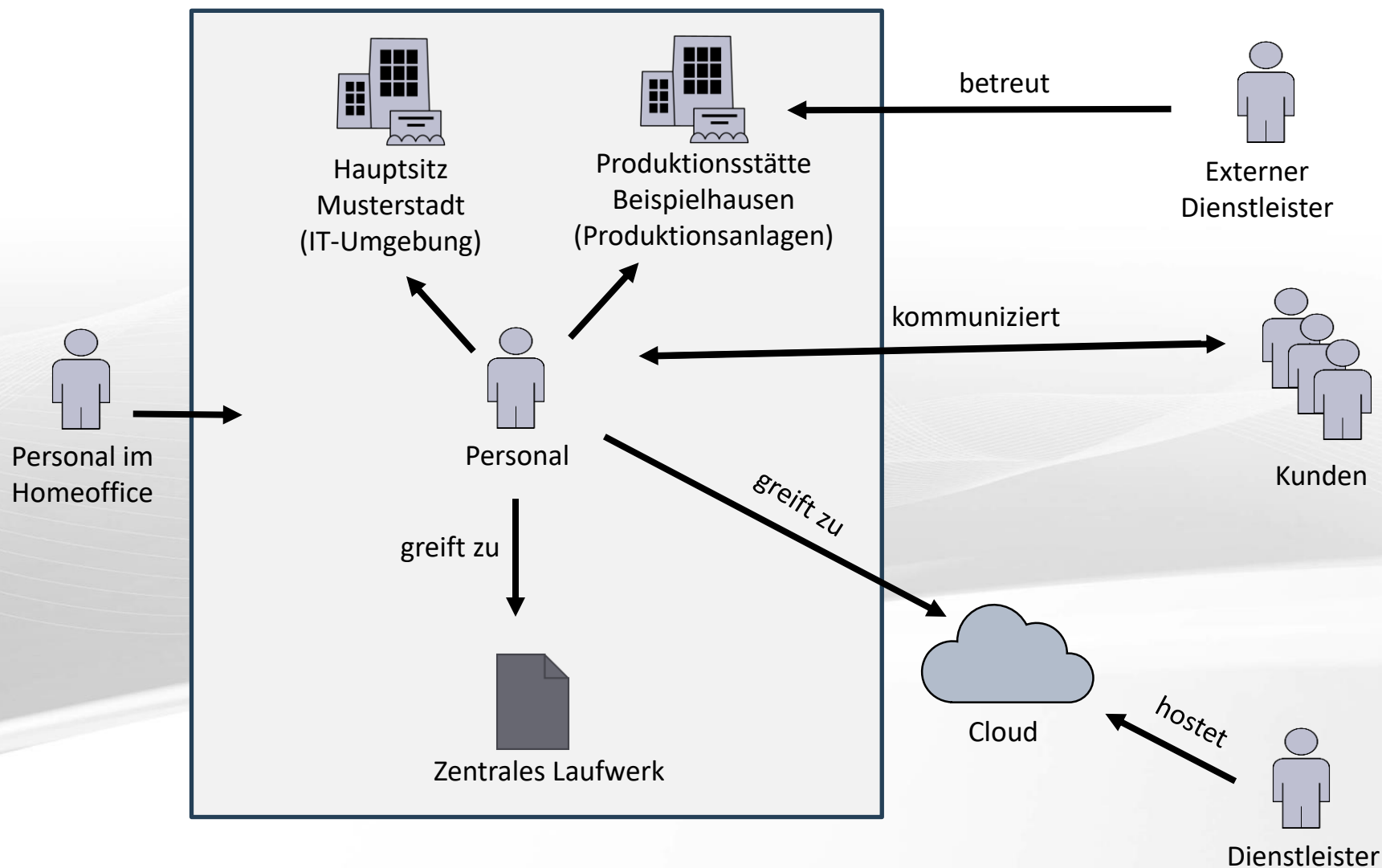
- Analyse der vorhandenen Informationen der Musterunternehmen GmbH
- Ableitung von Risiken im Bereich Informationssicherheit und IT-Sicherheit
- Erarbeitung von Maßnahmen aus der Handreichung zum Stand der Technik, um die Situation für die Musterunternehmen GmbH zu verbessern
 - Nennung des Kapitels aus der Handreichung zum Stand der Technik
 - Kurze Beschreibung der Maßnahme



Ergebnisse



Musterunternehmen GmbH



- 3.2.2 Starke Passwörter
- 3.2.3 MFA
- 3.2.5 / 3.2.6 Verschlüsselung
- 3.2.9 Einsatz von VPN
- 3.2.12 Datenablage in der Cloud
- 3.2.15 Management mobiler Geräte
- 3.2.17 Netzwerküberwachung mittels IDS
- 3.2.20 Fernzugriff auf Netzwerke
- 3.2.21 Serverhärtung
- 3.2.28 Absicherung administrativer IT-Systeme
- 3.2.30 Netzwerksegmentierung
- 3.3.5 Schwachstellen- und Patchmanagement
- 3.3.8 Umgang mit Dienstleistern
- 3.3.10 Absicherung privilegierter Accounts

KONTAKT

UNINET it-consulting GmbH

www.uninet.at, info@uninet.at

Büro:

Business Campus ONE

Softwarepark 32/1

4232 Hagenberg, Österreich

Firmenrechtlicher Sitz

Fichtenstraße 20, 4020 Linz, Österreich

FN 299242m LG Linz, ATU63752406

BBG Lieferant für IT-Consulting und IT-Sachverständige

Vertragsnummer: 3602.04434

